FORTINET

防火墙即服务用户指南

2025年7月

FY22Q1

1. 服务及license、设备注册激活
2. 设备及系统管理
3. 网络相关配置
4. VPN配置
5. 策略及安全控制
6. HA、VDOM等配置
7. 常用排错命令
8. Fortinet资源链接

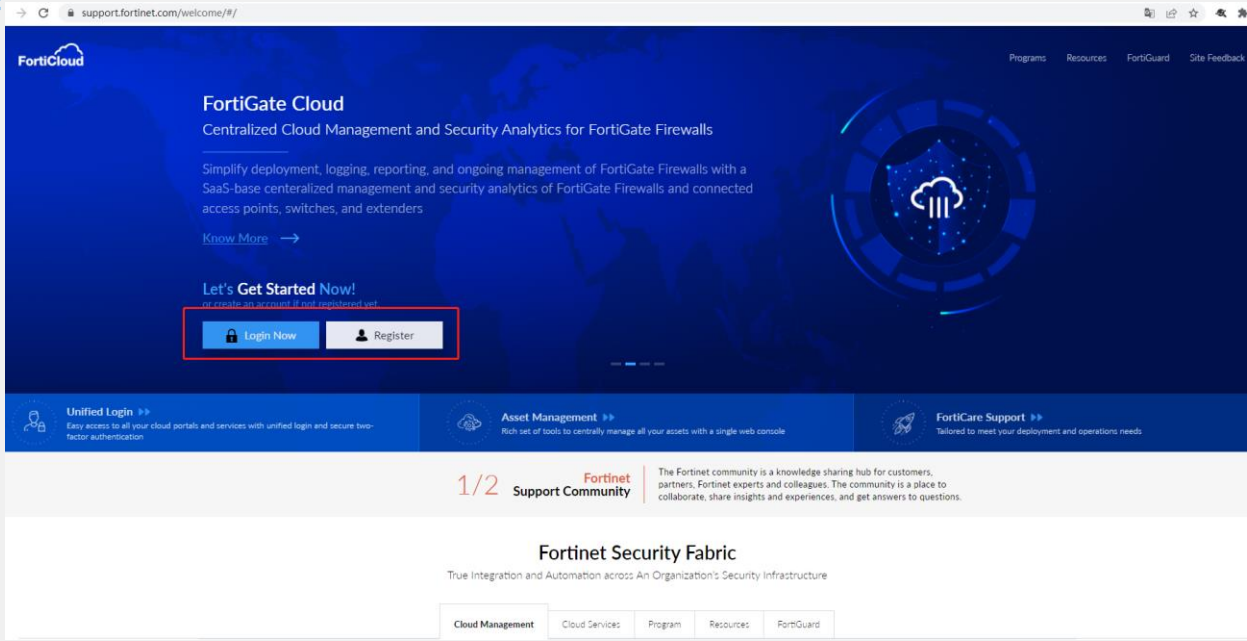
1、服务及license、设备注册激活

FortiGuard安全服务订阅

服务内容介绍			服务包种类			
类型	名称	内容简介	企业专业防护（EP）	统一威胁防护（UTP）	高级威胁防护（ATP）	基础保障服务（Premium）
FortiGuard	高级恶意软件防护服务 Advanced Malware Protection– AMP	防病毒 (Antivirus)：FortiGate 内置可实时更新的病毒特征库，通过扫描网络中的传输文件，防御最新的病毒、间谍软件和其他内容级的威胁。	✓	✓	✓	
		云沙盒 (FortiSandbox Cloud)：高级威胁防护解决方案，通过部署在云端的沙盒产品，实现对包括勒索软件在内的未知威胁进行识别后动态生成签名，并把签名下发到 FortiGate 进行阻挡。				
		僵尸网络防御 (Anti–botnet)：FortiGate 内置可实时更新的僵尸网络域名数据库和 IP 数据库，当匹配到数据库内的域名和 IP 流量时，进行实时阻挡。				
		移动设备安全 (Mobile Security)：防御包括 Android、iOS 等的移动平台的最新威胁。				
		病毒爆发防护 (Virus Outbreak Protection)：实时在线查询最新爆发的病毒，消除最新发生的病毒威胁与病毒特征库更新之间的缺口，检测和阻止在 FortiGate 病毒特征库更新之前发现的恶意软件威胁，防止威胁在网络系统中传播。				
		内容解除及重建 (Content Disarm & Reconstruction)：实时从文件中剥离所有活动内容，创建无害的文件。活动内容是文件中一种交互式或动态的内容，被视为可疑活动内容将被删除。				
	入侵防御系统 IPS	FortiGate 内置可实时更新的攻击防护特征库，以深度过滤的方式，打开数据包扫描其中的内容，查找已知的与签名匹配的漏洞，防御基于网络的威胁。	✓	✓	✓	
	Web过滤 web filter	实时扫描用户访问的 URL，并在 FortiGuard 上查询 URL 的网址分类。FortiGuard 对全球数以亿计的网址进行分类，管理员只需要对不同分类进行阻止或监视的操作，就可以阻止用户访问与企业无关的网站或对用户的网站访问行为进行记录。	✓	✓		
	垃圾邮件过滤 anti–spam	通过实时查询发件人的 IP 信誉数据库和垃圾邮件签名数据库，以及邮件中包含的钓鱼 URL，检测和阻止垃圾邮件信息。	✓	✓		
	安全评级 Security Rating	通过运行 Security Fabric 的安全审计，以可操作的配置建议和关键性能 / 风险指标的形式，帮助用户了解网络安全态势，指导用户设计、实现和持续维护适合其企业的安全架构。	✓			
	工业安全 Industrial Security	通过不断更新工业安全特征库，识别和监控大多数通用的 ICS/SCADA(监控和数据采集) 协议，以实现粒度可见性和控制。	✓			
	IoT检测服务 IoT Detection Service	FortiGate 在 FortiGuard 中检测本地设备数据库未检测到的未知设备。当服务激活时，FortiGate 可以向 FortiGuard 发送设备信息。当检测到一个新设备时，FortiGate 会查询 FortiGuard 查询的结果，以获取关于该设备的更多信息。	✓			
FortiCare	应用控制 Application control	FortiGate 内置的 4000+ 应用特征库，并分为 24 个分类。管理员可以快速创建允许、拒绝或限制对应用程序或应用程序分类的访问策略。	✓	✓	✓	✓
	Internet服务数据库 ISDB	数据库中收集了全球主要云服务、SaaS 服务的 IP 地址及服务类型。ISDB 可以在路由或防火墙策略中引用，快速实现 internet 服务的引流及访问控制。				
	IP声誉数据库 IP Reputation database	聚合来自 Fortinet、网络威胁联盟和其他全球资源的实时威胁数据。提供对恶意网络和僵尸网络攻击的保护，阻止来自已知受感染源的大规模 DDoS 攻击，以及来自代理的访问。通过全球地理 IP 库，还可以快速查找威胁的起源。				
	设备和操作系统检测 Device/OS Detection	通过多种条件，实现客户端设备和操作系统类型的检测，并在图形界面上进行展示				
	IP 地理服务 IP Geolocation Service	基于国家的 IP 地址库，用于 Fortinet 设备配置基于地理位置的策略地址对象。				
	IoT MAC地址库 IOT Mac Database	通过厂商 MAC 地址库，识别终端 IoT 设备类型				
	信任证书数据库 Trusted Certificate Database	内置的信任证书数据库，可以使 FortiGate 实现 SSL 流量检测时，识别服务器证书是否为安全的信任证书				
	动态DNS DDNS	基于云的动态 DNS 服务				
	硬件保修（Advanced HW） VM产品无此项服务	高级替换服务：硬件被 Fortinet 技术支持专家确认为无法远程解决需要将设备返厂维修的故障后，用户可以在发回设备前要求一台替换设备。我们将在 24 工作小时内将同型号或不低于原型号性能的替换机通过 Fortinet 付费的地面运输起运方式发送给客户。				
	固件升级服务 Firmware & General Update	Fortinet 将为注册的产品不断地发布软件的中间版本，以及维护版本和大的版本。所发布的版本将提供新特性，增强功能和补丁。				
	技术支持服务 Premium Support	Fortinet 通过邮件、电话、远程等多种方式响应客户的技术请求，定位设备故障，通过提供临时解决方案和补丁来修复系统，必要时候安排硬件替换。				

设备注册激活

设备注册需要创建一个fortinet账号，如下网址
https://support.fortinet.com



该账号可实现功能：

- ✓ 设备注册、服务激活
- ✓ 开Ticket （技术支持、硬件故障等case）
- ✓ FortiOS固件/FortiGuard服务包下载

建议是客户IT部门公共邮箱（邮箱一旦绑定，无法修改），根据提示一步步往下创建。

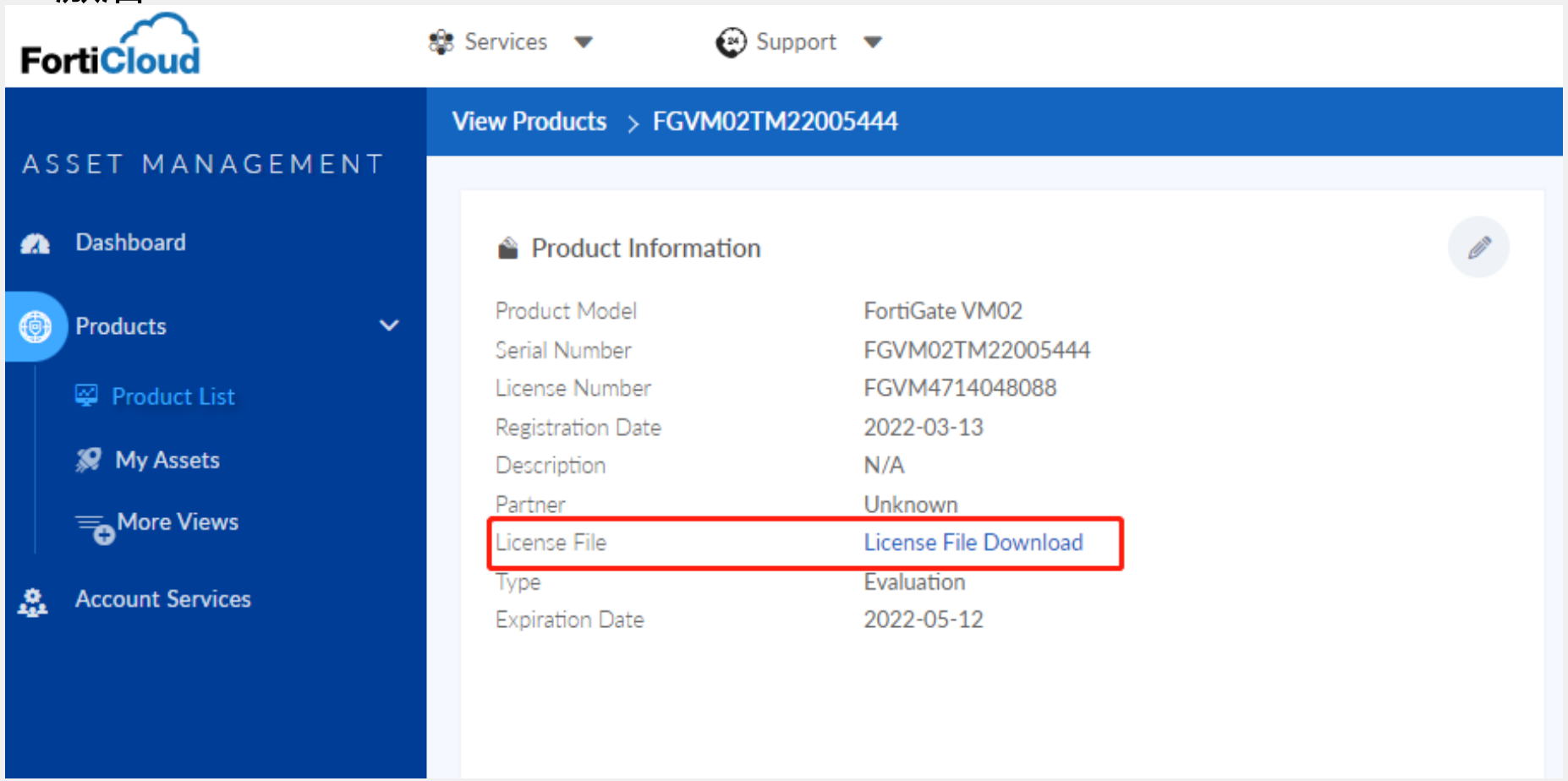
完成fortinet账号创建后，新设备主要操作有如下两步：

第一步：设备注册，即把设备绑定在该账号下，一个账号可绑定多台设备。

第二步，服务激活，服务序列号以PDF文件呈现（如未购买UTM服务，此步骤可忽略）

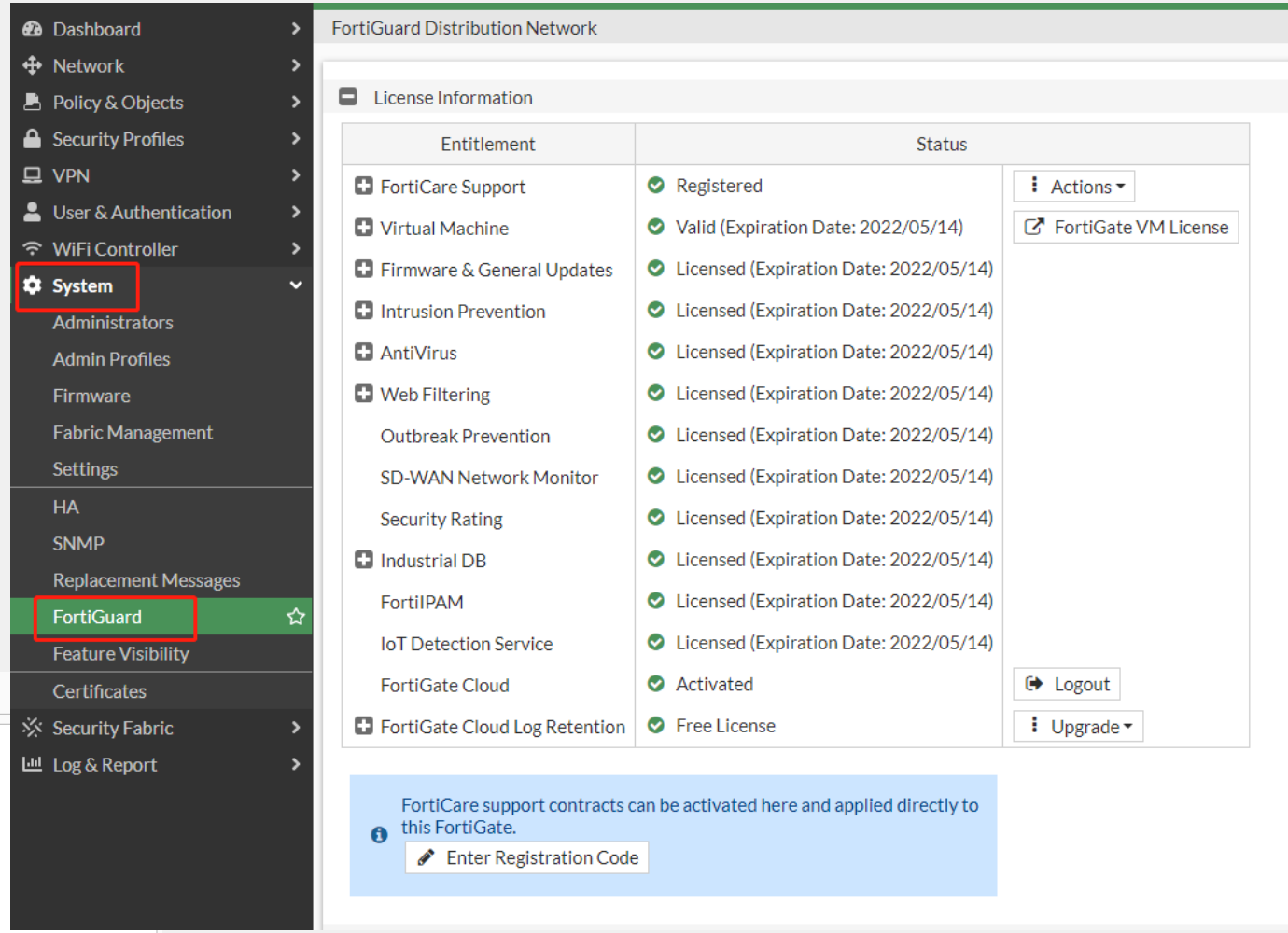
VM版license文件下载

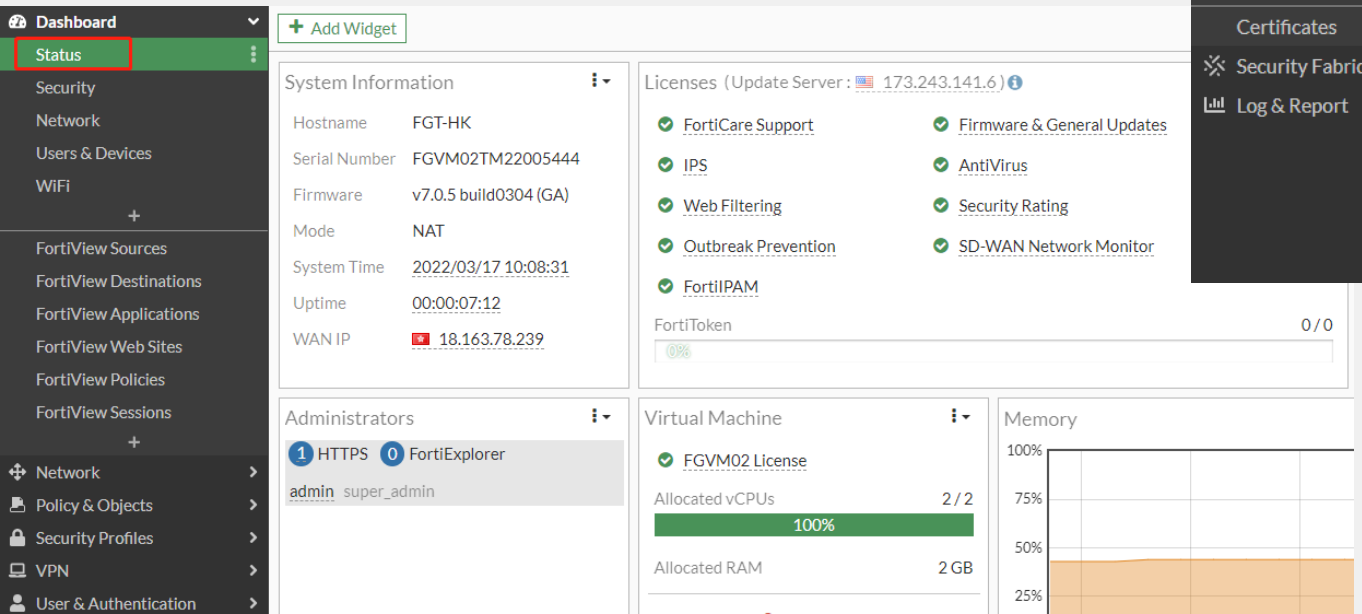
VM License注册完之后可以下载license文件，然后上传至FortiGate激活



查看设备license状态

可以在dashboard下status或者System/Fortiguard这里查看license状态





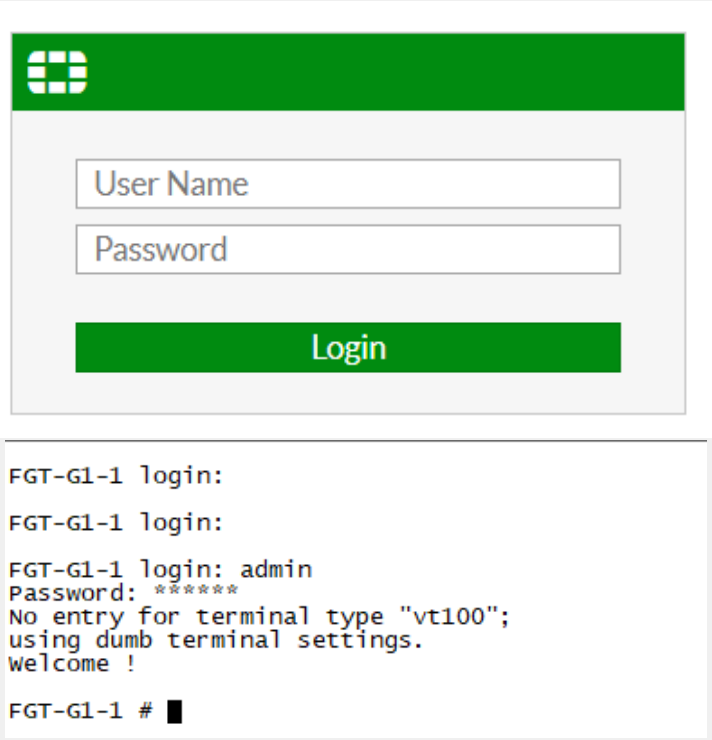
2、设备及系统管理

FortiGate登陆方式

FortiGate可以通过两种方式登陆管理：

1.WEB界面管理　2.命令行管理（包括Telnet、SSH、Console登陆）

- 低端设备
  a. 管理接口为LAN接口（port1？）；
  b. 默认管理IP：192.168.1.99/24，管理员admin，密码为空；
  c. Console波特率9600，其它管理协议：http/https/ssh/telnet/ping
- 中高端设备
  a. 有独立管理接口（MGMT1/MGMT2）；
  b. MGMT1默认管理IP：192.168.1.99/24，管理员admin，密码为空；
  c. MGMT2默认管理IP：192.168.2.99/24；
  d. Console波特率为9600，其它管理协议同上
- 虚拟化设备
  a. 默认PORT1接口IP为192.168.1.99/24，管理员admin，密码为空



若需要通过公网IP管理设备，80和443端口不通的情况下，可通过SSH或console修改https的管理端口为8443，修改之后需要在web地址栏加上端口号再访问 https://192.168.1.99:8443

```
config system global
set admin-sport 8443
end
```

