



FortiGate 运营管理维护注意事项

Aug 29, 2022

1 管理员账号分权管理

2 HA配置同步

3 CLI / GUI 配置检查

4 规范调试操作

5 SNMP信息采集/远程服务器日志记录

6 Comlog功能

7 设备定时配置备份



管理员账号分权管理



管理员账号分权管理

案例

某公司，代理商工程师巡检时误操作，将某台生产运行的防火墙进行了配置重置，严重影响了生产。

Summary

非甲方运维人员对FortiGate防火墙进行操作，使用的如果是最高级别权限super_admin的管理员帐号，那么有可能造成例如配置重置，配置恢复，设备重启等较为严重的误操作。



管理员账号分权管理

最佳实践

根据不同应用场景设定不同权限的管理员，遵循授权最小化原则，例如巡检这样的应用场景，完全不需要任何“写”权限的管理员帐号。

大规模部署的场景中，建议采用远端认证服务平台例如Radius服务器做管理员认证，FortiGate也支持基于Radius分配管理员权限，方便实现统一的管理员权限管控。（[ref](#)）

```
config system accprofile
  edit "read_only"
    set secfabgrp read
    set ftviewgrp read
    set authgrp read
    set sysgrp read
    set netgrp read
    set loggrp read
    set fwgrp read
    set vpngrp read
    set utmgrp read
    set wanoptgrp read
    set wifi read
  next
end
```