恢复出厂

第一种方式：进入命令行，执行execute factoryrest命令，回车后会提示此操作将会恢复出厂配置，是否继续，输入字母"y"即可

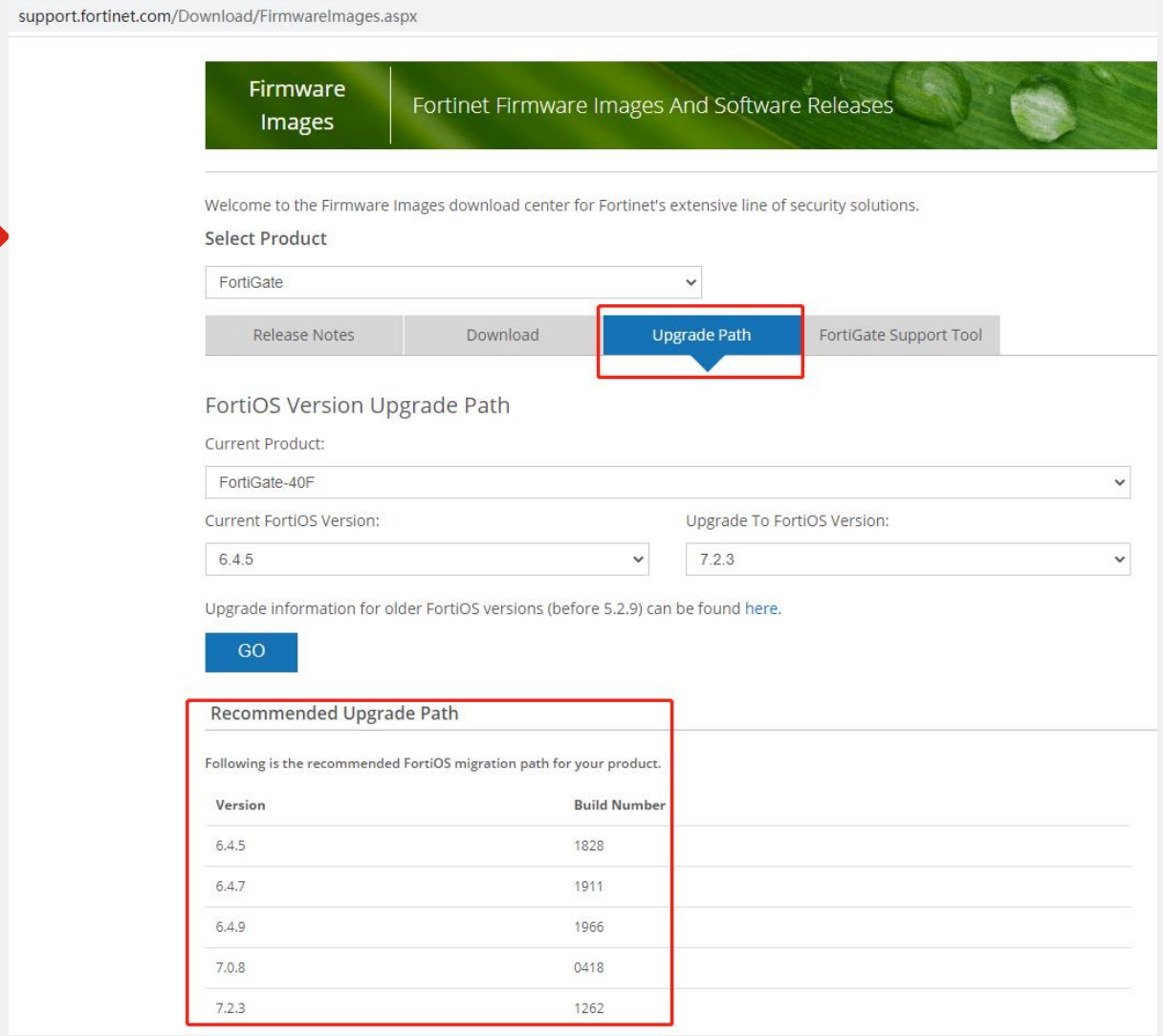
FortiGate # **execute factoryreset**
This operation will reset the system to factory default!
Do you want to continue? (y/n) **y**

第二种方式：通过设备上reset复位键（仅支持部分型号）：
reset键操作防火墙系统正常启动后（可以ping通或登录管理页面）30S内，长按10S左右，系统将自动重启，届时将恢复为出厂设置；

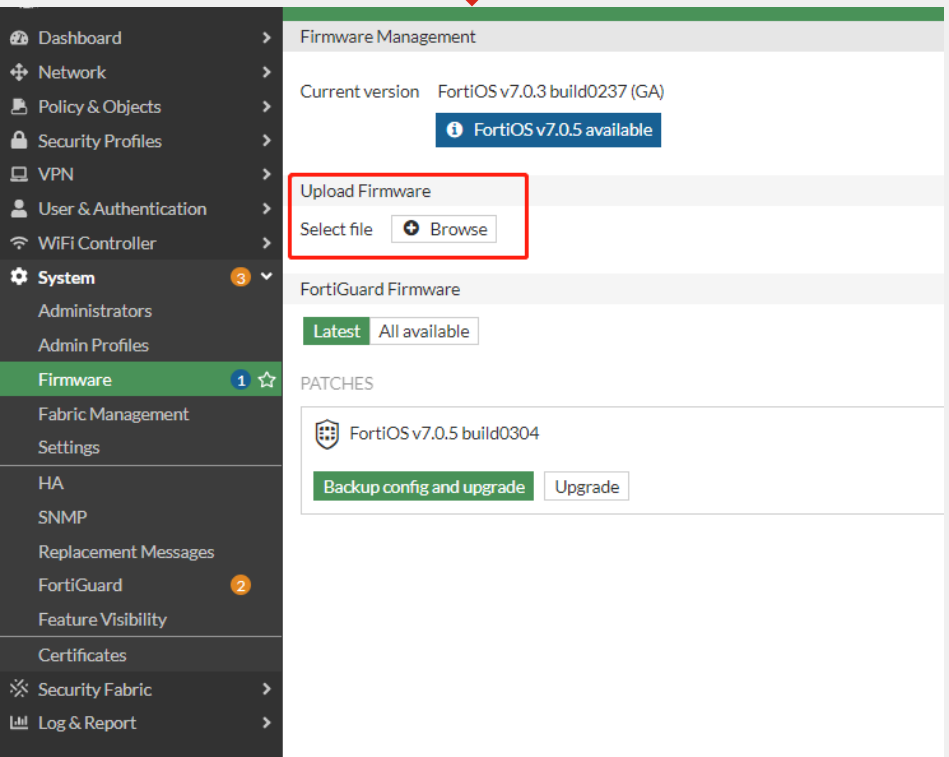
恢复出厂不清空硬盘日志，恢复出厂针对配置文件而言。

软件版本升级-web界面

升级之前需要先登陆到support.fortinet.com
查看升级路径，需要按步骤升级



可以在system/firmware这里手动上传镜像文件



软件版本升级-tftp方式

用console登陆设备
设备重启后按任意键打断
按C配置TFTP参数
TFTP Server和设备WAN或MGMT口（根据提示）ip可达
设置完成后按T开始连接TFTP并传文件

```
FortiGate-40F (18:55-07.27.2021)
Ver:05000021
Serial number: FGT40FTK2109ADL1
CPU: 1200MHz
Total RAM: 2 GB
Initializing boot device...
Initializing MAC... NP6XLITE#0
Please wait for OS to boot, or press any key to display configuration menu..

[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
[F]: Format boot device.
[I]: System information.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot.
[H]: Display this list of options.

Enter C,R,T,F,I,B,Q,or H:
```

```
[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
[F]: Format boot device.
[I]: System information.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot.
[H]: Display this list of options.

Enter C,R,T,F,I,B,Q,or H:

Please connect TFTP server to Ethernet port 'WAN'.

MAC: 94:ff:3c:03:9b:5e

Connect to tftp server 192.168.101.100 ...


#################################################################################################################
######################
Image Received.
Checking image... OK
This firmware image is certified!
Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?d

Programming the boot device now.The system must re-layout the boot device to install this firmware.
The default and backup firmware will be lost.
Continue:[Y/N]?
```

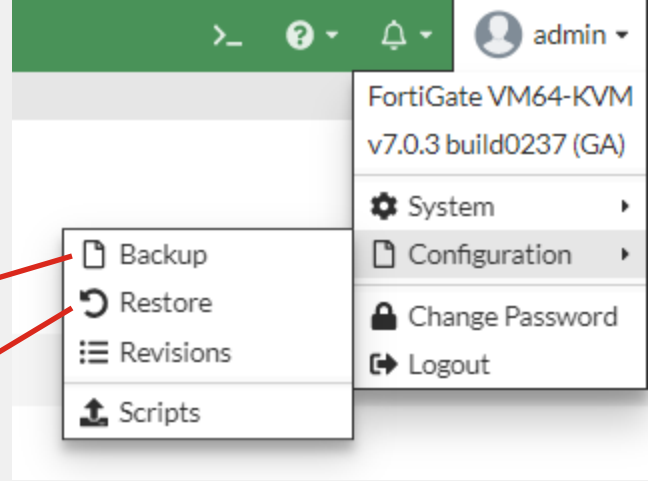
配置备份及恢复

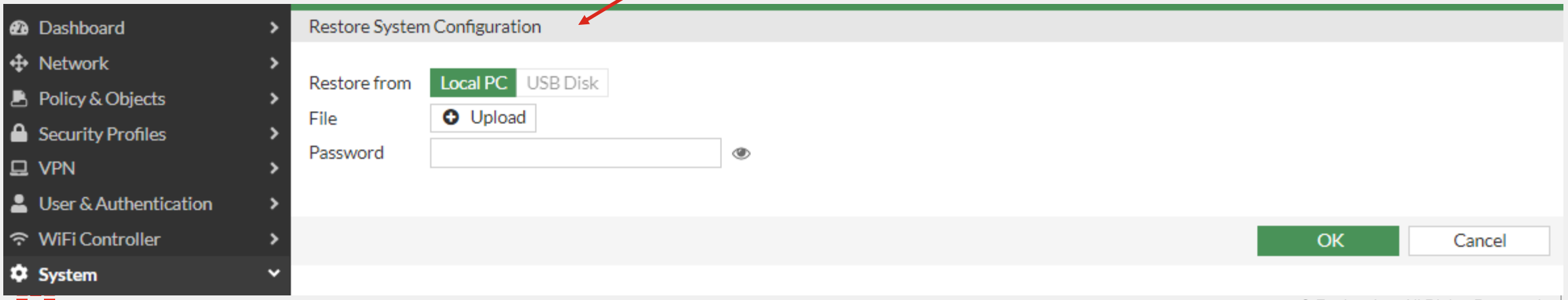
注意：

1、导入的配置文件必须是conf格式，否则无法识别。
2、导入配置后需要重启才会生效。
3、备份配置设置的密码必须谨记，如遗忘则无法导入恢复。
4、保存配置

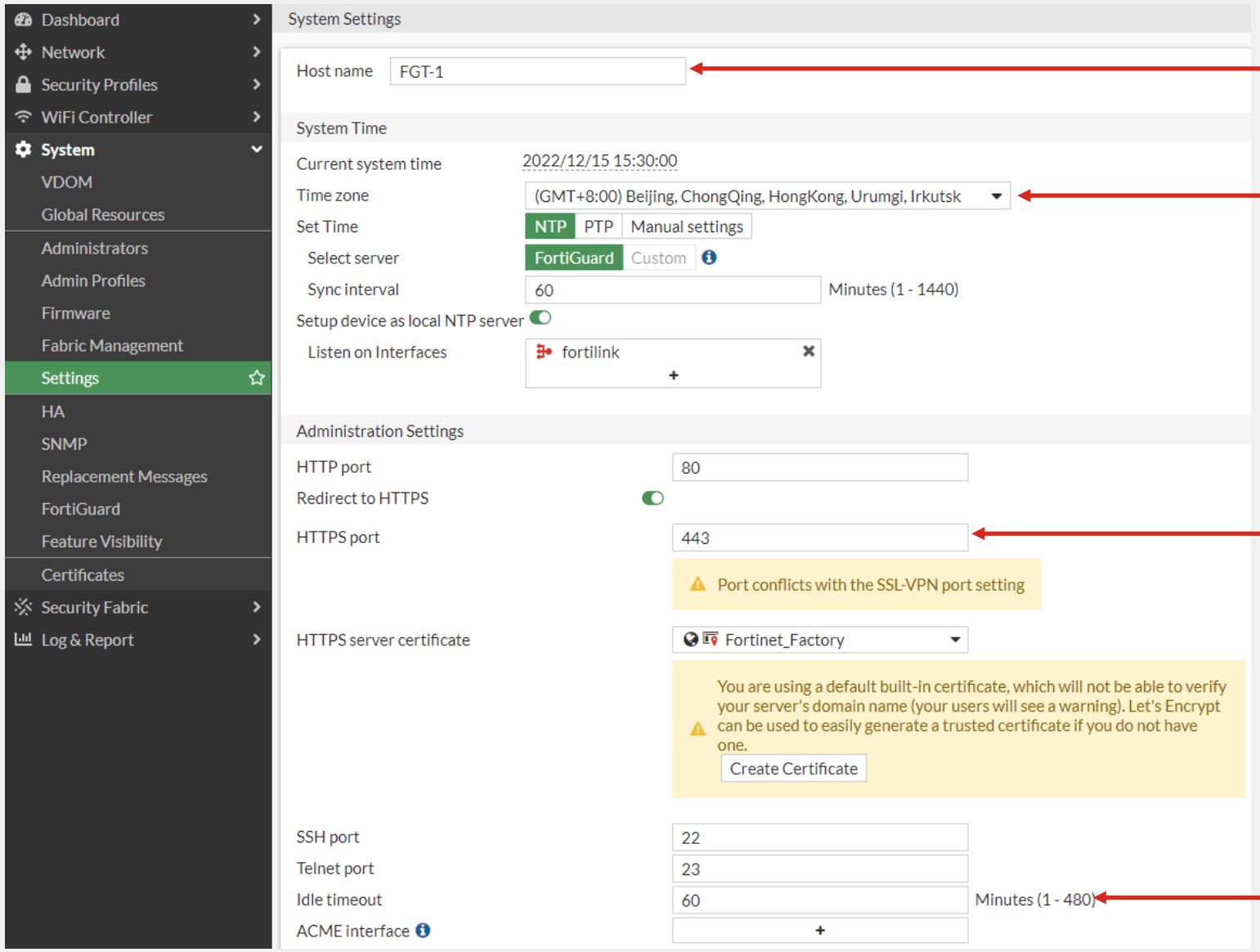
WEB：WEB上配置完，及时生效，且自动保存配置，无需手工保存。 每次修改配点击确认按钮后，配置自动保存。

CLI：命令行下 输入 next, end后配置生效自动保存。





系统基本设置



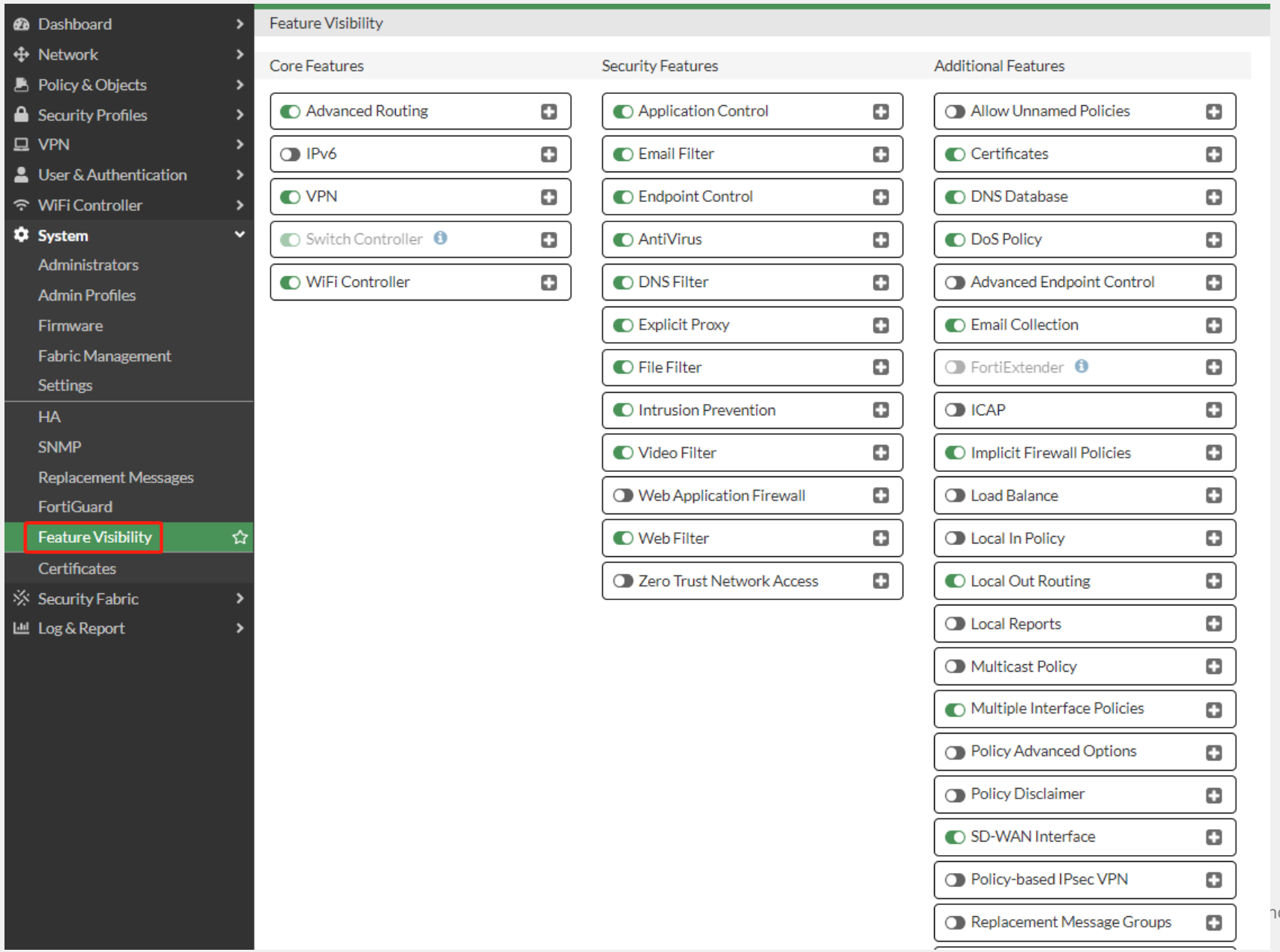
设置hostname

设置时区

设置HTTPS登陆端口

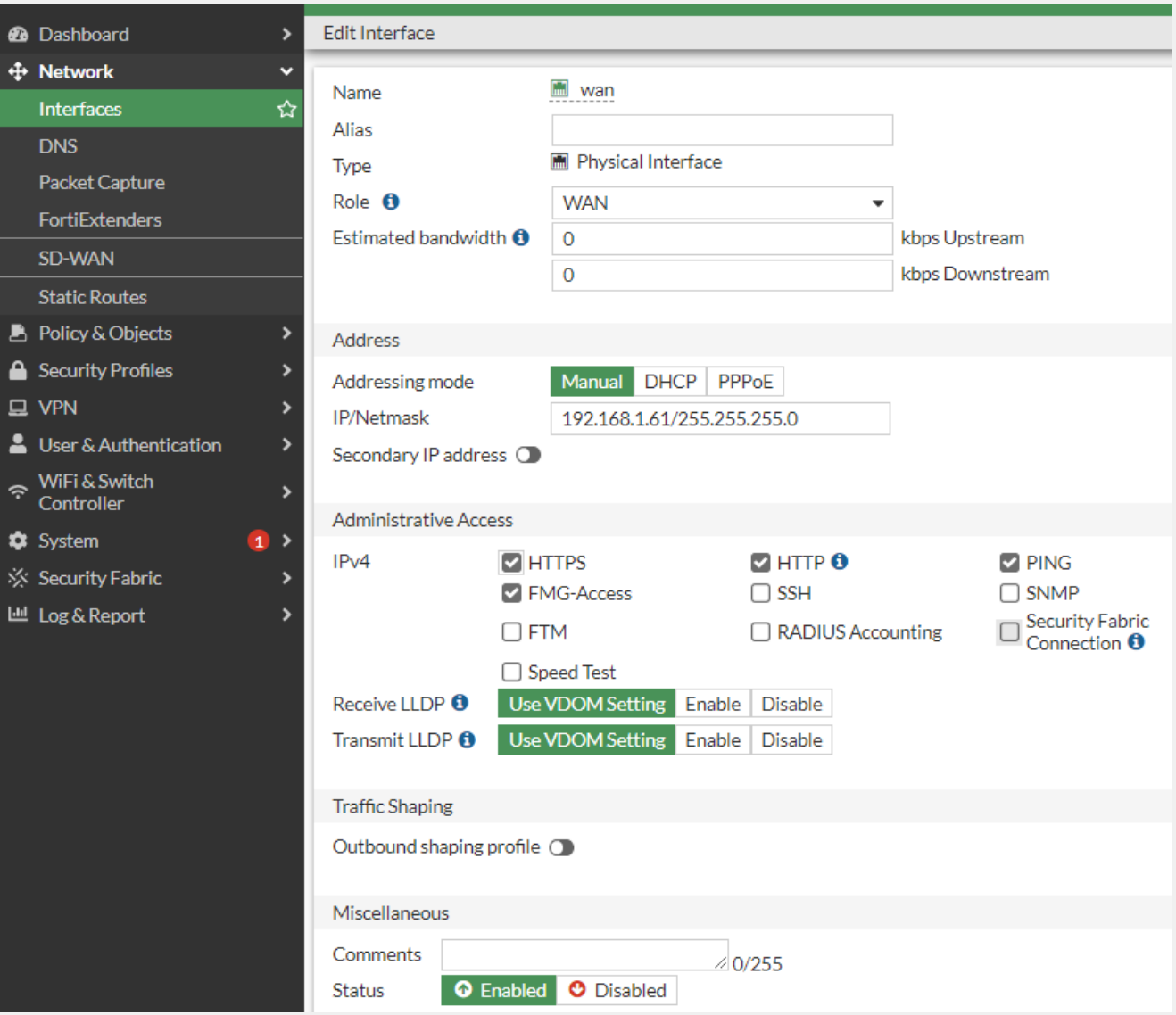
设置登陆空闲超时时间

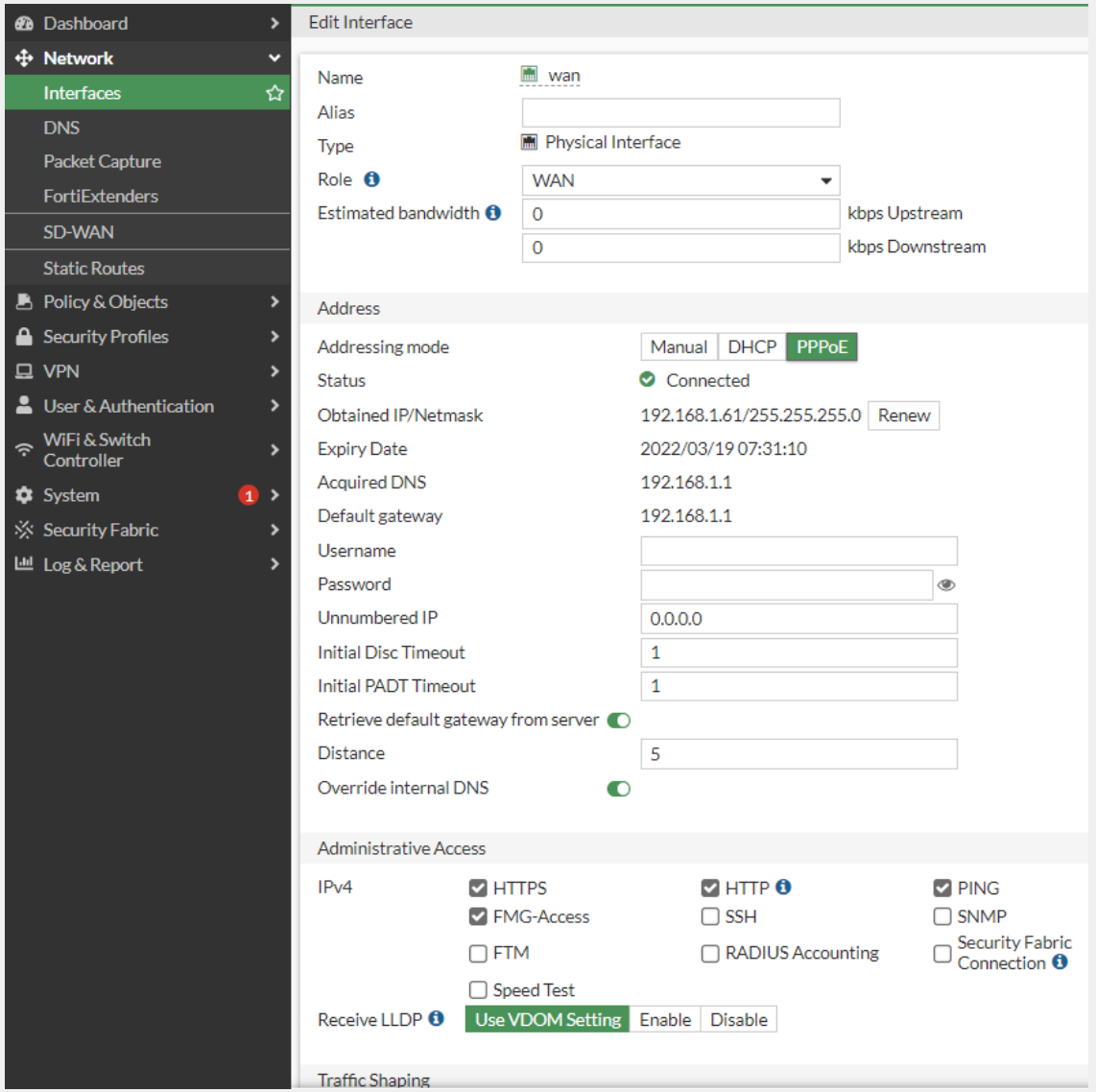
功能开启



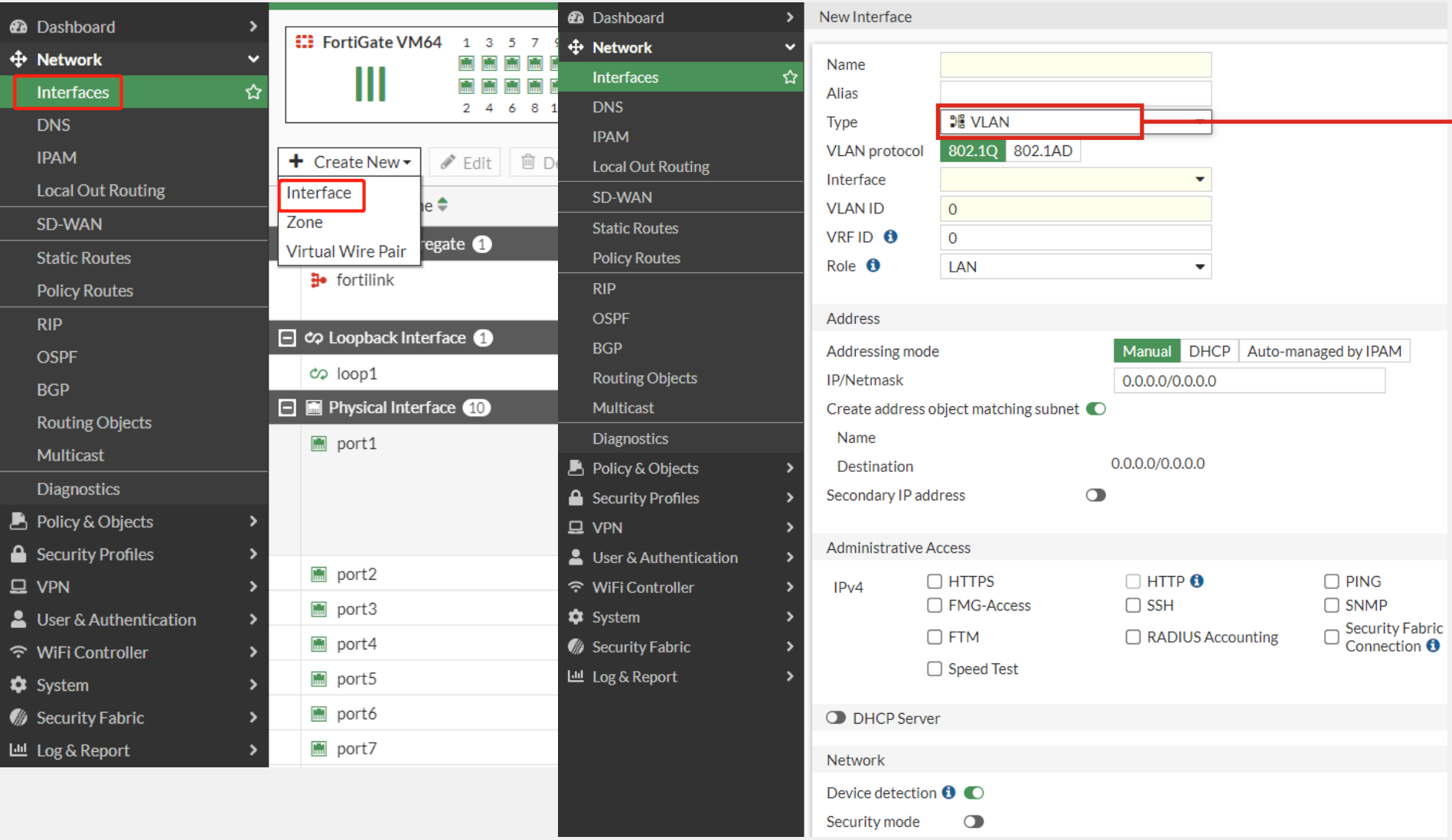
3、网络相关配置

接口配置

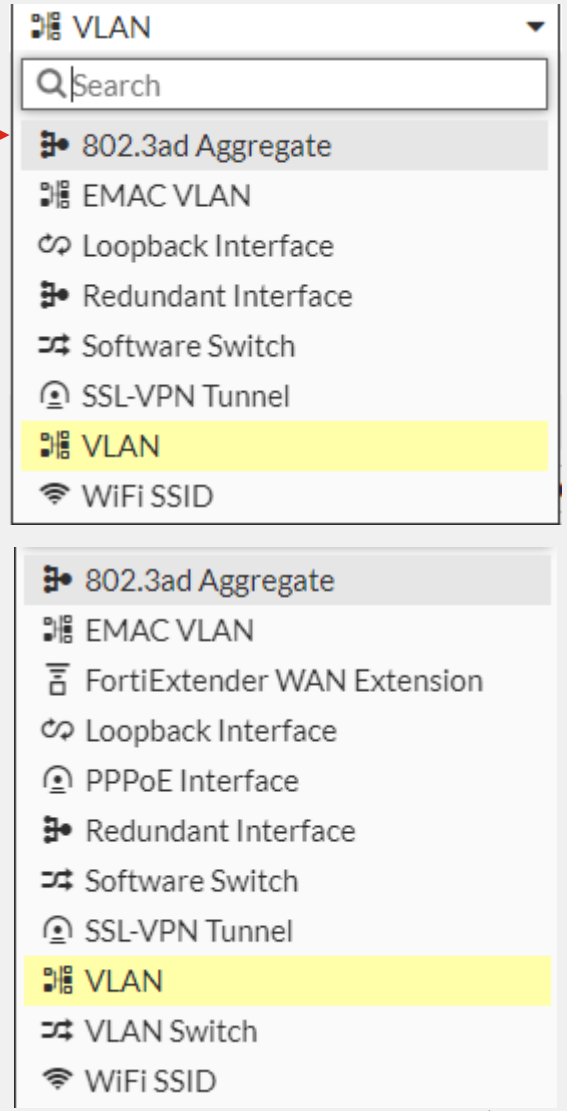




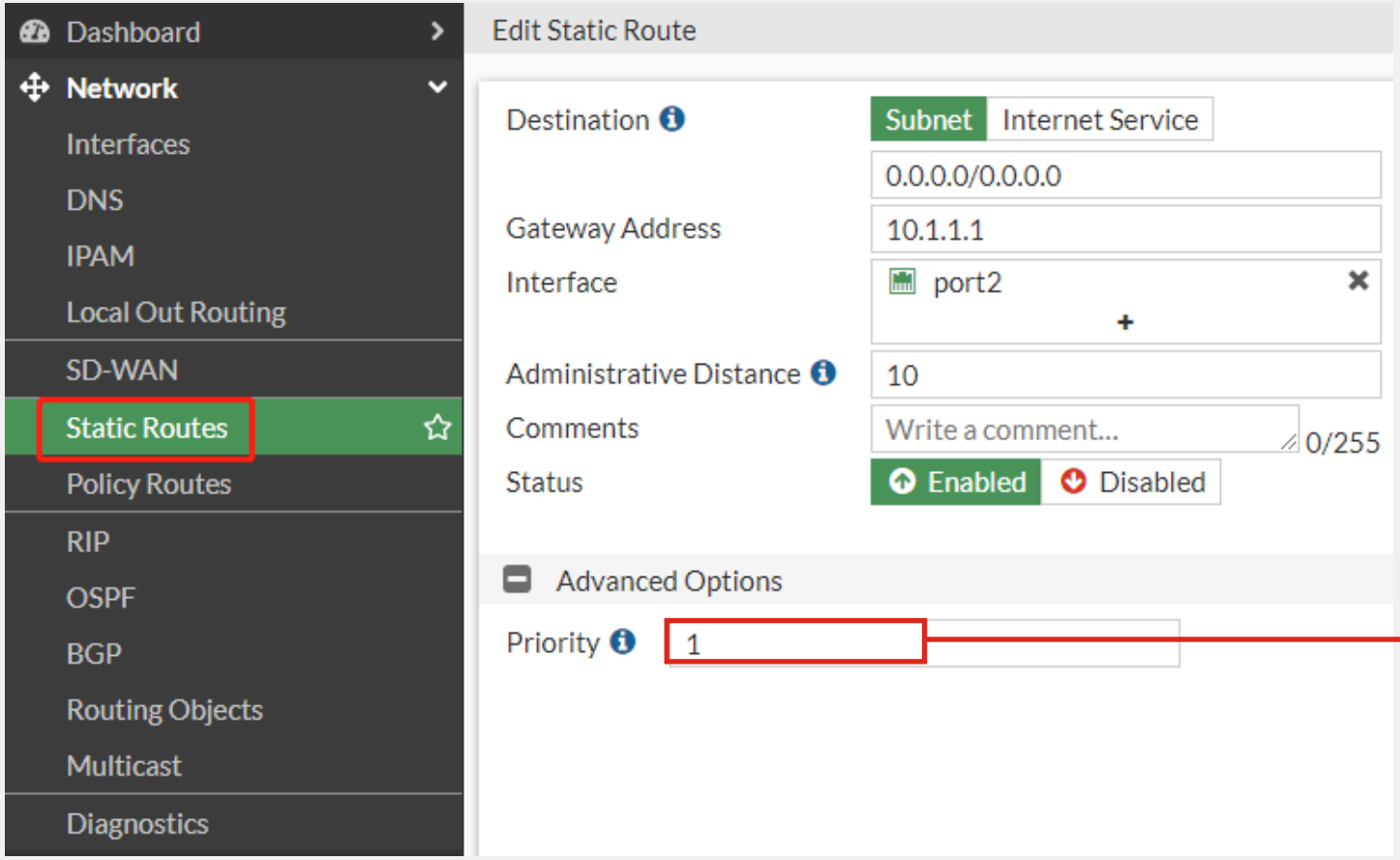
接口配置——创建接口



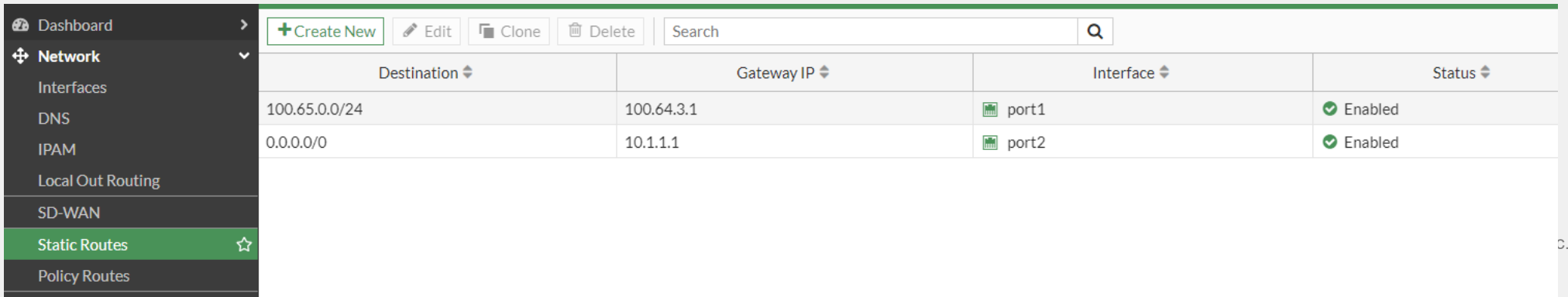
可创建接口的类型：



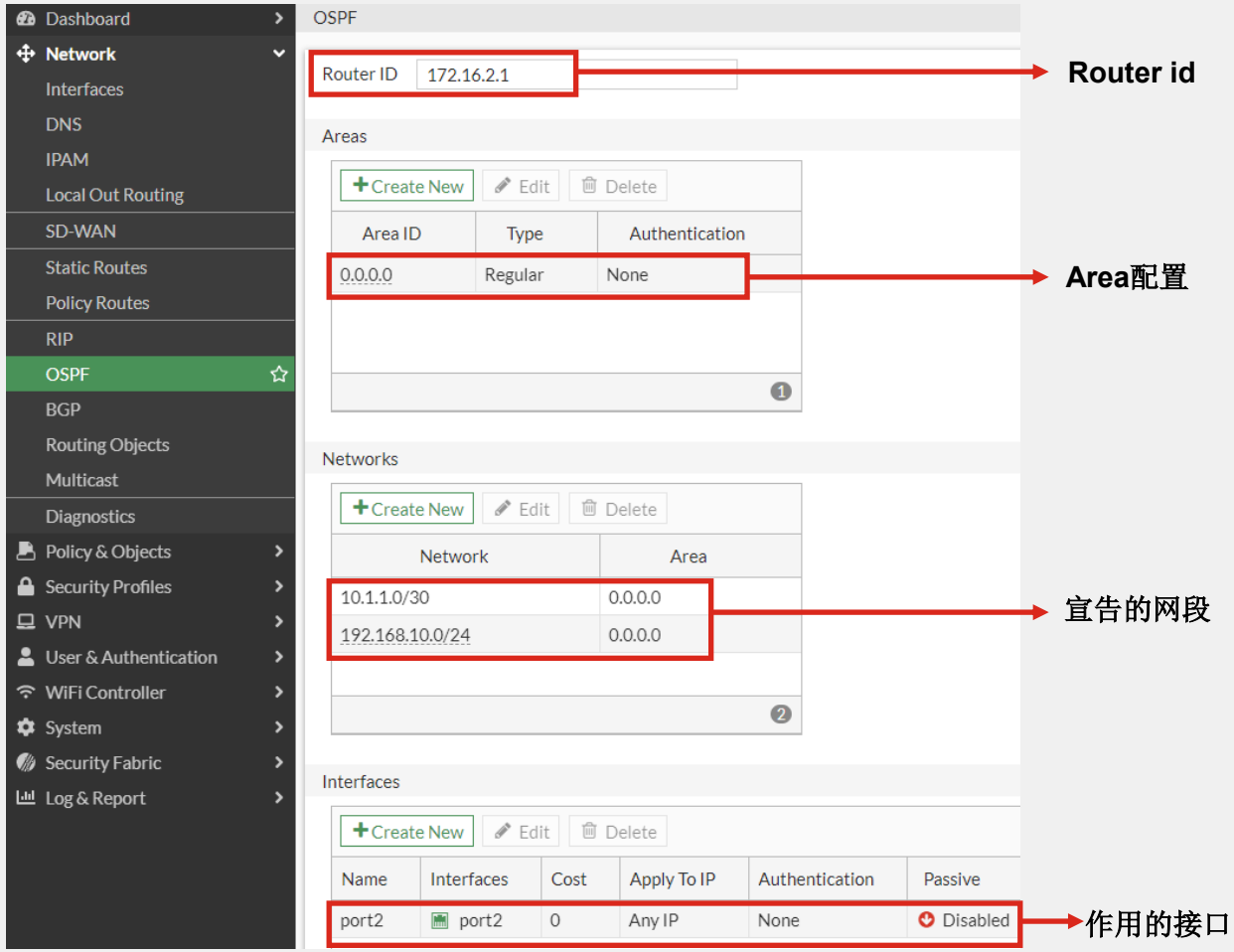
静态路由配置



优先级（值低的更优）



动态路由——ospf配置

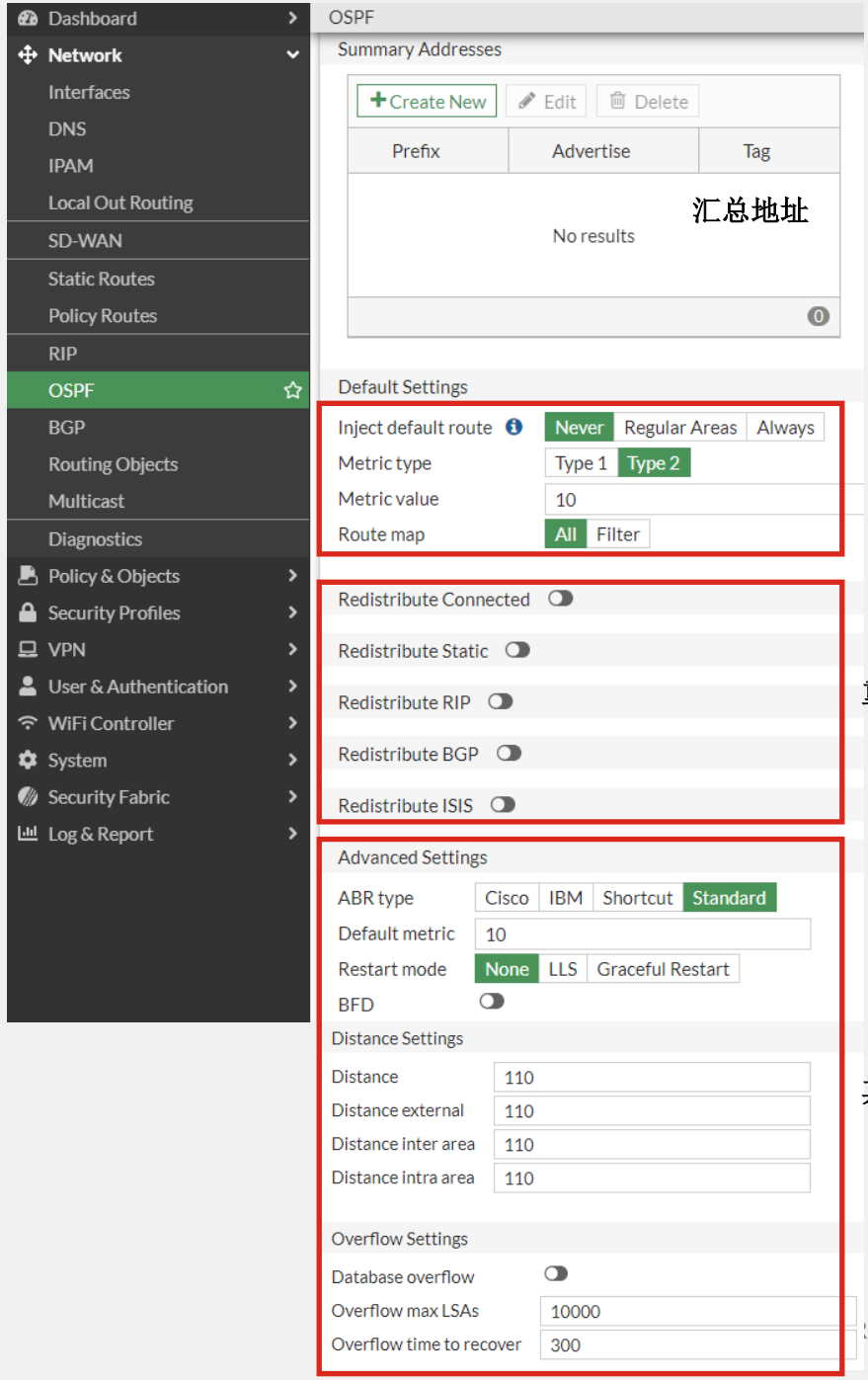


Router id

Area配置

宣告的网段

作用的接口

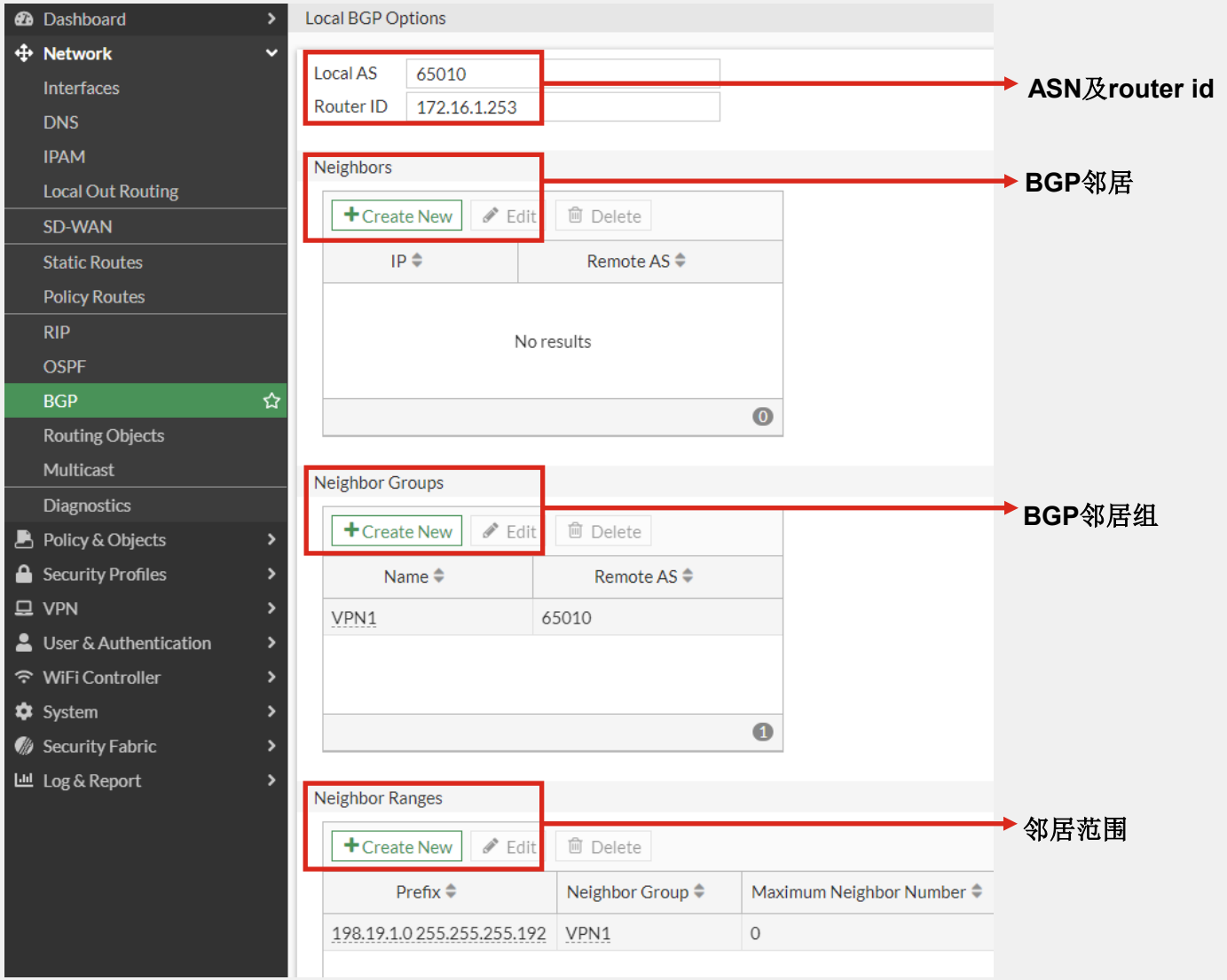


Metric、route-map等设置

重分布开关

其它设置

动态路由——BGP配置

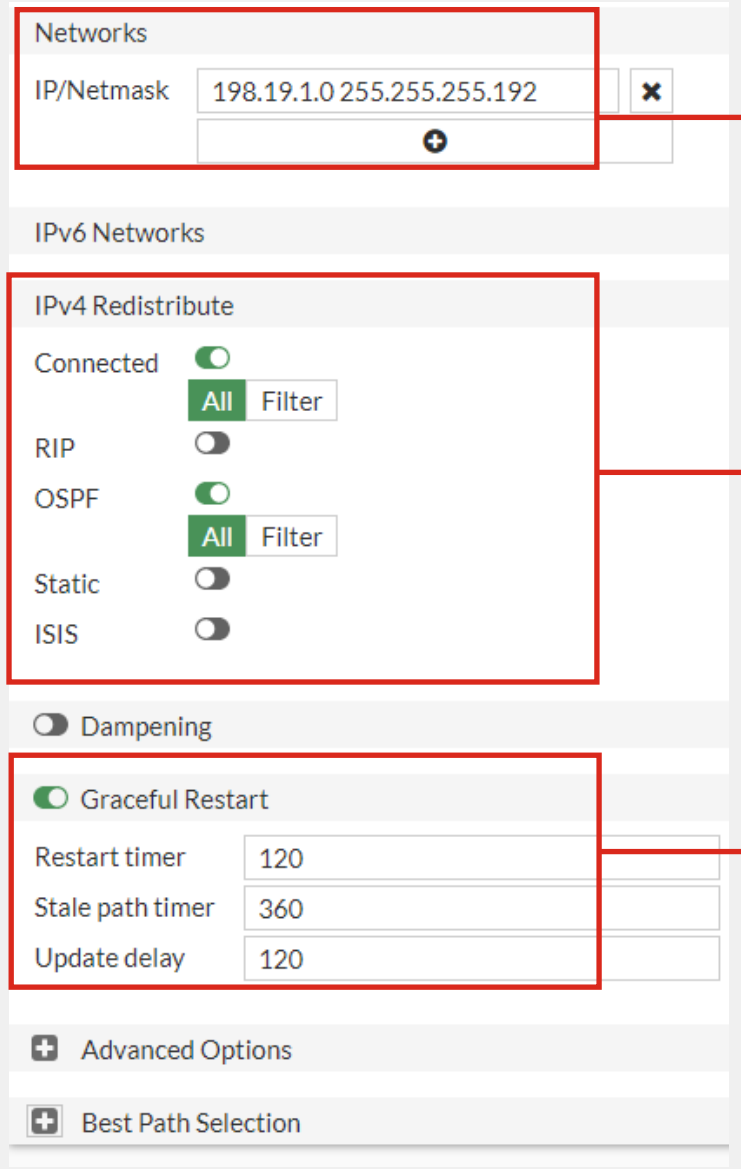


ASN及router id

BGP邻居

BGP邻居组

邻居范围

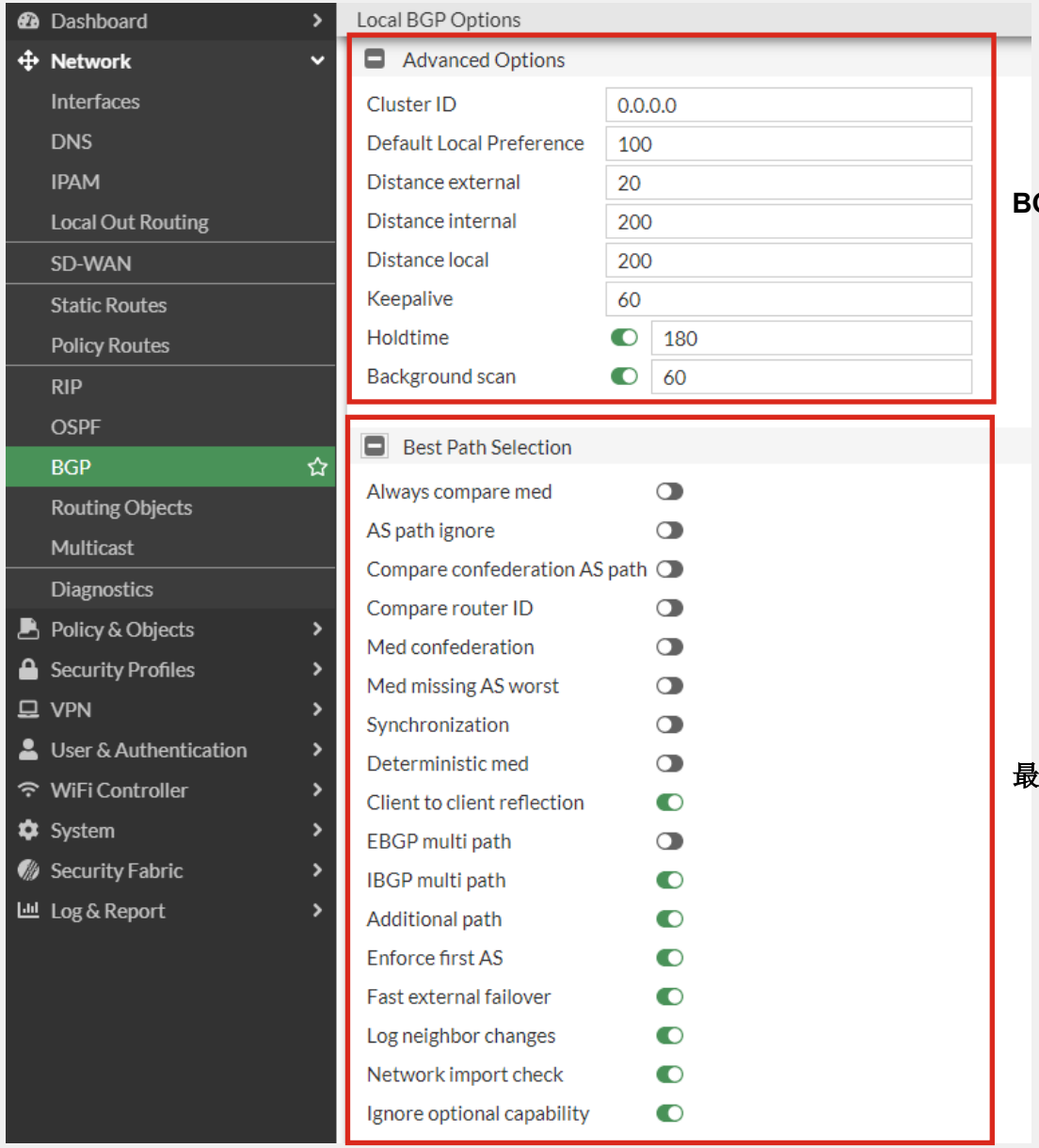


宣告网段

重分布设置

优雅重启，用FortiGate主备切换或设备重启时的路由保持

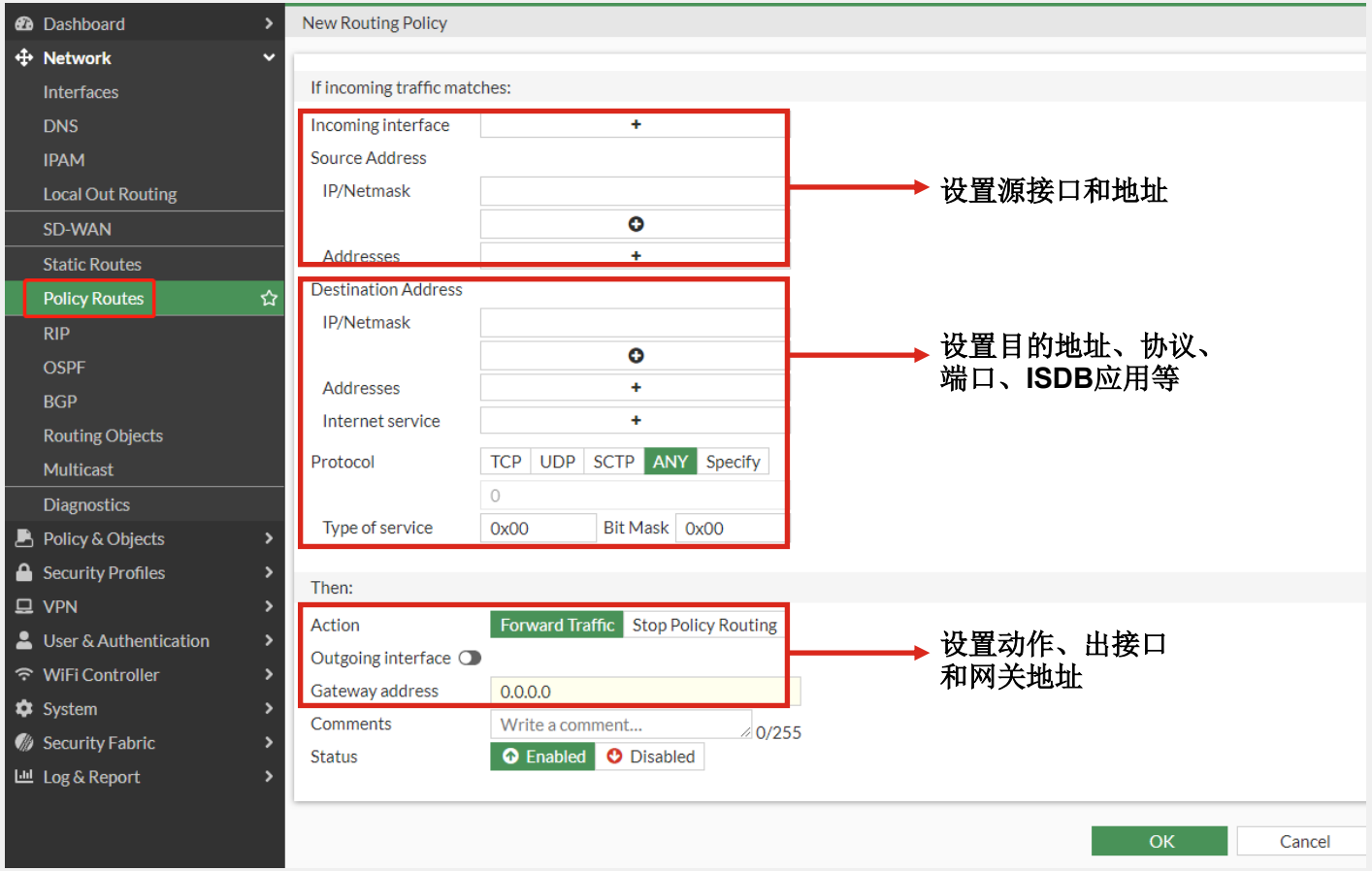
动态路由——BGP配置

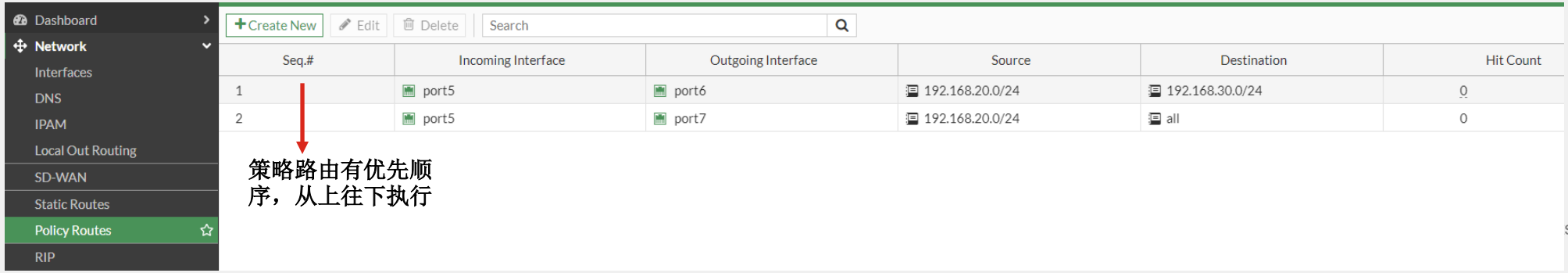


BGP高级设置

最佳路径设置

动态路由——策略路由





Link-monitor

在多条wan链路的情况下，建议设置link-monitor或者使用SD-WAN的SLA检测wan链路状态，确保在其中一条wan链路中断的情况下，让该链路的路由失效，使得流量路由至正常链路。

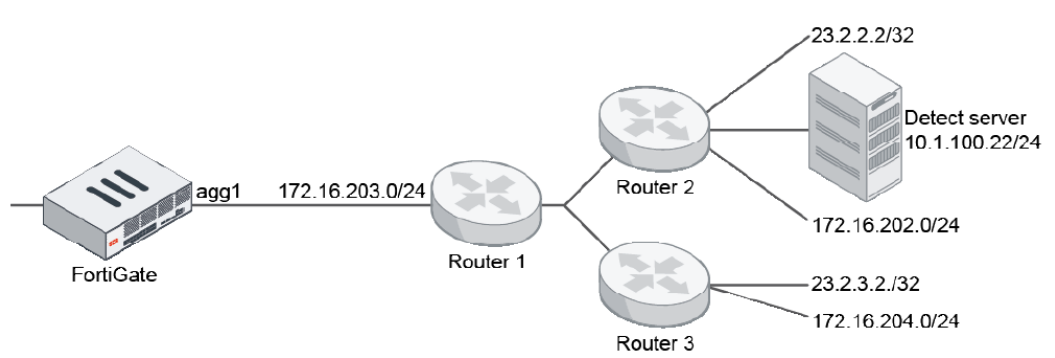
```
config system link-monitor
    edit "monitor1"
        set addr-mode ipv4
        set srcintf ''
        set server-config default
        set server-type static
        set protocol ping
        set gateway-ip 0.0.0.0
        set source-ip 0.0.0.0
        set interval 500
        set probe-timeout 500
        set failtime 5
        set recoverytime 5
        set probe-count 30
        set ha-priority 1
        set update-cascade-interface enable
        set update-static-route enable
        set update-policy-route enable
        set status enable
        set diffservcode 000000
        unset class-id
        set service-detection disable
    next
end
```

```
ping          PING link monitor.
tcp-echo      TCP echo link monitor.
udp-echo      UDP echo link monitor.
http          HTTP-GET link monitor.
twamp         TWAMP link monitor.
```

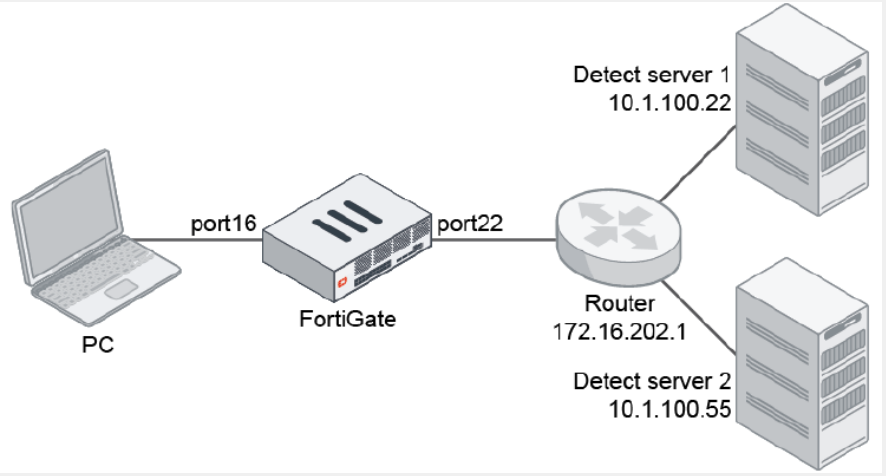
```
addr-mode                 Address mode (IPv4 or IPv6).
srcintf                   Interface that receives the traffic to be monitored.
server-config             Mode of server configuration.
server-type               Server type (static or dynamic).
*server                    IP address of the server(s) to be monitored.
protocol                  Protocols used to monitor the server.
gateway-ip                Gateway IP address used to probe the server.
route                     Subnet to monitor.