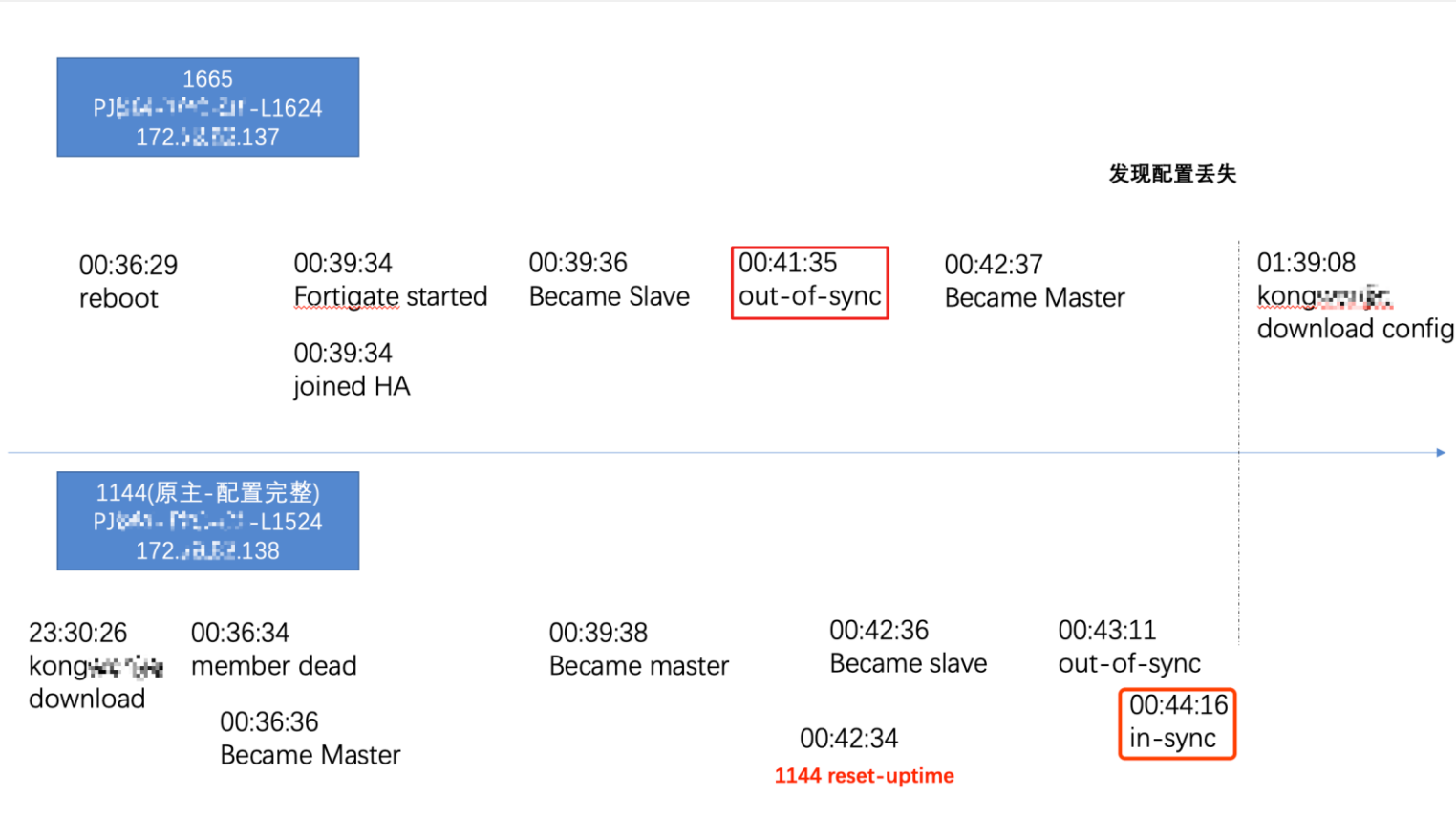
HA配置同步



HA配置同步

案例

某金融行业客户，安排进行防火墙切换测试，发现切换后出现配置丢失问题，通过配置备份以及事件日志等回溯后，发现故障原因是由于切换前主备防火墙的配置并不同步。



HA配置同步

案例总结

Summary

HA模式的防火墙配置同步状态是一个重要的参考状态，特别是在进行人工HA切换的场景下，是必须查看和处理的，尽可能保证HA配置同步后，才能避免配置丢失等风险。

HA 状态

模式 主动-被动

组 SVR

主  GD-XXXXXX-CF01

从  GD-XXXXXX-CF02

持续时间 00:03:34:19

状态改变 00:03:33:59

```
FGT-1 (global) # get sys ha status
FG380DTBXXXXXX50: hadiff-neversync-cnt=0
FG380DTBXXXXXX47: hadiff-neversync-cnt=0
HA Health Status: OK
Model: FortiGate-3800D
Mode: HA A-P
Group: 71
Debug: 0
Cluster Uptime: 13 days 6:10:17
Cluster state change time: 2022-06-06 21:51:33
Master selected using:
    <2022/06/06 21:51:33> FG380DTBXXXXXX50 is selected as the
    master because it has the largest value of uptime.
    <2022/06/06 17:40:15> FG380DTBXXXXXX47 is selected as the
    master because it has the largest value of uptime.
    <2022/06/06 17:19:04> FG380DTBXXXXXX50 is selected as the
    master because it has the largest value of uptime.
    <2022/06/06 16:58:00> FG380DTBXXXXXX47 is selected as the
    master because it has the largest value of uptime.
ses_pickup: enable, ses_pickup_delay=enable (delay 30 seconds)
override: disable
Configuration Status:
    FG380DTBXXXXXX50(updated 1 seconds ago): in-sync
    FG380DTBXXXXXX47(updated 1 seconds ago): out-of-sync
...
Master: FGT-1, FG380DTBXXXXXX50, cluster index = 0
Slave : FGT-2, FG380DTBXXXXXX47, cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Master: FG380DTBXXXXXX50, operating cluster index = 0
Slave : FG380DTBXXXXXX47, operating cluster index = 1
```



HA配置同步

最佳实践

人工进行切换测试前，务必先检查和排除配置不同步的问题。

HA配置不同步问题的处理办法：

- 检查HA配置不同步的VDOM
- 检查上述VDOM里不同步的具体配置菜单
- 对比实际配置尝试手动修正
- 尝试重新计算HA配置校验和

[详细排查参考说明](#)

```
FGT-1# diagnose sys ha checksum cluster

===== FG380DTBXXXXXX50 =====

is_manage_master()=1, is_root_master()=1
debugzone
global: c1 d6 84 41 b6 01 65 96 f5 82 17 cd 6f a1 b3 85
root: 25 fd 0d df 9b 09 67 1b ce 88 6c 0d 29 5d a1 a3
all: af ff 02 ed 4f 94 13 c6 d9 97 c1 6f 96 6c 06 80

checksum
global: c1 d6 84 41 b6 01 65 96 f5 82 17 cd 6f a1 b3 85
root: 25 fd 0d df 9b 09 67 1b ce 88 6c 0d 29 5d a1 a3
all: af ff 02 ed 4f 94 13 c6 d9 97 c1 6f 96 6c 06 80

===== FG380DTBXXXXXX47 =====

is_manage_master()=0, is_root_master()=0
debugzone
global: c1 d6 84 41 b6 01 65 96 f5 82 17 cd 6f a1 b3 85
root: 25 fd 0d df 9b 09 67 1b ce 88 6c 0d 29 5d a1 a3
all: af ff 02 ed 4f 94 13 c6 d9 97 c1 6f 96 6c 06 80

checksum
global: c1 d6 84 41 b6 01 65 96 f5 82 17 cd 6f a1 b3 85
root: 25 fd 0d df 9b 09 67 1b ce 88 6c 0d 29 5d a1 a3
all: af ff 02 ed 4f 94 13 c6 d9 97 c1 6f 96 6c 06 80
```