source-ip                 Source IP address used in packet to the server.
interval                  Detection interval in milliseconds (500 - 3600 * 1000 msec, default = 500).
probe-timeout             Time to wait before a probe packet is considered lost (500 - 5000 msec, default = 500).
failtime                  Number of retry attempts before the server is considered down (1 - 3600, default = 5).
recoverytime              Number of successful responses received before server is considered recovered (1 - 3600, default = 5).
probe-count               Number of most recent probes that should be used to calculate latency and jitter (5 - 30, default = 30).
ha-priority               HA election priority (1 - 50).
update-cascade-interface  Enable/disable update cascade interface.
update-static-route       Enable/disable updating the static route.
update-policy-route       Enable/disable updating the policy route.
status                    Enable/disable this link monitor.
diffservcode              Differentiated services code point (DSCP) in the IP header of the probe packet.
class-id                  Traffic class ID.
service-detection         Only use monitor to read quality values. If enabled, static routes and cascade interfaces will not be updated.
```

Link-monitor

可以通过Link-monitor影响静态路由和策略路由，可以设置多个检测的目标服务器，给每个检测目标设置权重，达到权重阈值后触发link-monitor dead



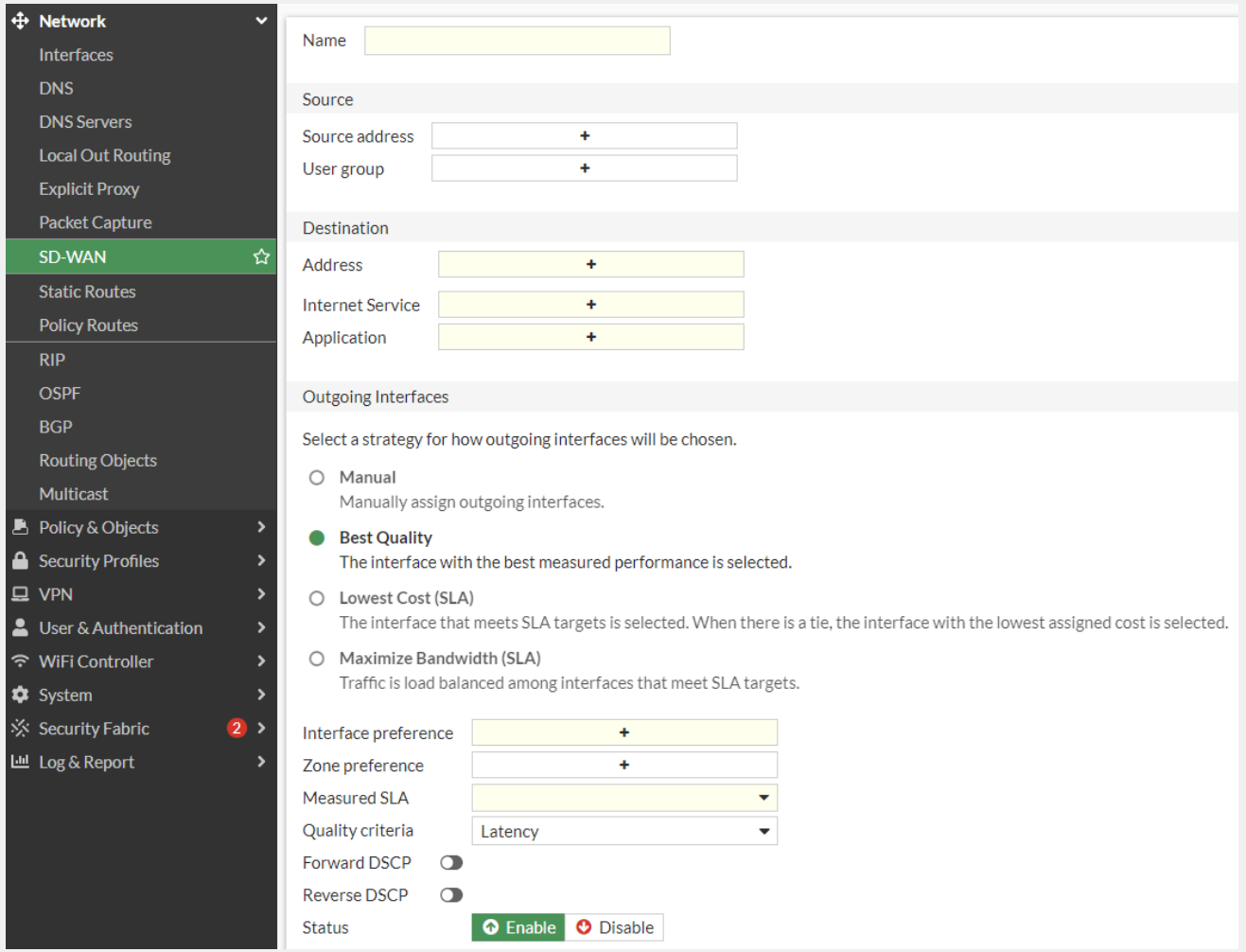

```
config system link-monitor
    edit "22"
        set srcintf "agg1"
        set server "10.1.100.22"
        set gateway-ip 172.16.203.2
        set route "23.2.2.2/32" "172.16.202.0/24"
    next
end
```




```
config system link-monitor
    edit "test-1"
        set srcintf "port22"
        set server-config individual
        set gateway-ip 172.16.202.1
        set failtime 3
        set fail-weight 40
        config server-list
            edit 1
                set dst "10.1.100.22"
                set weight 60
            next
            edit 2
                set dst "10.1.100.55"
                set weight 30
            next
        end
    next
end
```

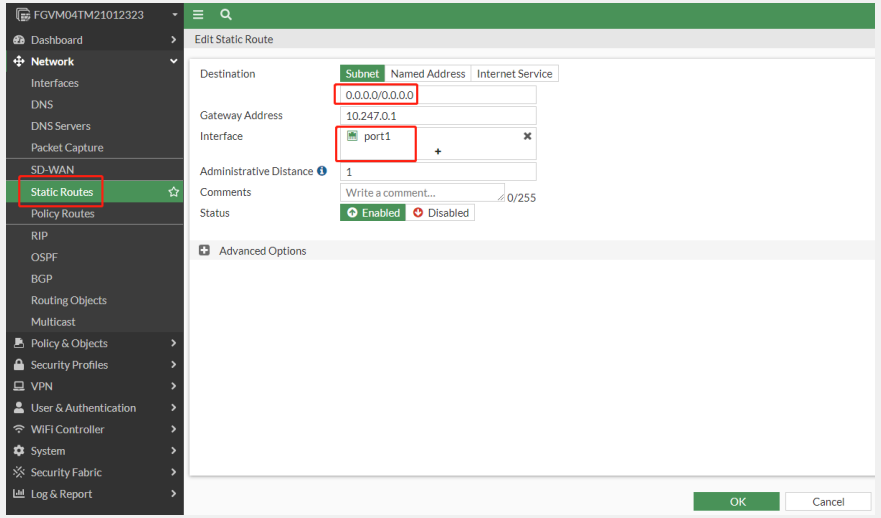
SD-WAN

- **地址对象：**ip subnet、ip range、FQDN、地理位置、dynamic（fabric connector自动同步）、MAC地址；
- **SD-WAN应用识别：**Internet Service库（4层）和APP库（7层）共4000+应用；
- **SD-WAN选路：**手动、最佳质量、最低cost、最大带宽四种选路方式，结合SLA、线路带宽、DSCP Tag以及各参数权重（延迟、丢包、抖动、带宽等），实现各种所需的动态选路；
- **SD-WAN链路检测：**可通过ping、http、dns等协议探测链路质量及服务器响应情况，配合SD-WAN动态选路
- **SD-WAN链路优化：**FEC前向纠错、包复制
- 控制器：FortiManager（option）
- 零接触部署

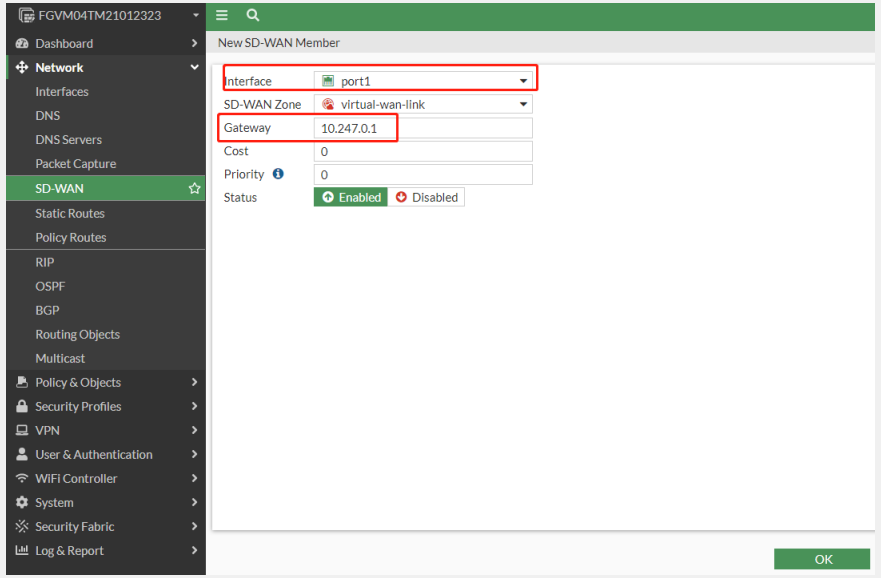


SD-WAN配置

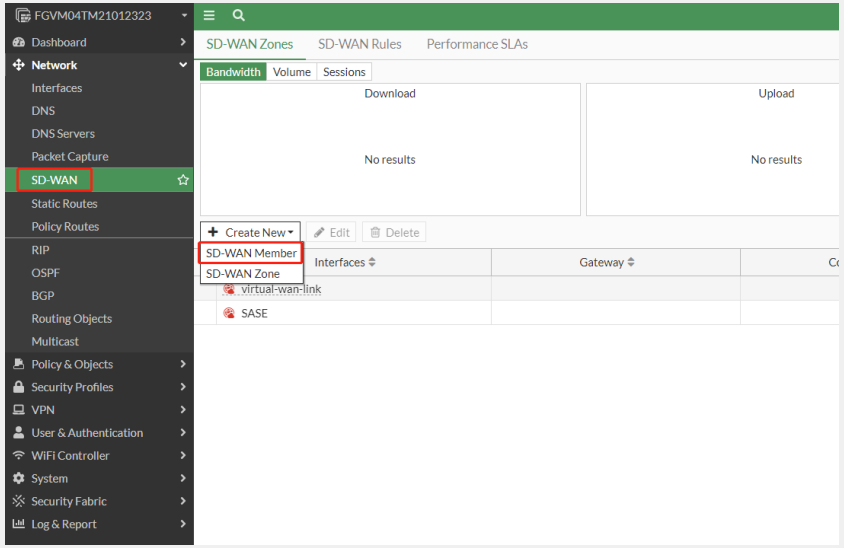
设置一条默认路由，执行port1所在网关



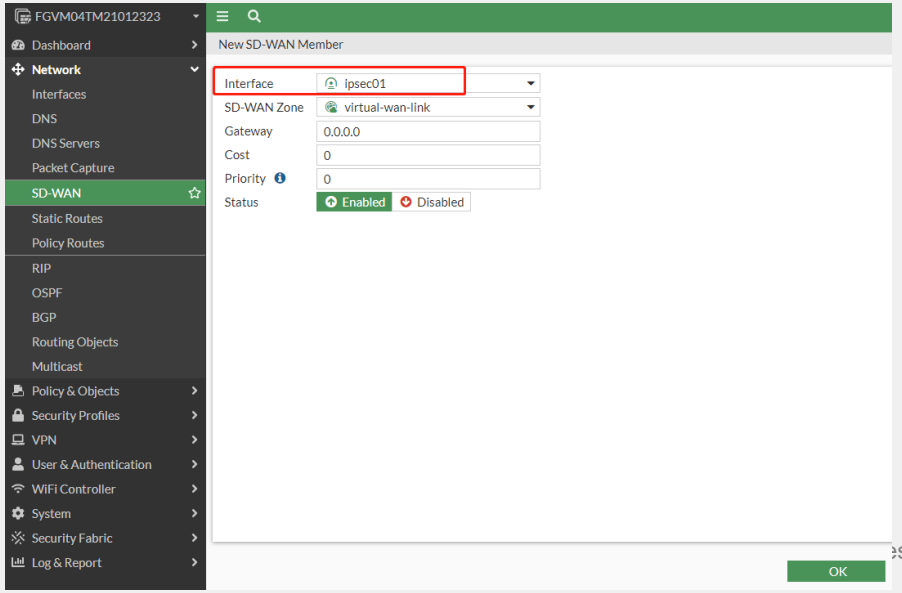
创建sdwan接口成员：port1



创建sdwan接口成员

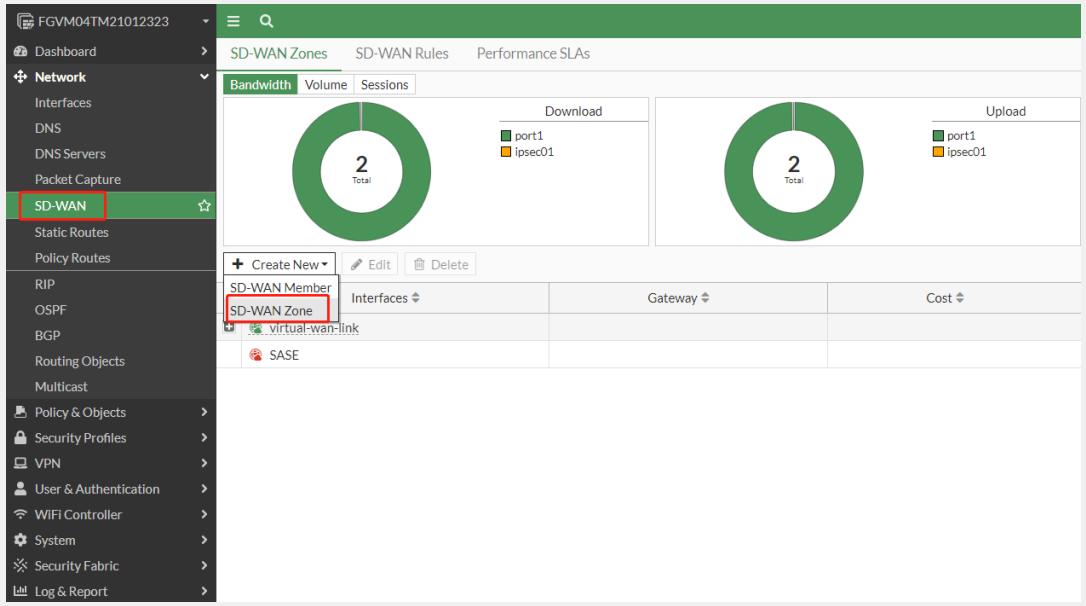


创建sdwan接口成员：ipsec vpn

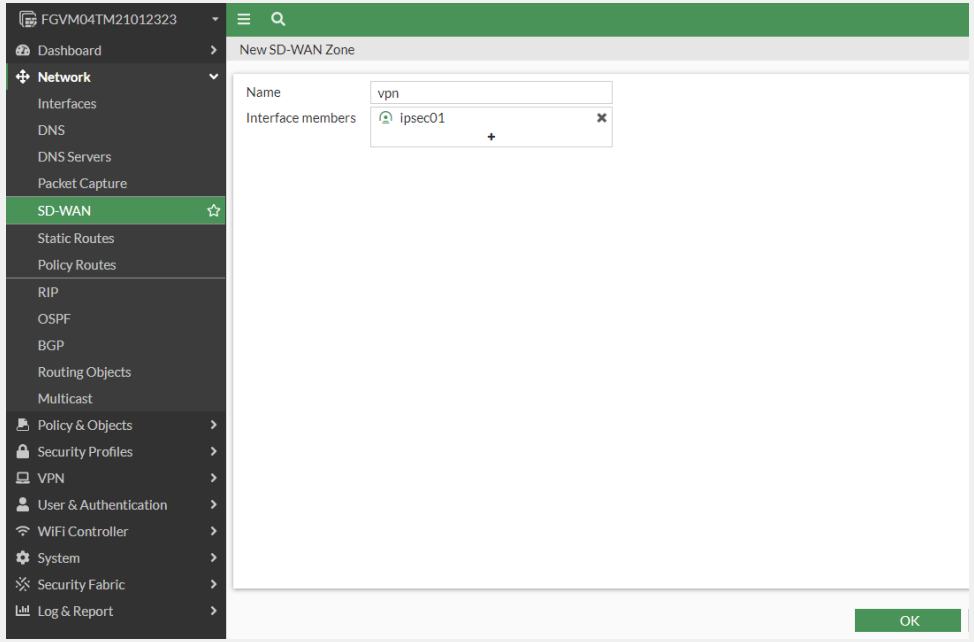


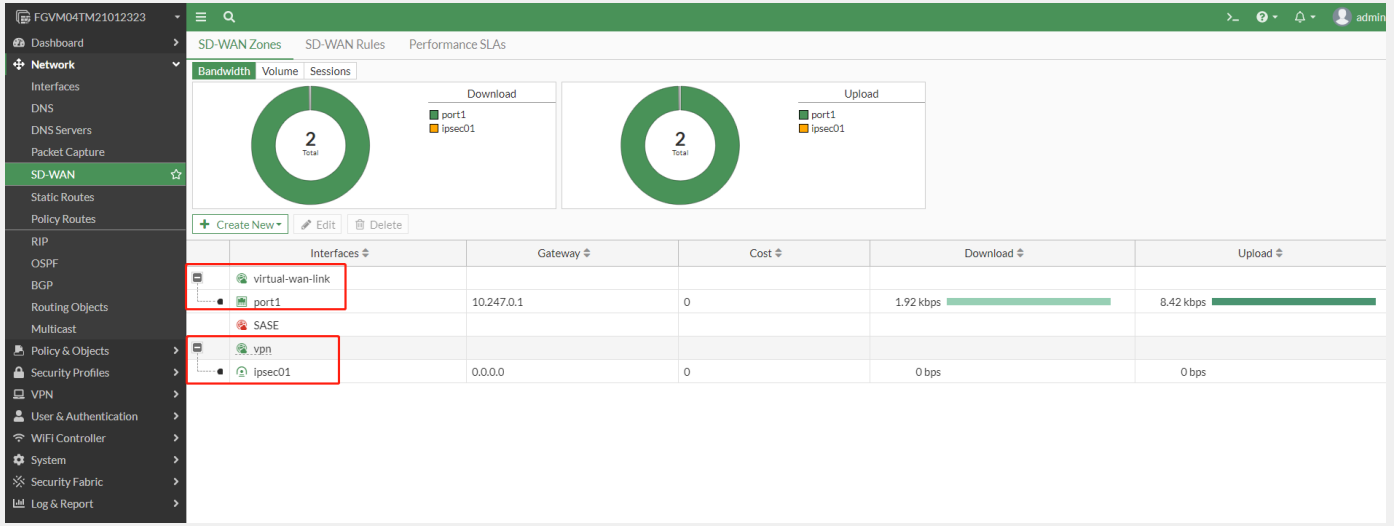
SD-WAN配置

创建sdwan zone



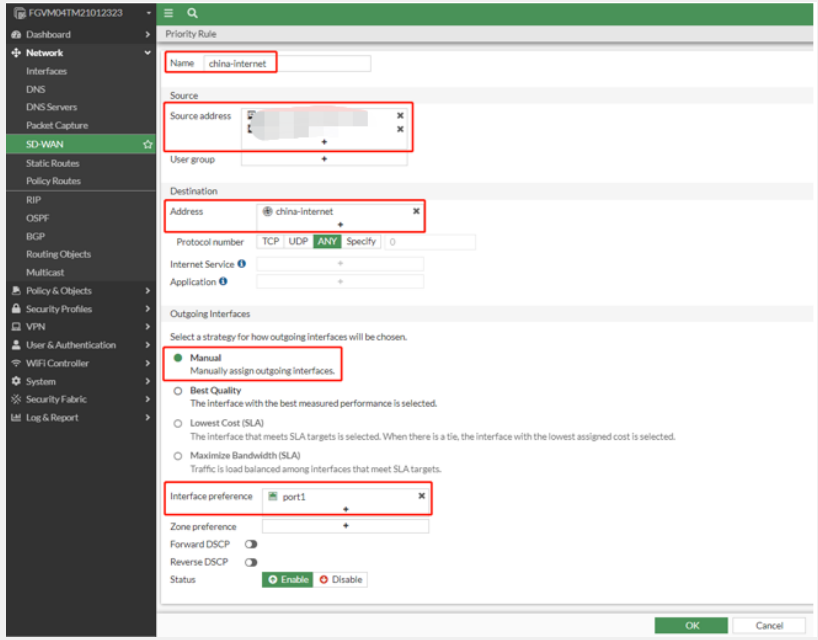
创建sdwan zone：vpn，并选择ipsec vpn作为接口成员



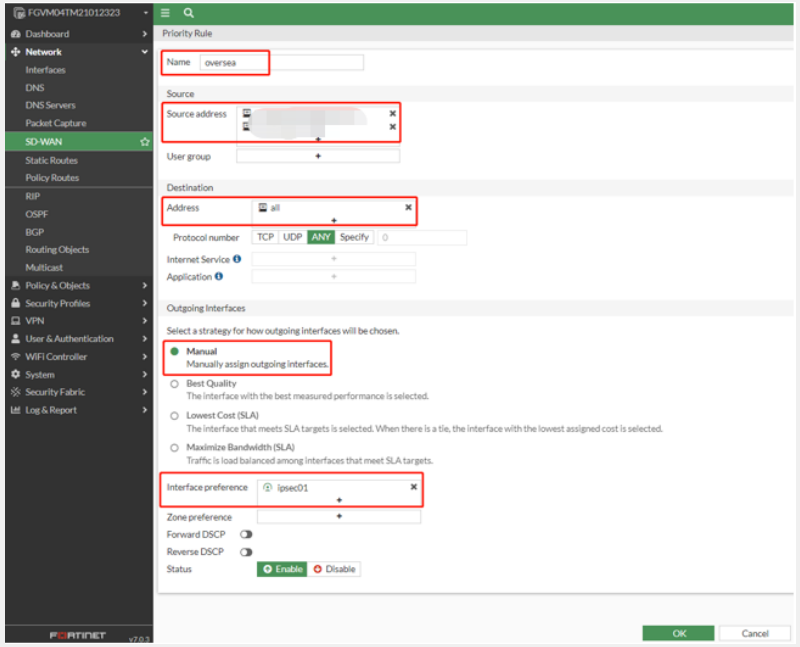


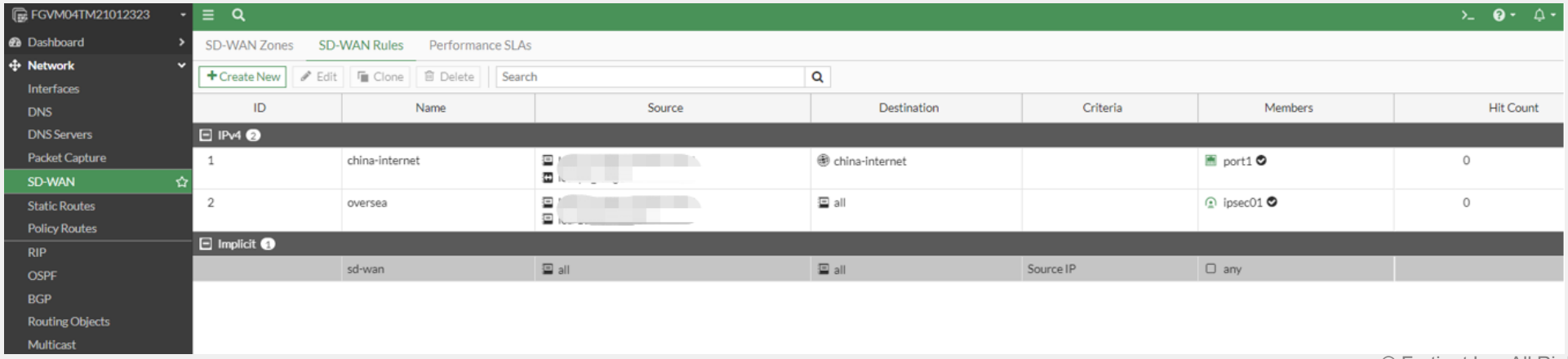
创建SD-WAN规则

创建规则1：部分流量走port1

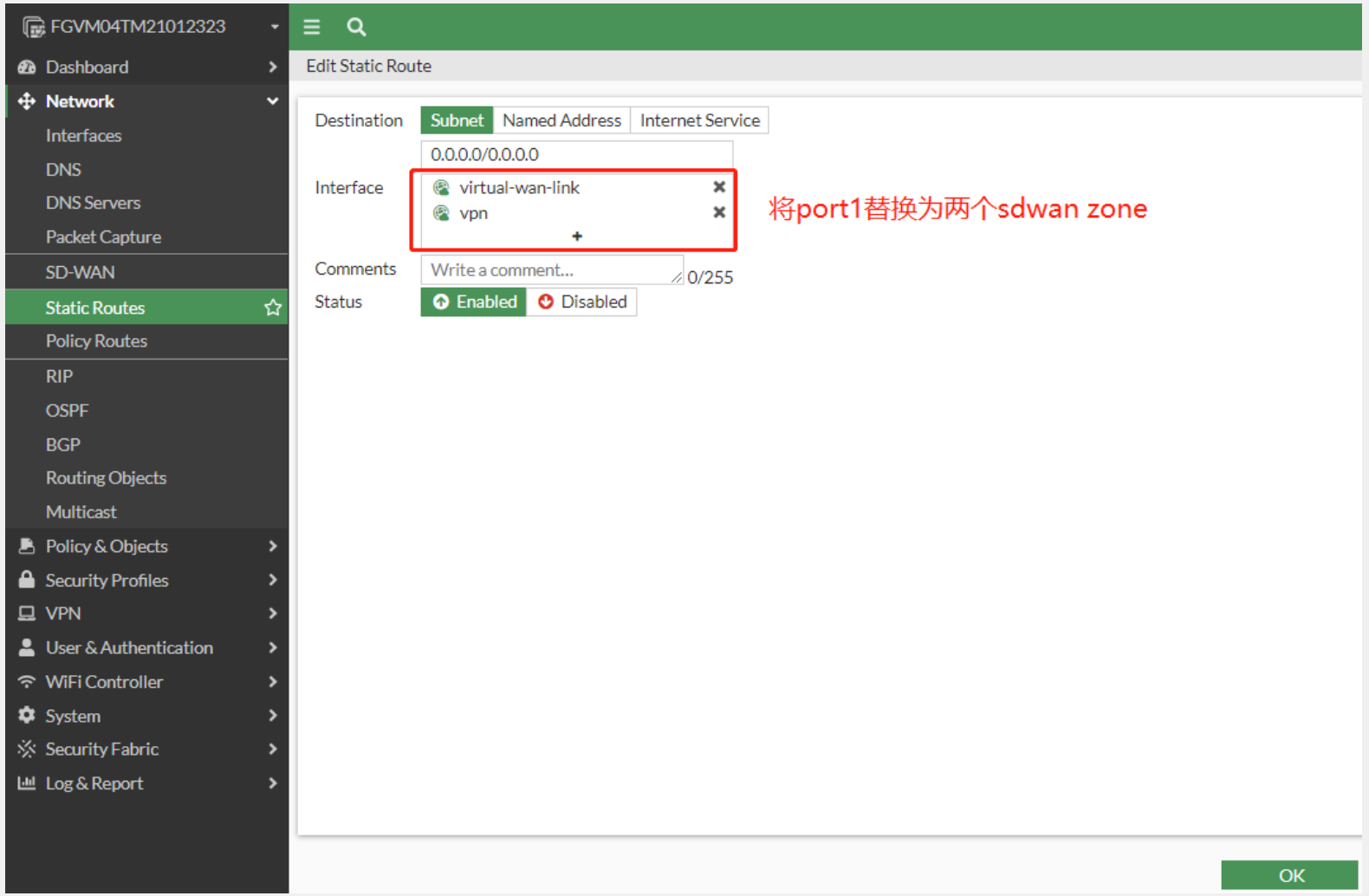


创建规则2：默认流量走ipsec vpn





修改默认路由



将port1替换为两个sdwan zone

4、VPN配置

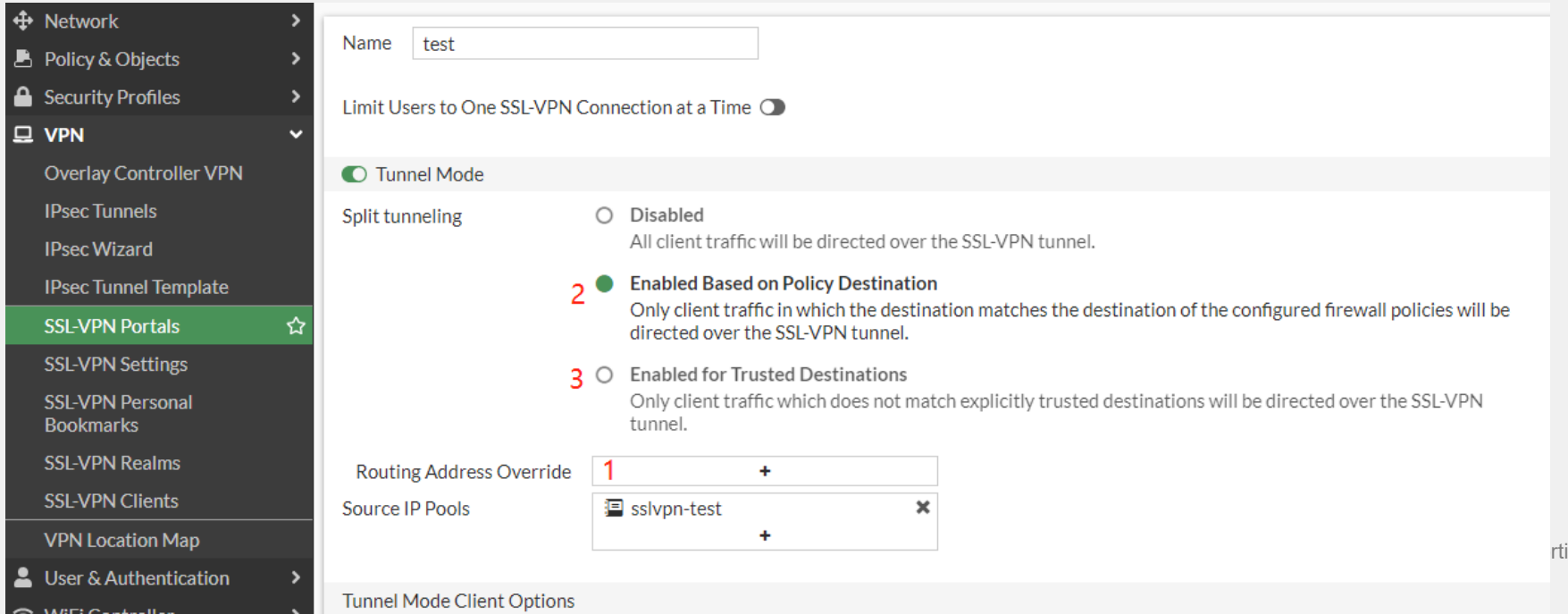
SSL VPN功能

- 同时监听多个接口：
- 隧道分离：三种方式

  1、下发明细IP网段路由走SSLVPN隧道，默认路由走客户端本地

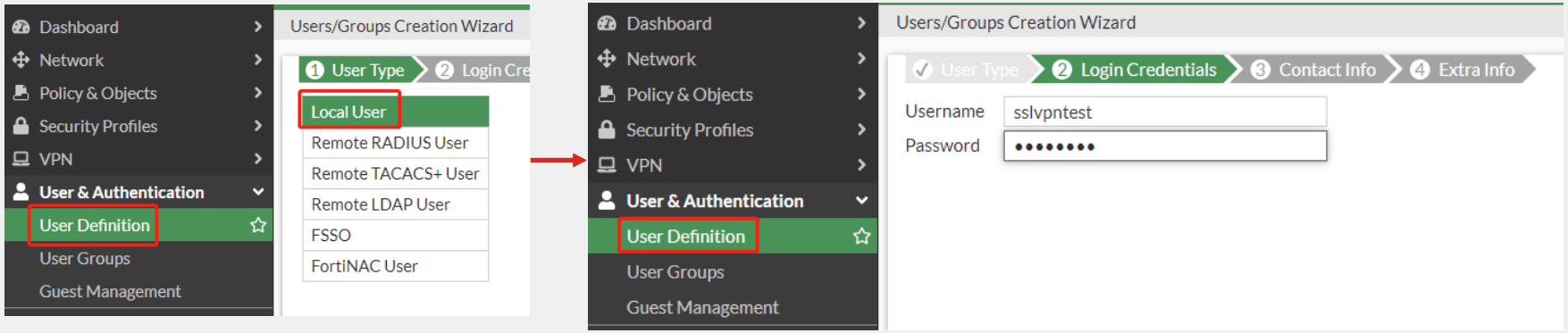
  2、下发防火墙策略中的目的地址走SSLVPN隧道（目的地址对象可以是FQDN地址），默认路由走客户端本地