校验HA配置不同步的vdom

```
diagnose sys ha checksum recalculate [<vdom-name> | global]
```

尝试重新计算HA配置校验和





CLI脚本导入检查

CLI脚本导入检查

案例

某公司，在对防火墙的静态路由进行新增配置下发时，脚本命令有误，导致某条命令下发失效，但是创建出了默认路由，导致流量转发出错，造成业务中断。

Summary

通过CLI命令行对FortiGate进行配置下发时，下发结果可能与预期不符，如果出现错误或者疏忽，有可能造成业务流量中断。

```
FGT # config firewall address
FGT (address) # edit OA_server
new entry 'OA_server' added
FGT (OA_server) # set subnet 192.168.10.100/32
FGT (OA_server) # set allow-routing enable
FGT (OA_server) # next
FGT (address) # end
FGT #
FGT # config router static
FGT (static) # edit 100
new entry '100' added

FGT (100) # set dstaddr OA_Server
entry not found in datasource

value parse error before 'OA_Server'
Command fail. Return code -3

FGT (100) # set device port1
FGT (100) # set gateway 192.168.20.254
FGT (100) # next
FGT (static) # end
```

```
FGT # show full-configuration router static 100
config router static
  edit 100
    set status enable
    set dst 0.0.0.0 0.0.0.0
    set gateway 192.168.20.254
    set distance 10
    set weight 0
    set priority 0
    set device "port1"
    ...
  next
end
```



CLI脚本导入检查

最佳实践

- 校验CLI命令，条件允许的情况下，在测试设备上尝试执行至少一遍脚本，以验证命令有效性。
- 如果还有测试环境，建议模拟变更过程验证变更命令的可靠性。
- 实际操作前做好配置备份，操作时及时验证变更结果并做好检查工作。





CLI添加成员对象

- 用append 命令，不要用set 命令



CLI添加地址成员对象

案例

某公司，CLI添加防火墙地址对象时，用set member 添加地址对象，没有包括所有已经存在的地址对象，导致原有地址的业务受影响

Summary

CLI添加地址对象时，要用append member命令添加对象，添加后show命令确认是否符合预期。

```
config firewall addrgrp
  edit "supportGroup"
    set member "host1" "host2" "host3"
  next
end
```

在地址组里添加成员

```
config firewall addrgrp
  edit "supportGroup"
    append member eastern-team
  next
end
```

```
config firewall addrgrp
  edit "supportGroup"
    set member "host1" "host2" "host3" "eastern-team"
  next
end
```

如果 set member eastern-team, 结果就丢失了host1,2,3

```
config firewall addrgrp
  edit "supportGroup"
    set member "eastern-team"
  next
end
```



CLI添加zone区域成员

案例

某公司，CLI添加zone区域成员时，用set interface 添加接口，没有包括所有已经存在的接口列表，导致原有接口列表的业务受影响

Summary

CLI添加zone区域成员时，要用append interface命令添加接口，添加后show命令确认是否符合预期。

```
config system zone
  edit "portZone"
    set interface "port1" "port2" "port3"
  next
end
```

在zone区域里添加成员

```
config system zone
  edit "portZone"
    append interface port4
  next
end
```

```
config system zone
  edit "portZone"
    set interface "port1" "port2" "port3" "port4"
  next
end
```

如果 set interface port4, 结果就丢失了port1,2,3

```
config system zone
  edit "portZone"
    set interface "port4"
  next
end
```





GUI界面配置地址对象

- 全0问题



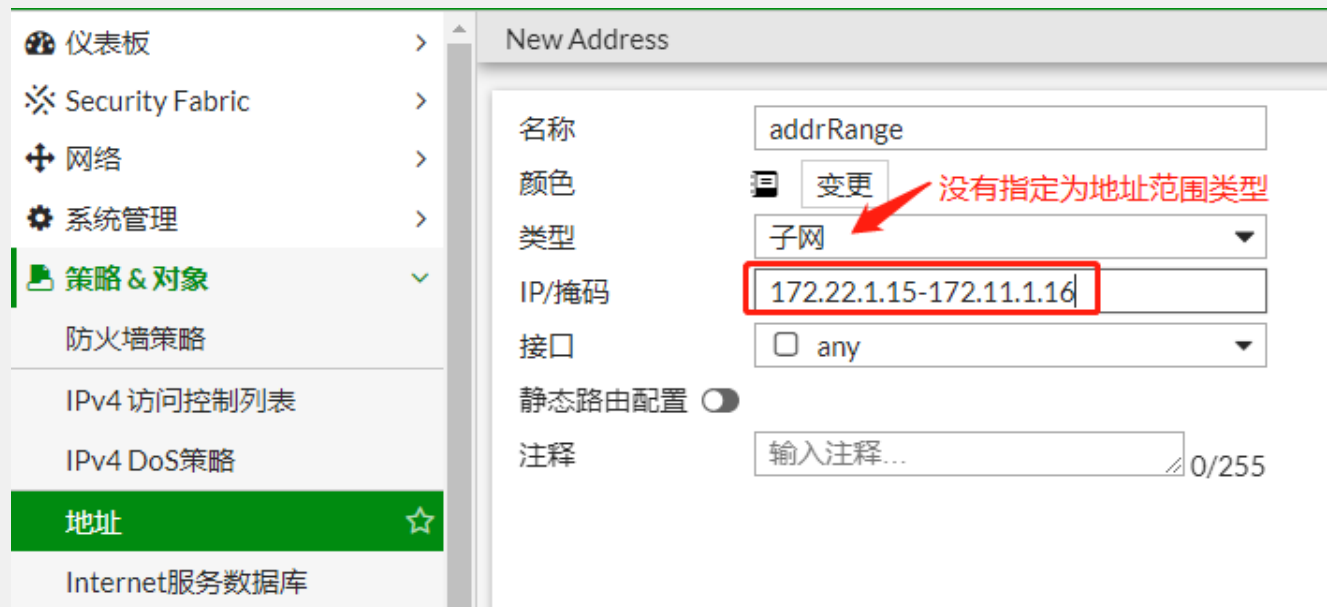
GUI配置地址对象

案例

某公司，在配置防火墙地址对象时，地址类型和输入的地址对象不一致，结果地址自动填充0.0.0.0/0，造成断网事故。

Summary

通过GUI配置编辑地址对象时，要确认输入内容与预期值是否一致，否则带来不必要的网络中断。



New Address

名称: addrRange

颜色: 变更

类型: 子网

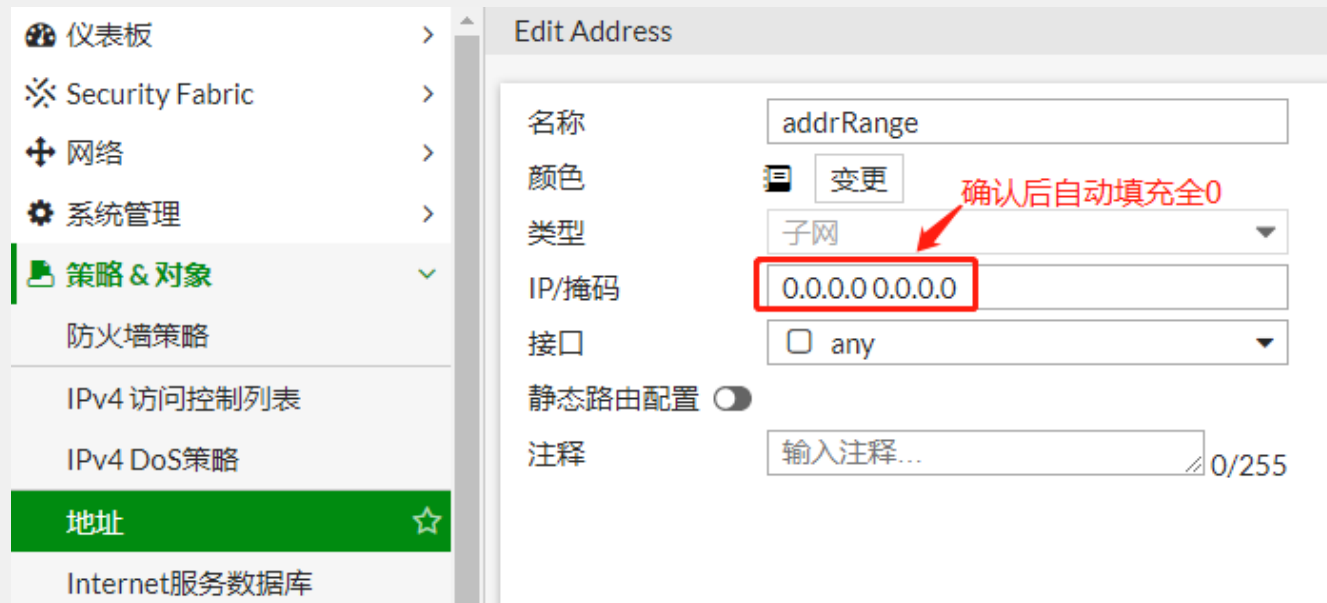
IP/掩码: 172.22.1.15-172.11.1.16

接口: any

静态路由配置: ☐

注释: 输入注释... 0/255

没有指定为地址范围类型



Edit Address

名称: addrRange

颜色: 变更

类型: 子网

IP/掩码: 0.0.0.0 0.0.0.0

接口: any

静态路由配置: ☐

注释: 输入注释... 0/255

确认后自动填充全0



规范调试操作



规范调试操作

案例

某金融行业客户，通过日常设备巡检，发现防火墙的CPU性能消耗相比过往上涨了很多，整机加速会话SPU占比也有明显下降。经过排查，发现由于先前排查其他问题时新增的排查用配置没有及时删除，这就导致原本匹配后续策略的流量匹配上了这条临时策略，平白增加了CPU的消耗。最终删除了临时策略后，防火墙性能监控显示恢复了正常。

Summary

为了排查故障，通常会尝试新增测试配置或者启用一些诊断功能，部分操作需要注意及时还原。

```
config firewall policy
  edit 9999
    set uuid b6610544-ed18-51ec-f204-5f744a1e6ffb
    set srcintf "port1"
    set dstintf "port2"
    set srcaddr "OA_server"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set auto-asic-offload disable
    set comments "temp_for_troubleshooting"
  next
end
```

示例：为排错新增的临时策略

```
FGT #diagnose debug info
debug output:      enable
console timestamp:  enable
console no user log message:  disable
zebos debug level:  306783954 (0x124926d2)
ike debug level:    -1 (0xffffffff)
CLI debug level:    3
WAD console log:    enable

===== IPS debug settings =====

===== IPS SSL debug settings =====

===== IP router debug settings =====
...

Current debug duration is unlimited.
```

debug设置的状态，标红部分示例表示启用了部分设置



规范调试操作

最佳实践

每次做排错诊断是新增或者修改的配置，需要在排查完毕后及时还原，特别是像NPU加速关闭、临时防火墙策略等。

```
FGT # diagnose debug disable
FGT # diagnose debug reset
```

关闭并重置已经启用过的任意diagnose debug设置

```
FGT # show | grep -f auto-asic-offload
config firewall policy
  edit 9999
    set uuid b6610544-ed18-51ec-f204-5f744a1e6fffb
    set srcintf "port1"
    set dstintf "port2"
    set srcaddr "OA_server"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set auto-asic-offload disable <---
    set comments "temp_for_troubleshooting"
  next
end
```