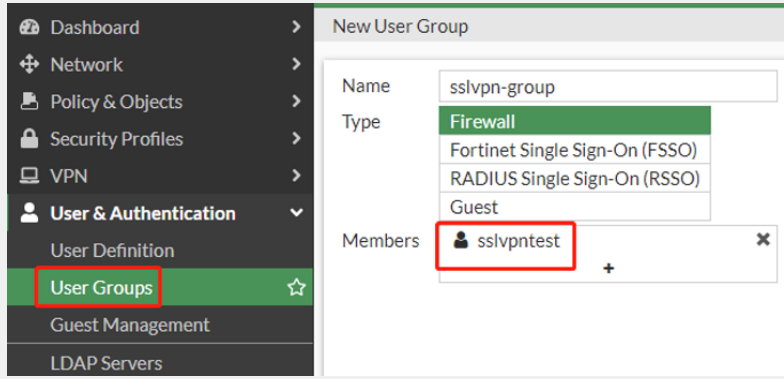
  3、下发明细IP网段路由走客户端本地，默认路由走SSLVPN隧道
- Portal：可单独设置dns server及Split DNS
- 认证：LDAP、RADIUS、双因子、SSO、证书+LDAP的双因子，通过FAC对接短信网关
- FortiOS 7.0支持FortiGate作为SSL VPN Client，并可结合SD-WAN执行流量选路，同时支持Split-DNS功能
- 零信任：结合EMS

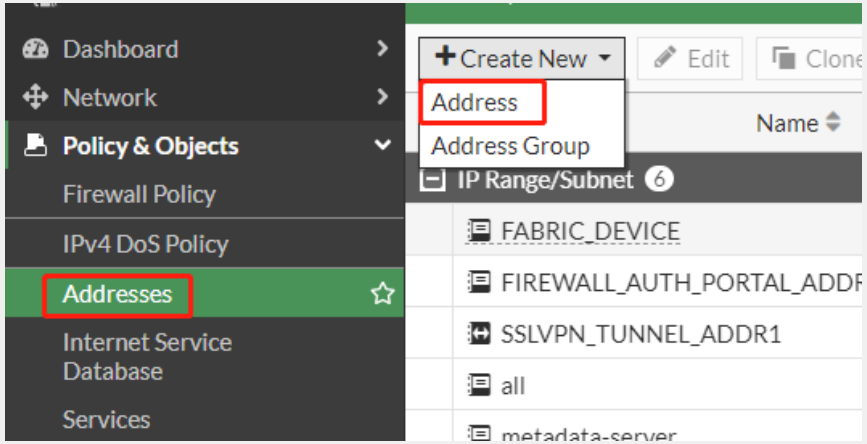


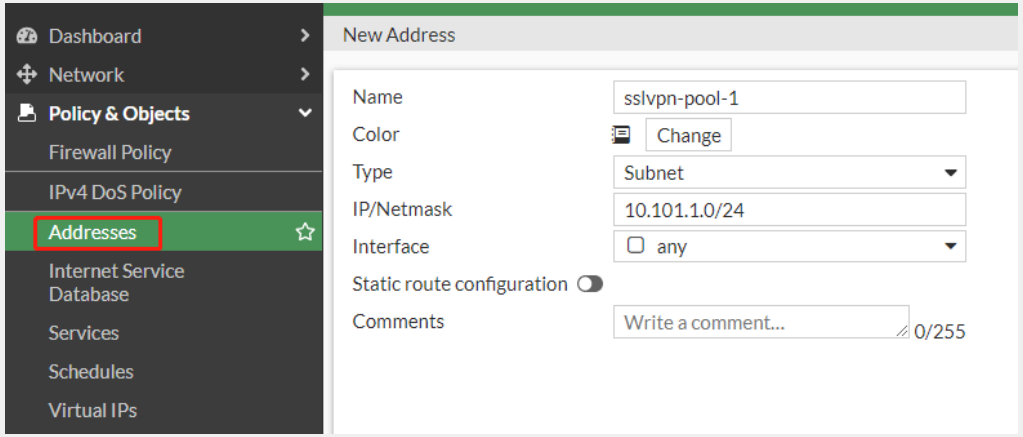
SSL VPN配置

- 配置用户、用户组及地址对象



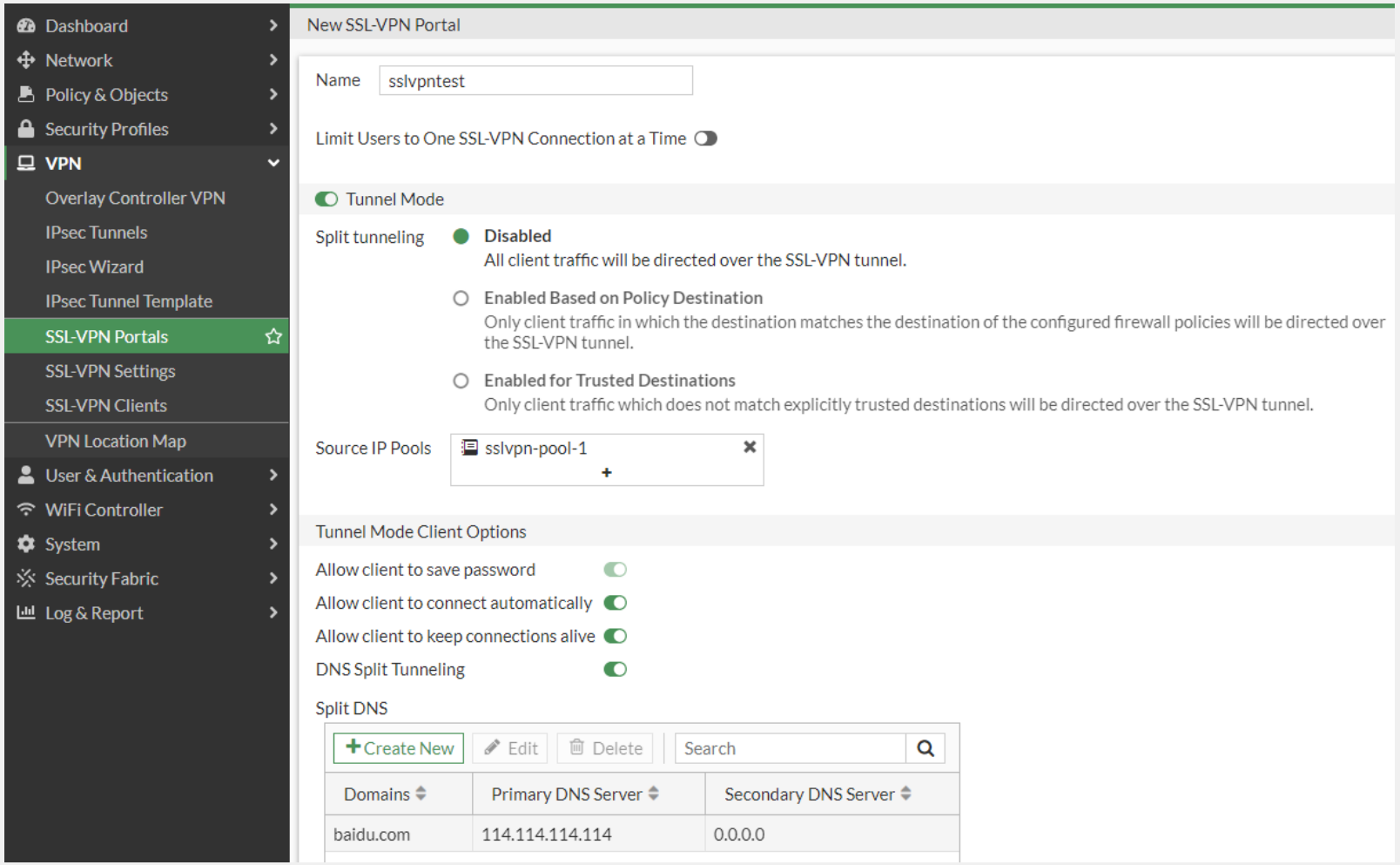






SSL VPN配置

- 配置SSL VPN Portal

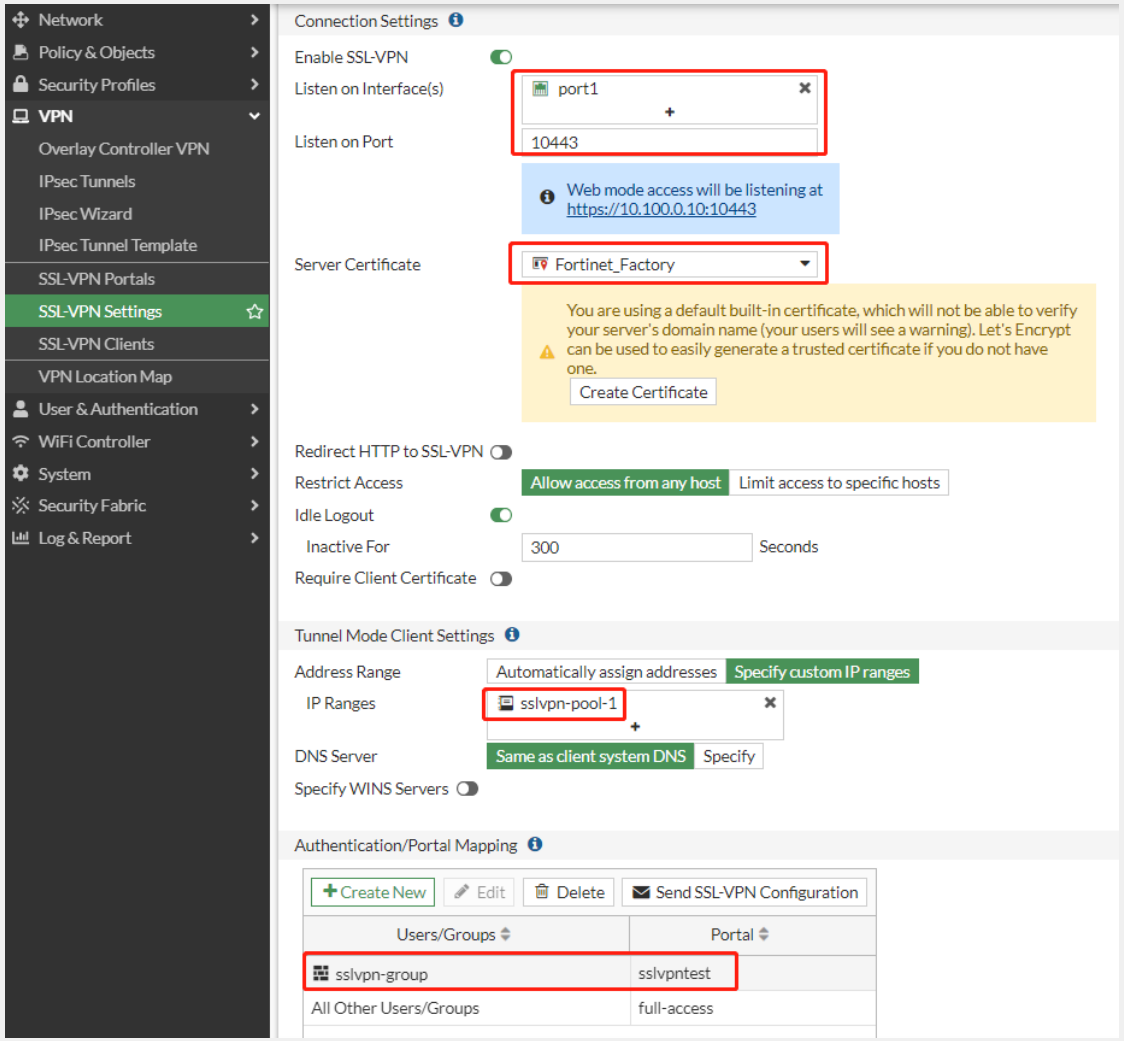


CLI Console (1)

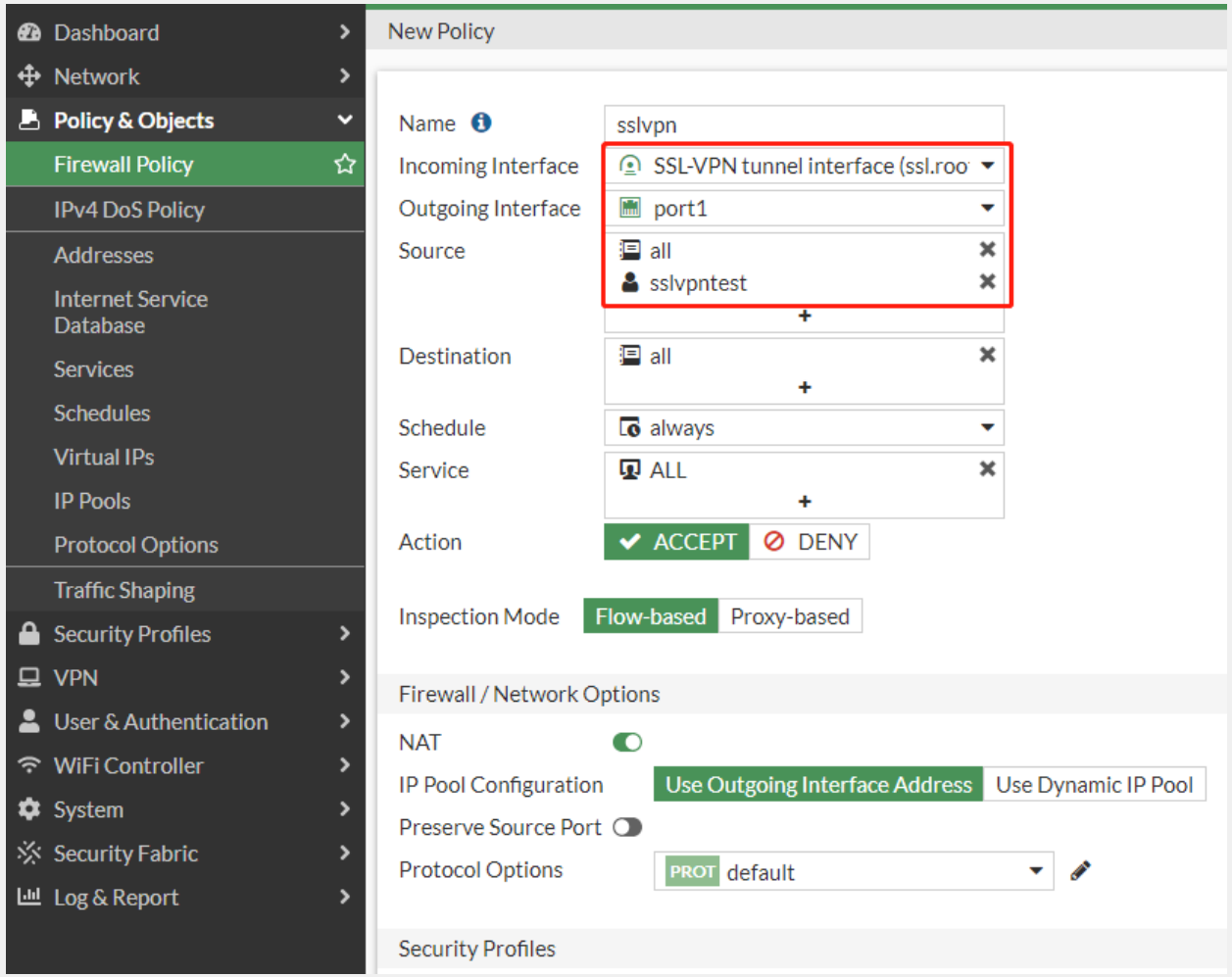
```
FGT-HK # config vpn ssl web portal

FGT-HK (portal) # edit sslvpntest

FGT-HK (sslvpntest) # set dns-server1 8.8.8.8

FGT-HK (sslvpntest) # set dns-server2 8.8.4.4

FGT-HK (sslvpntest) # sh
config vpn ssl web portal
    edit "sslvpntest"
        set tunnel-mode enable
        set web-mode enable
        set auto-connect enable
        set keep-alive enable
        set save-password enable
        set ip-pools "sslvpn-pool-1"
        set split-tunneling disable
        set dns-server1 8.8.8.8
        set dns-server2 8.8.4.4
        config bookmark-group
            edit "gui-bookmarks"
            next
        end
        config split-dns
            edit 1
                set domains "baidu.com"
                set dns-server1 114.114.114.114
            next
        end
    next
end

FGT-HK (sslvpntest) # end
```

SSL VPN配置

- 配置SSL VPN Setting



- 配置防火墙策略

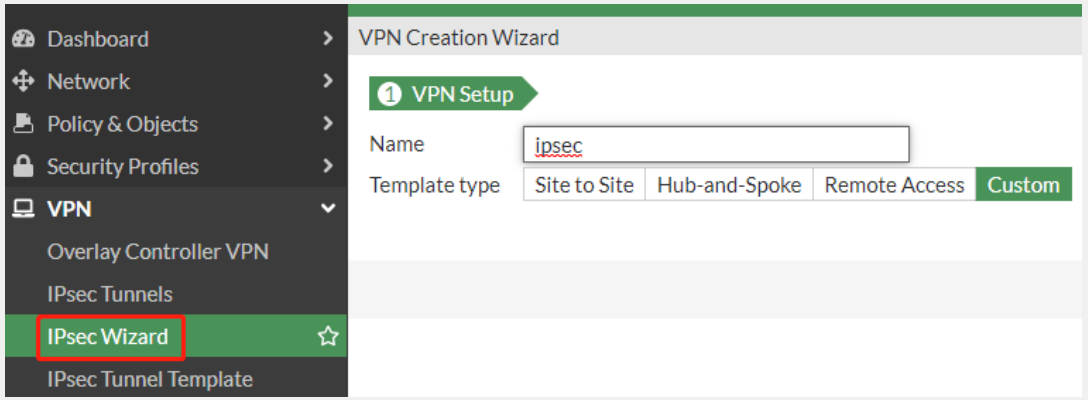


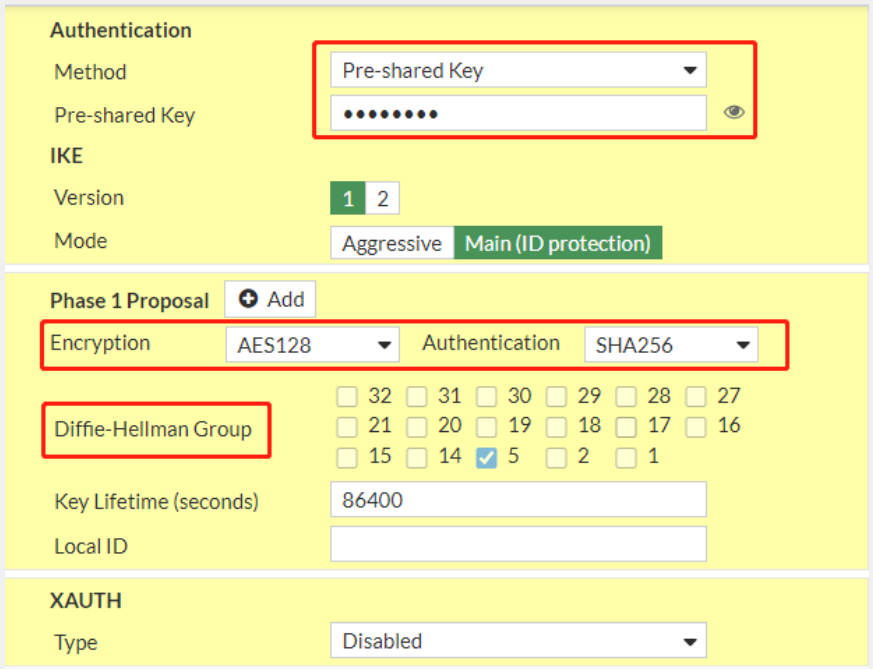
SSL VPN Client端配置

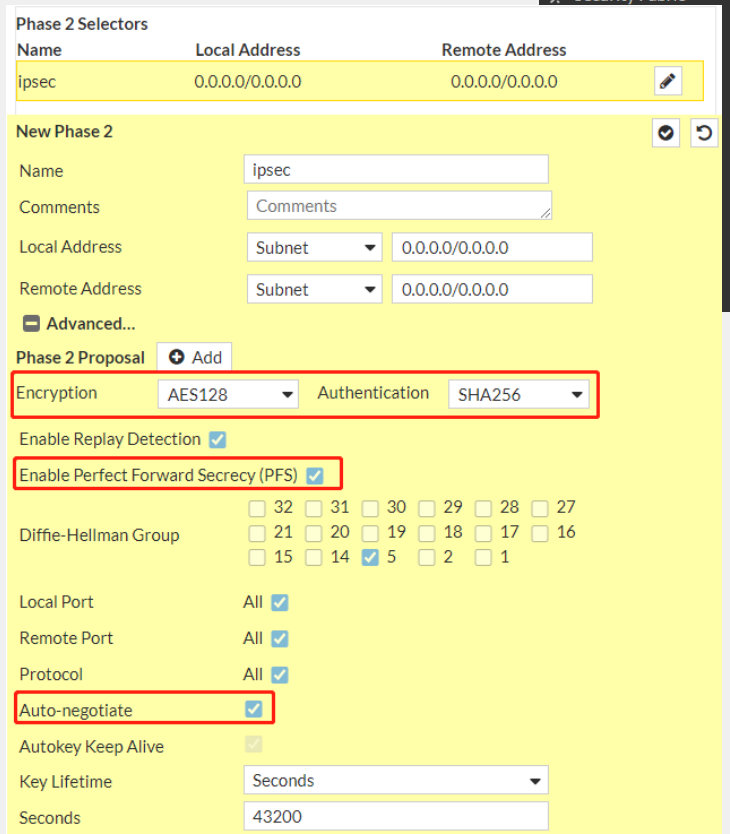

```
以太网适配器 以太网 3:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . : Fortinet SSL VPN Virtual Ethernet Adapter
   物理地址. . . . . : 00-09-0F-AA-00-01
   DHCP 已启用 . . . . . : 否
   自动配置已启用. . . . . : 是
   本地链接 IPv6 地址. . . . . : fe80::4d07:3ee5:dab:2f29%8(首选)
   IPv4 地址 . . . . . : 10.101.1.1(首选)
   子网掩码 . . . . . : 255.255.255.255
   默认网关. . . . . : 10.101.1.2
   DHCPv6 IAID . . . . . : 1207961871
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-28-5B-4F-E8-C0-3E-BA-57-93-2F
   DNS 服务器 . . . . . : 8.8.8.8
                          8.8.4.4
   TCPIP 上的 NetBIOS . . . . . : 已启用
```