grep工具可以快速筛选出包含特定字符串的配置





SNMP信息采集/ 远程服务器日志记录



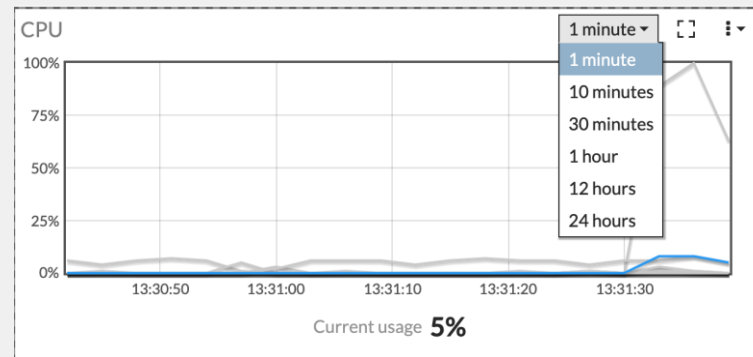
SNMP信息采集/远程服务器日志记录

案例

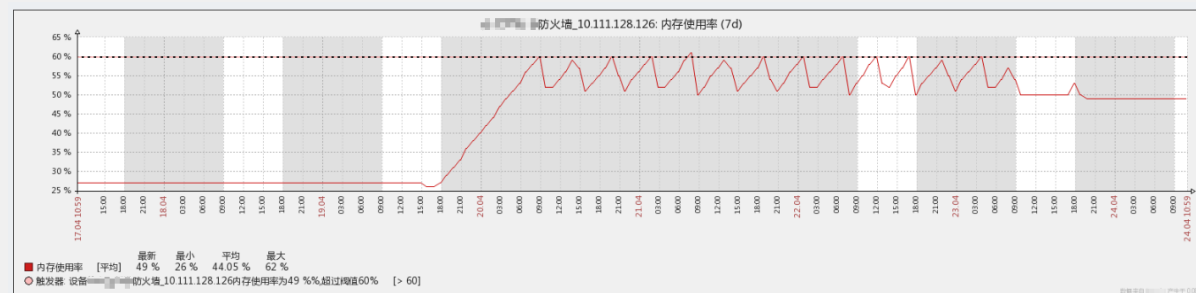
某企业客户，已使用FG超过5年，反馈在业务高峰时段，开始频繁发生流量中断的情况。后面通过SNMP监控发现，随着数年业务增长，防火墙CPU内存等对于新建会话进行安全检测的性能消耗也在缓慢上涨，直至承受不住，导致部分会话出现新建失败的情况。最终通过设备硬件升级替换更高性能的防火墙后，问题得到解决。

Summary

故障排查时，通常都需要回溯设备性能运行情况、系统事件状态变化或者个别功能告警情况等等，用以综合分析故障的根本原因和影响。



示例：FortiGate CPU性能微件覆盖时间范围最长24小时



示例：防火墙内存占用的SNMP平台监控

```
date=2021-04-30 time=16:46:51 logid="0100022012" type="event"
subtype="system" level="critical" vd="root" eventtime=1619790412368187095
tz="+0300" logdesc="Memory conserve mode exited" service="kernel"
conserve="exit" total="3962 MB" used="3157 MB" red="3487 MB" green="3249 MB" msg="Kernel exits memory conserve mode"

date=2021-04-30 time=16:45:01 logid="0100022011" type="event"
subtype="system" level="critical" vd="root" eventtime=1619790301771917456
tz="+0300" logdesc="Memory conserve mode entered" service="kernel"
conserve="on" total="3962 MB" used="3487 MB" red="3487 MB" green="3249 MB" msg="Kernel enters memory conserve mode"
```

示例：防火墙进入和退出保护模式的事件日志

SNMP信息采集/远程服务器日志记录

最佳实践

部署FAZ/SYSLOG服务器用来收集防火墙事件日志，部署SNMP服务器定期收集防火墙的CPU/内存/每秒并发会话/每秒新建会话/接口带宽统计等信息，并且记录SNMP trap。

对于SNMP建议采集的OID，可以参考[一本通手册](#)“系统管理->设备管理->SNMP”。

与第三方监控平台对接时，可以参考并使用设备自带的MIB库，例如和zabbix对接可以参考使用zabbix的FortiGate社区模板，示例可以参考[一本通手册](#)“系统管理->设备管理->SNMP”。

```
config system interface
    edit mgmt
        set allowaccess ping https ssh snmp
    next
end
config system snmp sysinfo
    set status enable
end
config system snmp community
    edit 1
        set name "fortinet"
        config hosts
            edit 1
                set ip 10.23.1.244 255.255.255.255
                set ha-direct enable
                set host-type query
            next
        end
    next
end
```

SNMPv2配置示例，通过HA预留网管接口与SNMP服务平台交互时，需要启用ha-direct

```
config log syslogd filter
    set filter-type include
    set filter "logid(40704,32042)"
end
```