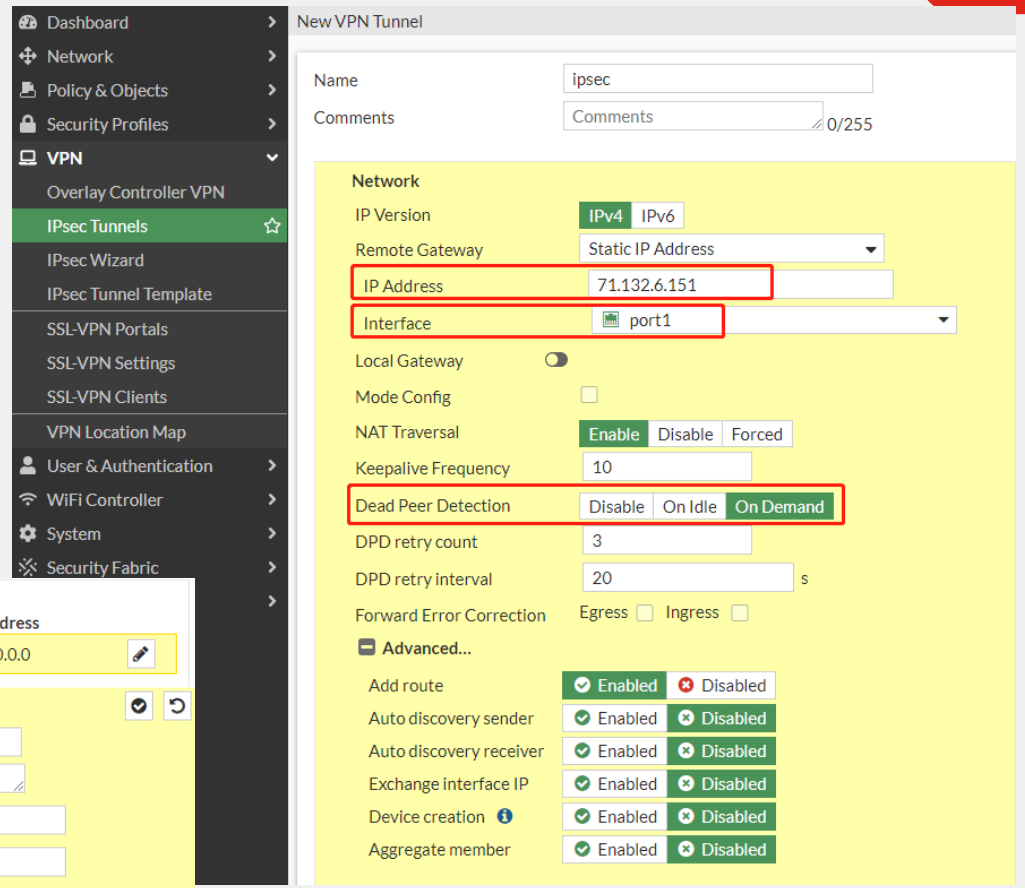
```
IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0      192.168.2.1    192.168.2.2    281
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.21    50
          0.0.0.0          0.0.0.0         10.101.1.2     10.101.1.1     1
         10.1.1.0    255.255.255.0         在链路上         10.1.1.1    291
         10.1.1.1  255.255.255.255         在链路上         10.1.1.1    291
       10.1.1.255  255.255.255.255         在链路上         10.1.1.1    291
         10.1.2.0    255.255.255.0         在链路上         10.1.2.1    291
         10.1.2.1  255.255.255.255         在链路上         10.1.2.1    291
       10.1.2.255  255.255.255.255         在链路上         10.1.2.1    291
         10.1.3.0    255.255.255.0         在链路上         10.1.3.1    291
         10.1.3.1  255.255.255.255         在链路上         10.1.3.1    291
       10.1.3.255  255.255.255.255         在链路上         10.1.3.1    291
       10.101.1.1  255.255.255.255         在链路上       10.101.1.1    257
   18.163.78.239  255.255.255.255      192.168.2.1    192.168.2.2     25
        127.0.0.0        255.0.0.0         在链路上         127.0.0.1    331
        127.0.0.1  255.255.255.255         在链路上         127.0.0.1    331
  127.255.255.255  255.255.255.255         在链路上         127.0.0.1    331
      192.168.1.0    255.255.255.0         在链路上       192.168.1.21    306
```

IPSEC VPN配置



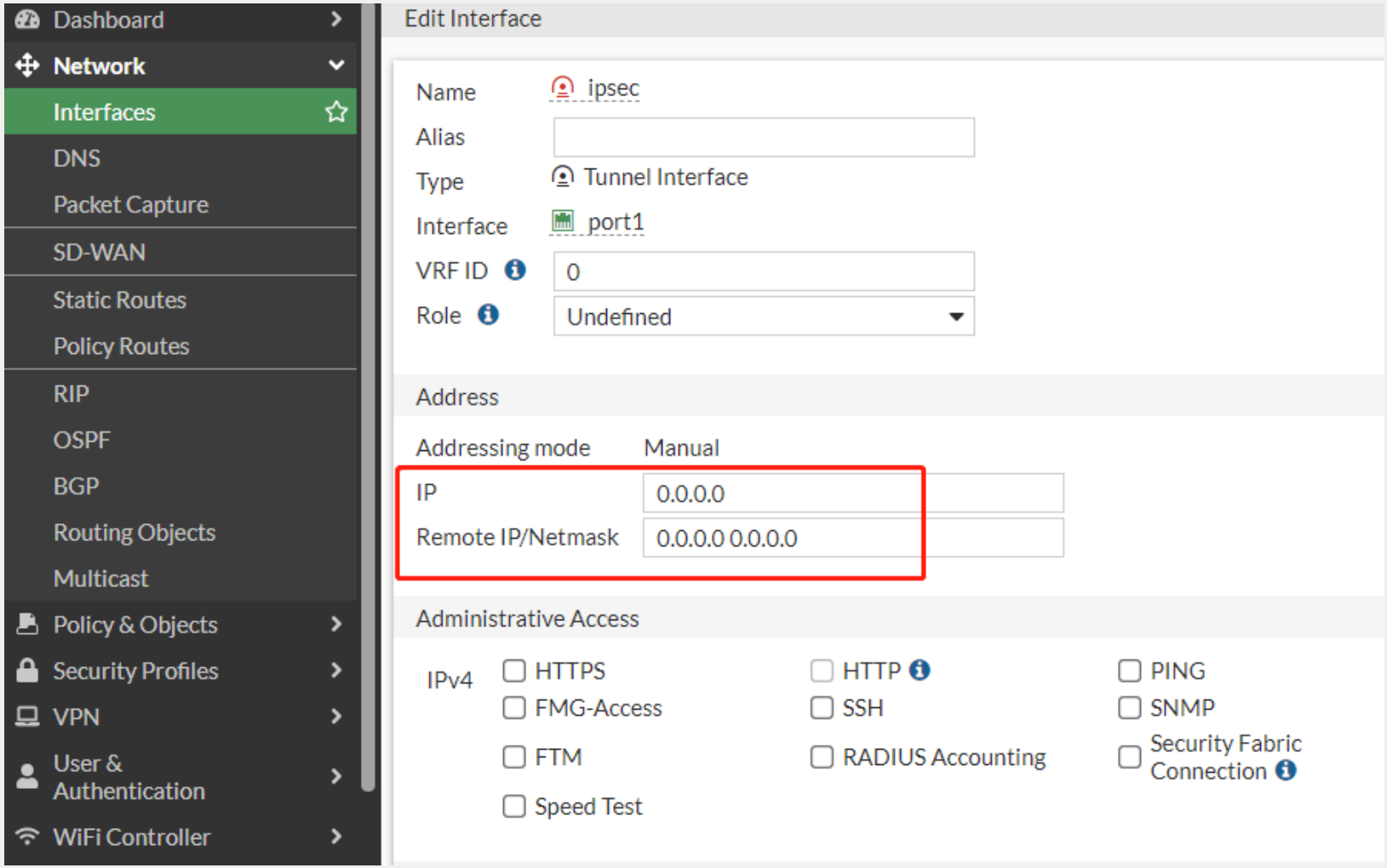






IPSEC VPN配置

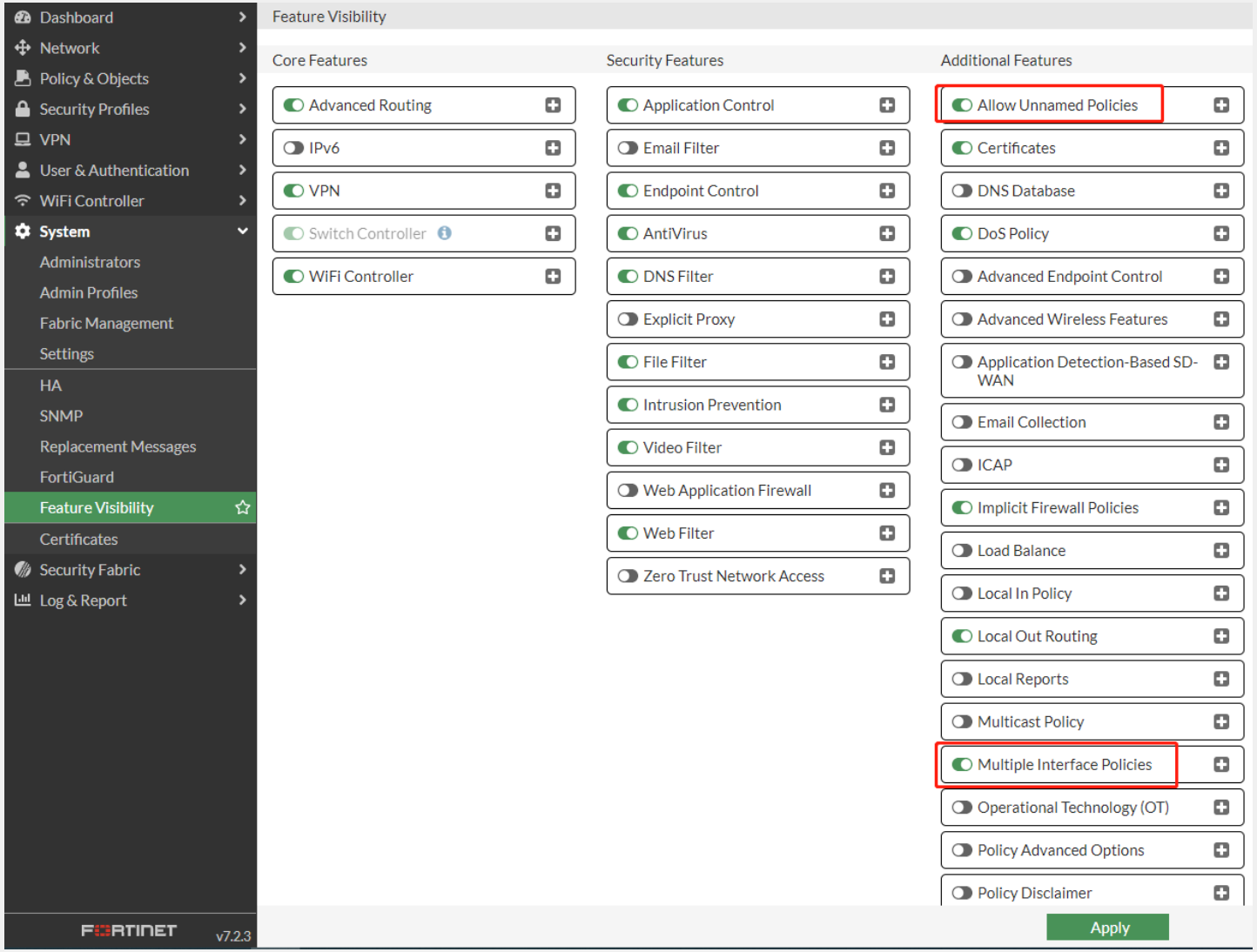
- FortiGate可以给Ipsec vpn接口分配ip地址，可以利用ipsec vpn建立BGP路由



5、策略及安全控制

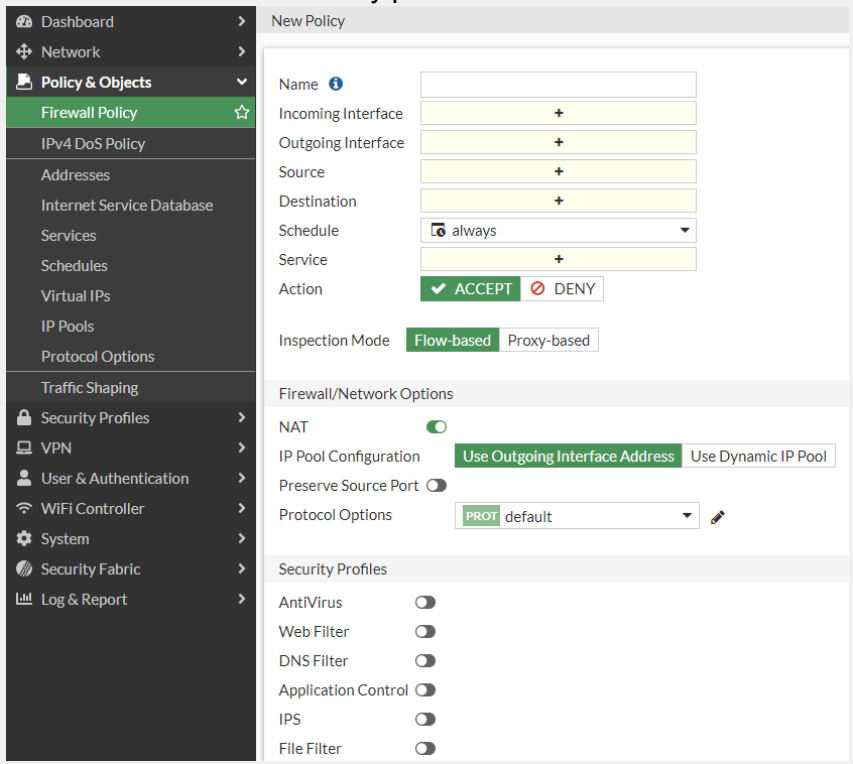
防火墙策略

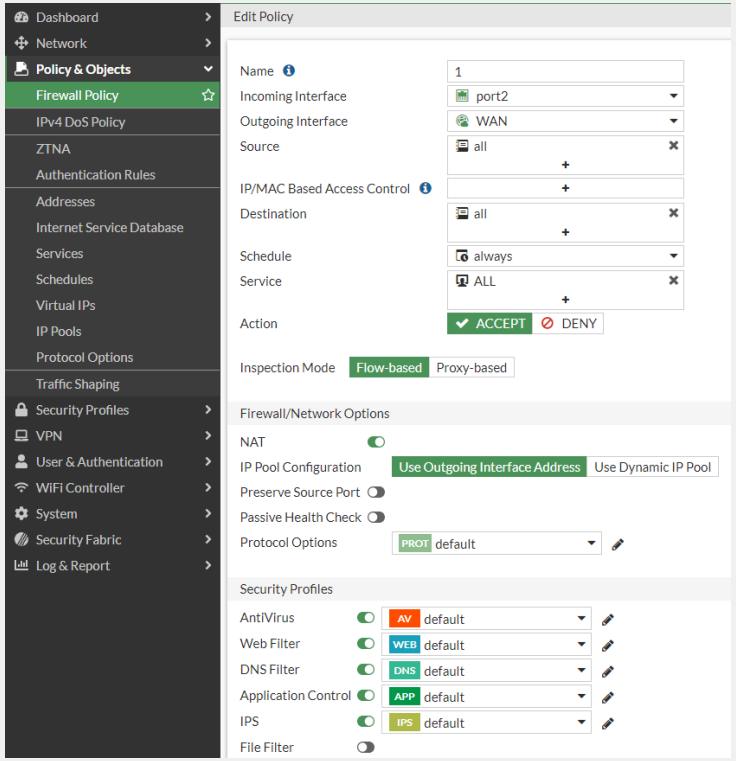
可根据需要开启“允许未命名策略”及“多接口策略”

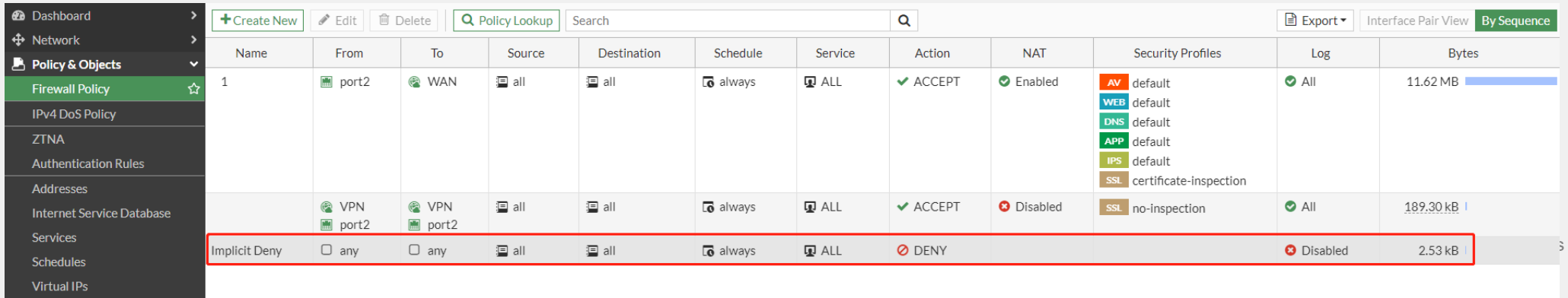


防火墙策略

FortiGate默认将所有转发流量阻止，若需要放通需要转发的流量，需要添加相应的防火墙策略，需要设置入接口、出接口、源地址（或ISDB应用，可结合用户）、目的地址（或ISDB应用）、Schedule（可选）、服务（协议端口），策略的动作可以是接受或阻止，Inspection mode默认是flow-based，可以选择开启或关闭NAT（这里是SNAT），可以根据需要开启所需的security profile。





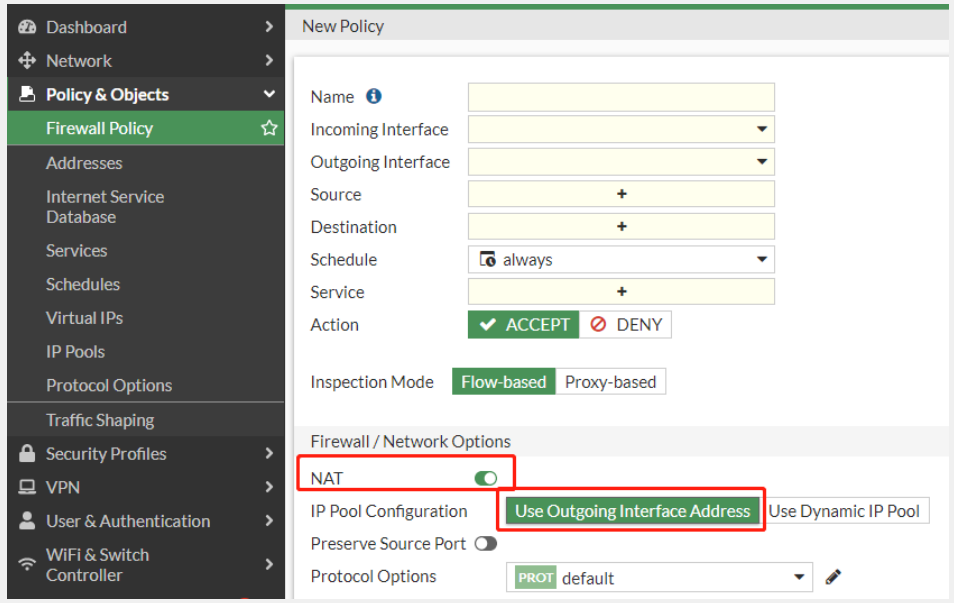


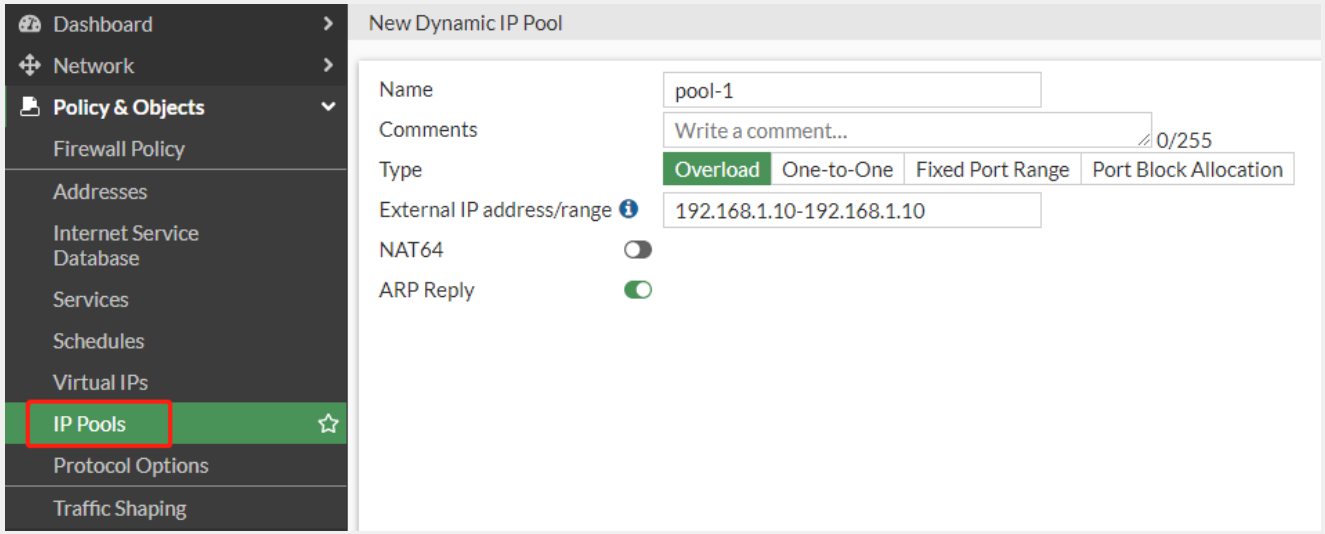
SNAT配置

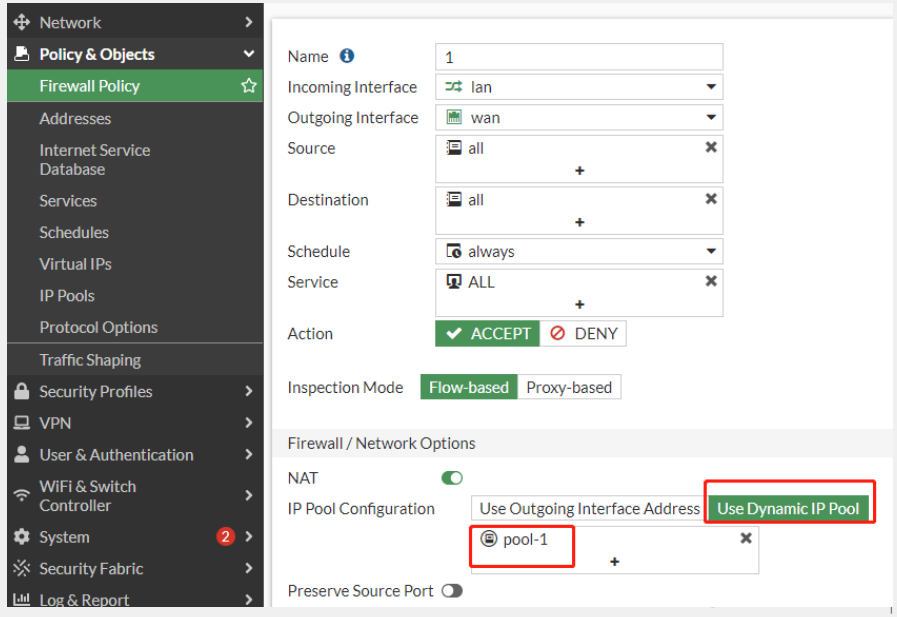
在防火墙策略里启用NAT

可以用出接口的地址作为NAT地址

也可以建立一个IP POOL指定NAT地址

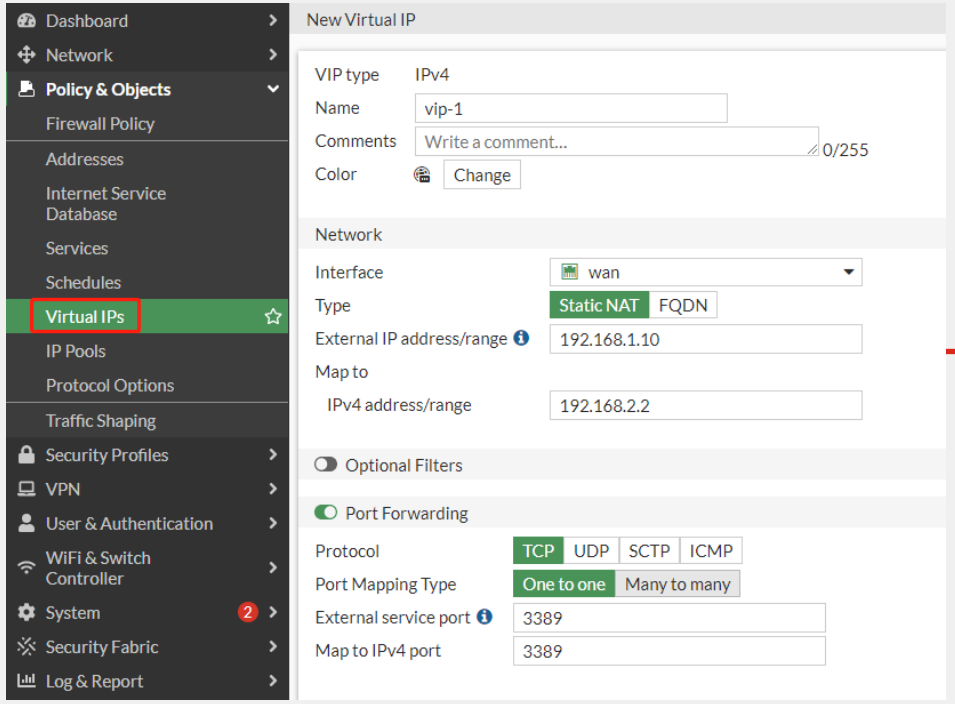


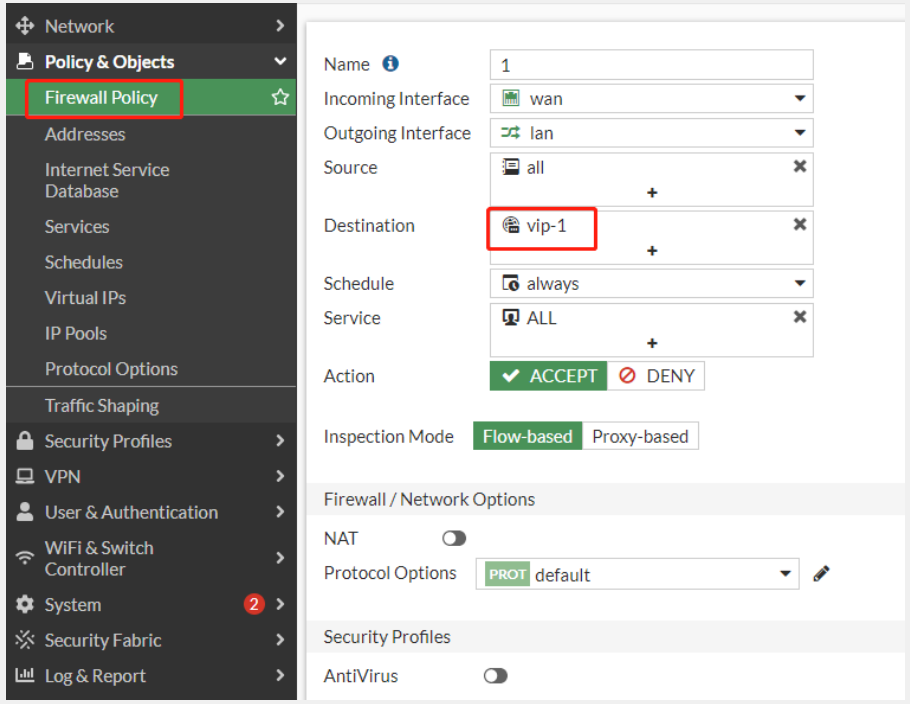




DNAT配置

创建Virtual IP，指定外部ip和内部ip及端口，在防火墙策略调用Virtual IP对象





VIP命令行配置

```
config firewall vip
    edit "1"
        set id 0
        set uuid e5f1bd16-7f8b-51ed-1c36-11cf6649399c
        set comment ''
        set type static-nat
        set extip 0.0.0.0
        set nat44 enable
        set nat46 disable
        set extintf ''
        set arp-reply enable
        set nat-source-vip disable
        set portforward disable
        set gratuitous-arp-interval 0
        set ssl-client-rekey-count 0
        set color 0
    next
end
```