可以按需对syslog发送的日志内容进行自定义过滤，可参考[KB](#)。





Comlog功能

案例

某企业客户，其中某一台办公网防火墙发生了一次异常重启，需要回溯故障原因，可惜没有开启comlog功能，开启后，直到下一次故障复现后，才通过comlog记录采集到了重启前的底层报错信息，最后反馈报错信息后，得到了软件修复。

Summary

设备异常重启或者无响应，需要分析根本原因，comlog可以记录设备启动后console所有的输出记录，因此comlog在这个场景通常都是值得参考的诊断信息。

[illegible]

comlog功能

最佳实践

对于支持comlog功能的FortiGate，请尽早启用该功能。

对于客户目前已有的FortiGate型号，comlog的支持情况如下：

平台	支持 comlog	平台	支持 comlog
FG201F	No	FG1000D	Yes
FG300D	Yes	FG1101E	Yes
FG600D	Yes	FG1500D	Yes
FG601E	No	FG1801F	Yes

```
FGT (global) # config sys console
FGT (console) # set output standard
FGT (console) # show
config system console
    set output standard
end

FGT (console) # end
```

读取comlog前，建议修改控制台输出模式，改成standard方式可以一次性输出完整comlog

```
FGT (global) # diagnose debug comlog enable
OK

FGT (global) # diagnose debug comlog info
control_byte = 3 (Logging enabled)
com_speed    = 0 (9600)
flash_size   = 0x00400000
log_start    = 0x001C5322
log_end      = 0x001C56DE
log_size     = 956
```

comlog功能启用方法以及配置状态查看方法





设备定时配置备份



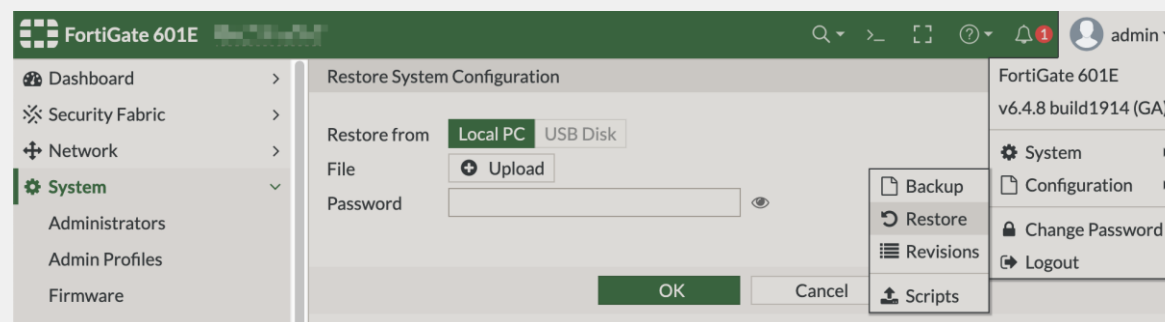
设备定时配置备份

案例

某企业客户，防火墙出现硬件故障无法启动，需要将备件恢复原有配置上线，但是没有近期的配置备份，所以最终只能重新配置上线，花费了更多的时间成本来恢复丢失的配置内容。

Summary

FortiGate防火墙配置由于意外或者故障导致配置丢失/缺失时，只能使用配置备份进行还原恢复。



设备定时配置备份

最佳实践

部署服务器，可以通过FMG/SCP/脚本工具等方式，定期下载防火墙配置备份。
(FortiManager也可以在每次配置变更时生成配置备份)

FortiGate支持多种配置备份方式：

- GUI下载
- CLI下载到内/外部设备，包括flash/ftp/sftp/tftp/usb等，还可以配合automation功能做定时执行 ([ref](#))
- REST API下载 ([ref](#))
- SCP下载 ([ref](#))

```
FGT # execute backup config
flash          <----- Backup config file to flash.
ftp            <----- Backup config file to FTP server.
management-station <----- Backup config file to management
station.
sftp           <----- Backup config file to SFTP
server.
tftp           <----- Backup config file to TFTP
server.
usb            <----- Backup config file to USB disk.
usb-mode       <----- Backup config file for USB mode.

FGT# execute backup config sftp <file name> <SFTP
server><:SFTP port> [user] [password]
```

SFTP supported from FortiOS 7.0.1

```
config system global
    set admin-scp enable
end
```

在FGT上启用SCP功能

```
Linux# scp admin@<FortiGate_IP>:sys_config <location>
```

在Linux终端上使用SCP下载FGT配置备份



FORTINET®