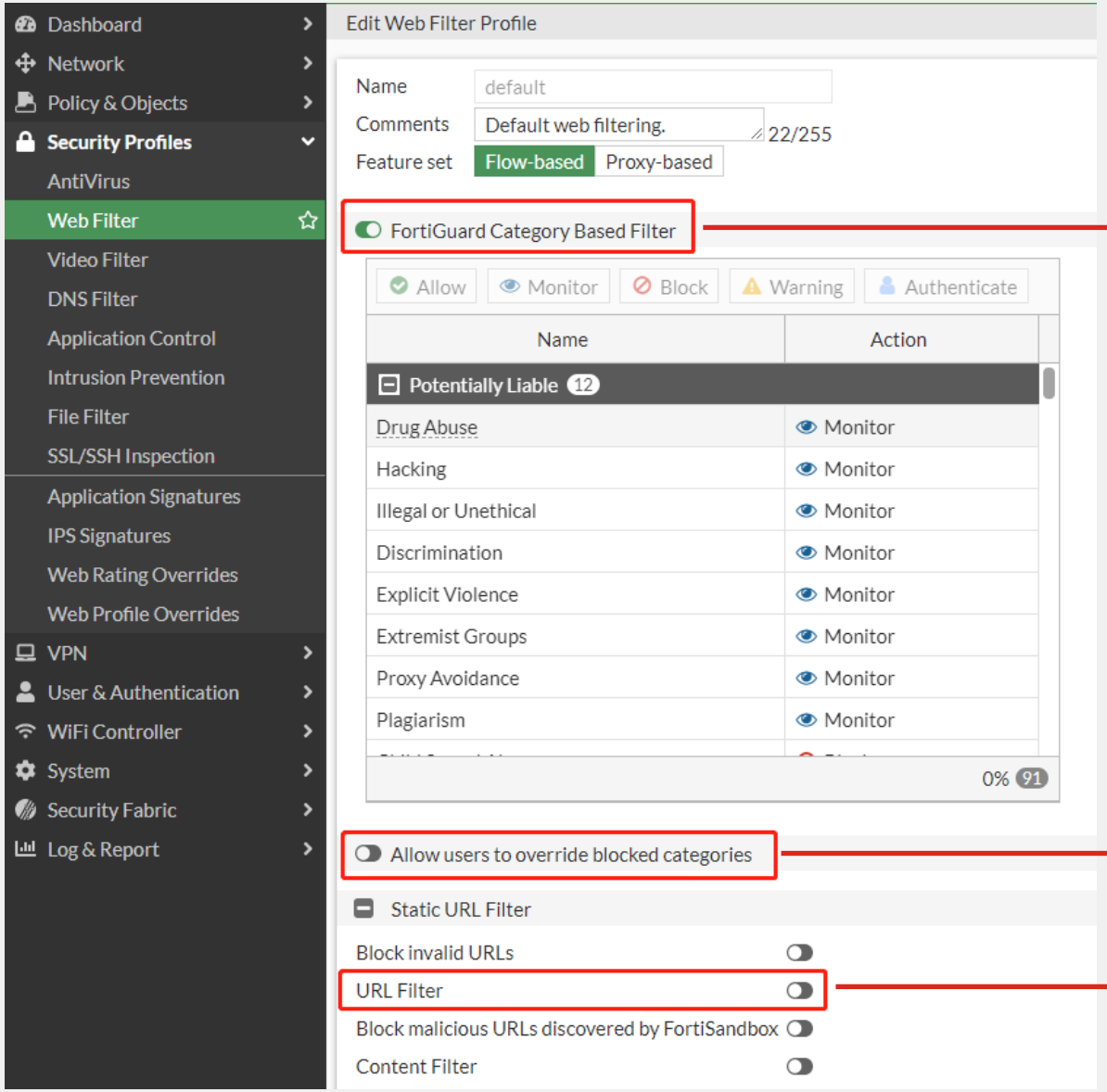
设置了VIP之后，对于流量的SNAT的优先级顺序如下：

1、如果VIP下开启了nat-source-vip，则VIP的返回流量的SNAT优先匹配VIP的对应关系；

2、防火墙策略中调用的IP Pools；

3、接口IP

安全策略——web filter



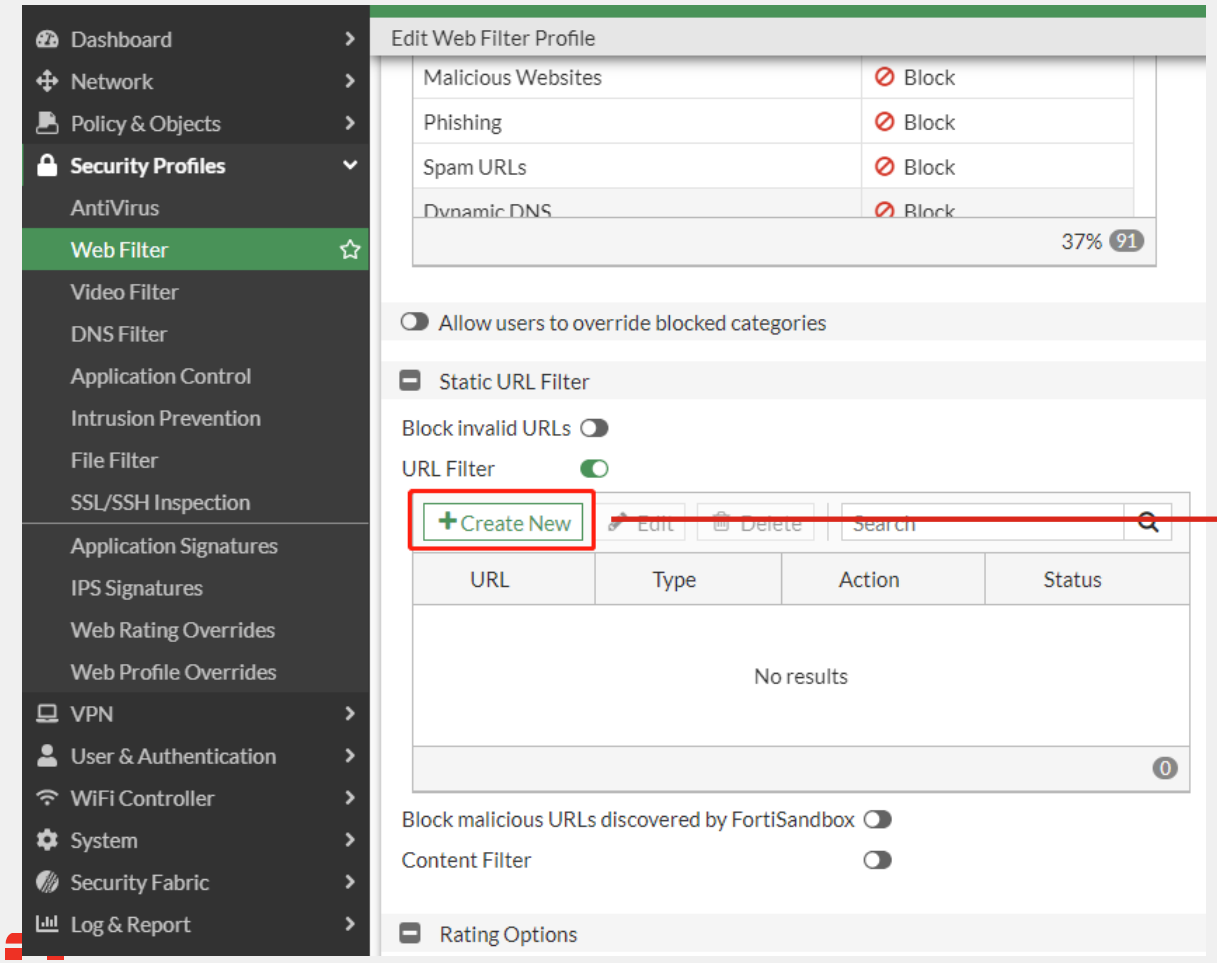
基于**Fortiguard**分类做管控

可允许用户采用单独策略

可设置域名过滤的黑白名单

安全策略——web filter

参考以下链接文章：
https://community.fortinet.com/t5/FortiGate/Technical-Tip-URL-Filter-expressions-for-the-FortiGate/ta-p/192746?externalID=FD37057



Simple:

比如键入net.com，将匹配fortinet.com

比如net.com/prod，将匹配www.fortinet.com/products/next-generation-firewall

Wildcard：

for*guard，将匹配fortiguard.com

*.Fortinet.com将匹配www.Fortinet.com或者support.Fortinet.com

Regular Expression

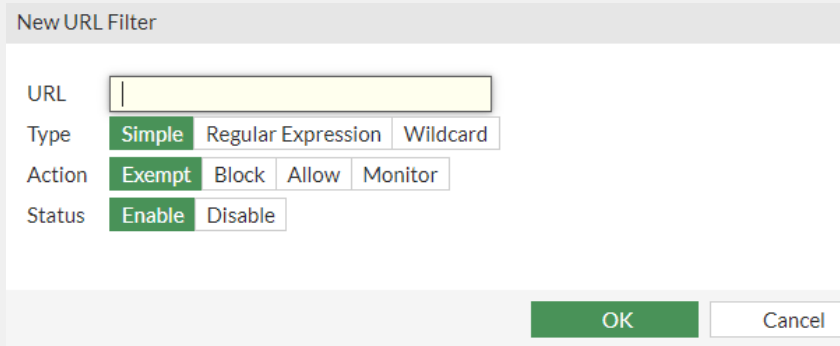
正则表达式用于包含一个或多个与使用某些 Perl 语法的模式相关或不相关的 URL，例如：

‘*’符号表示：匹配该符号前的字符0次或多次，例如：'fortinet*.com' 将匹配 'fortinetttttt.com' 但不匹配 'fortinetsupport.com’。

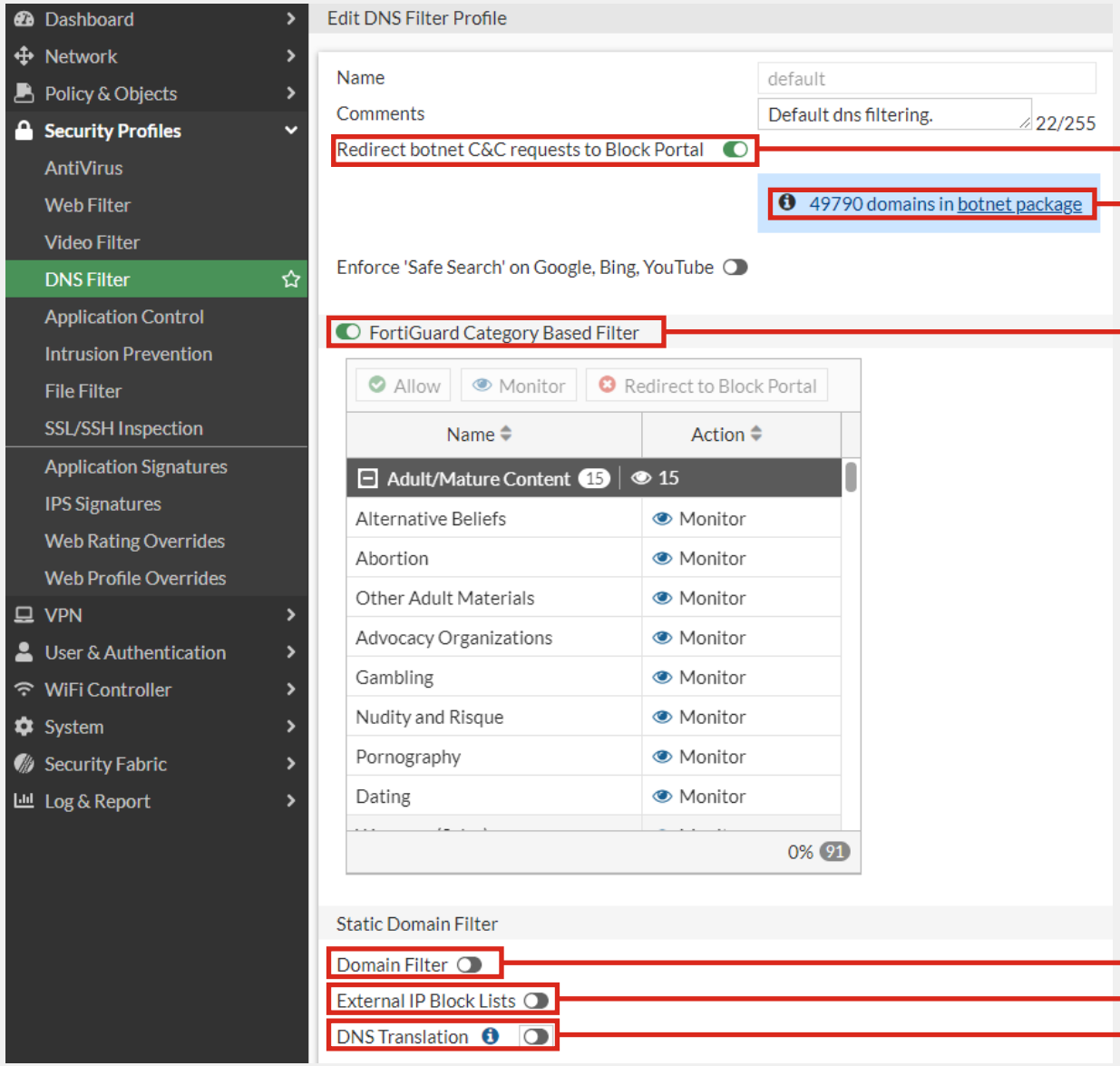
'/i' 符号表示：使模式区分大小写。- 例如：'/FORTINET/i' 将与'fortinet' 不匹配。

'^' 符号表示：在字符串的开头。- 例如：'^fo' 将匹配 'fortinet.com' 但不匹配 'support.fortinet.com' 或 'notfortinet.com‘。

更多字符用法可参阅https://perldoc.perl.org/perlre



安全策略——dns filter



重定向bonet C&C请求到一个阻止页面

点击可查询bonet域名列表

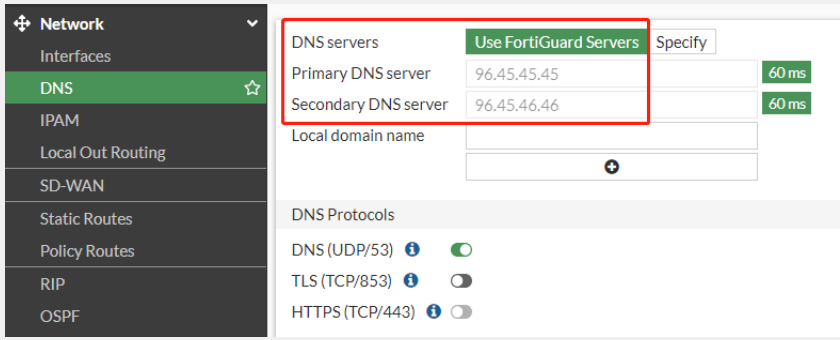
基于Fortiguard分类做管控，
需要有web filter许可

可设置域名过滤的黑白名单，设置的规则同上一页的web filter

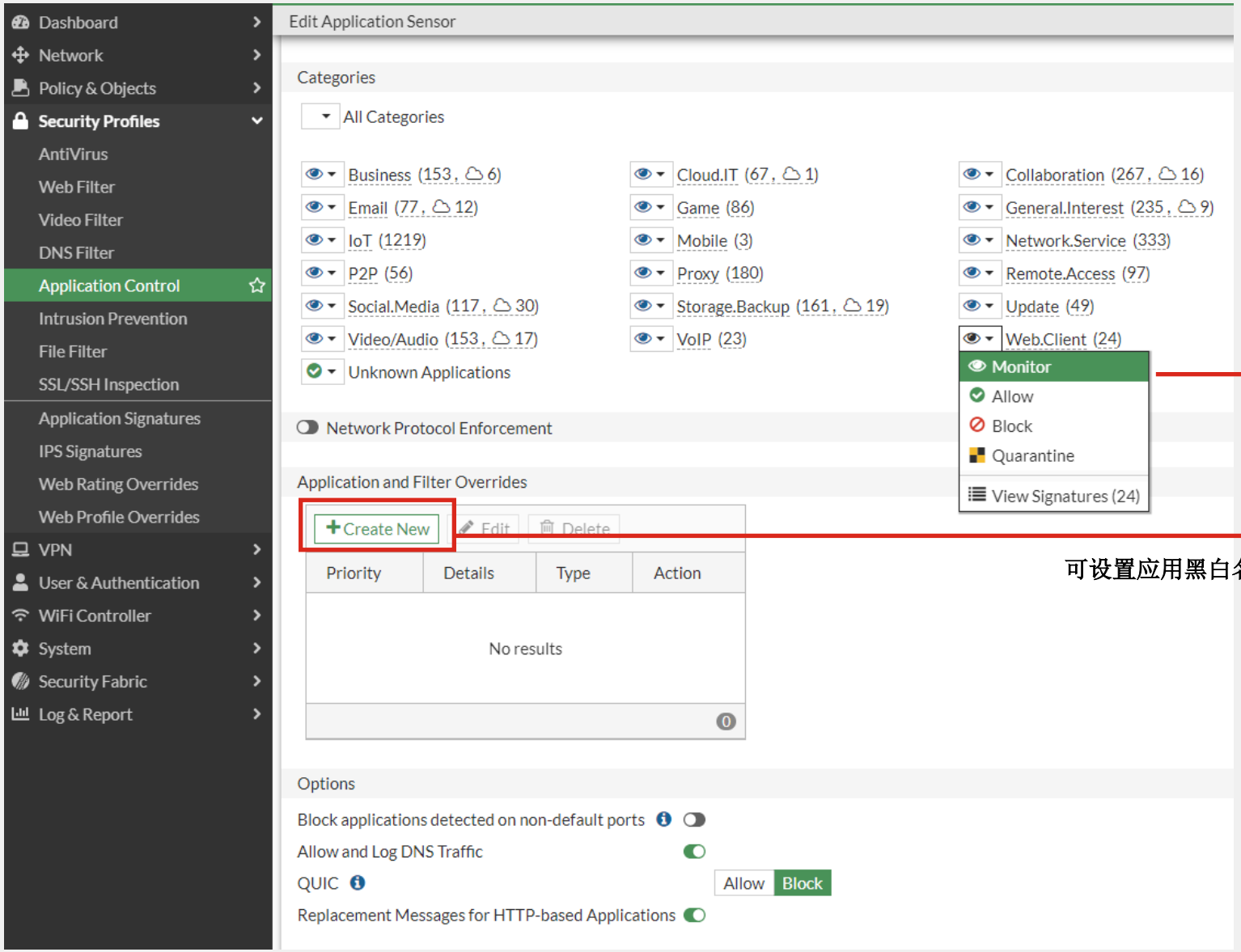
可引入外部IP阻止清单

可设置替代解析的IP地址

使用dns filter，FortiGate本机DNS需要设置为FortiGard DNS（初始默认）

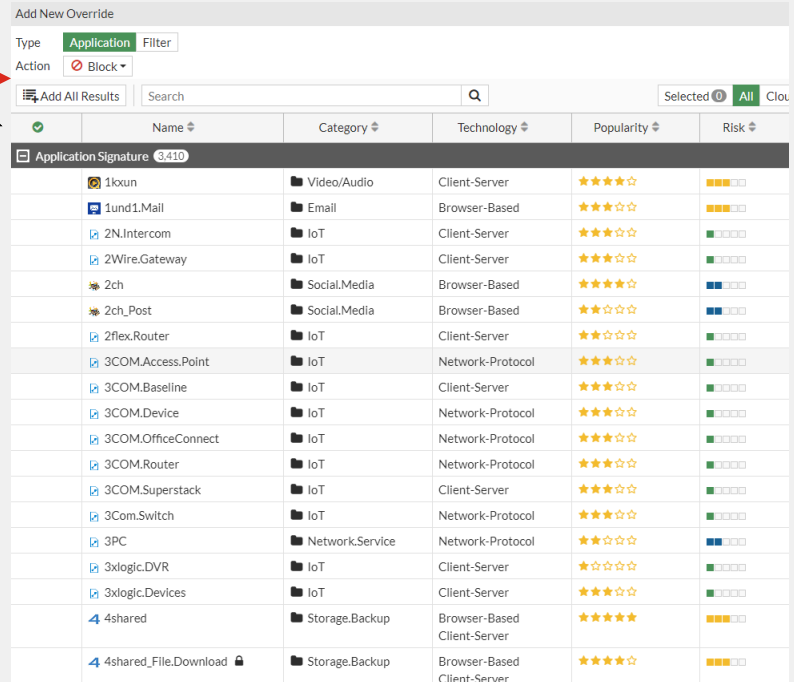


安全策略——application control



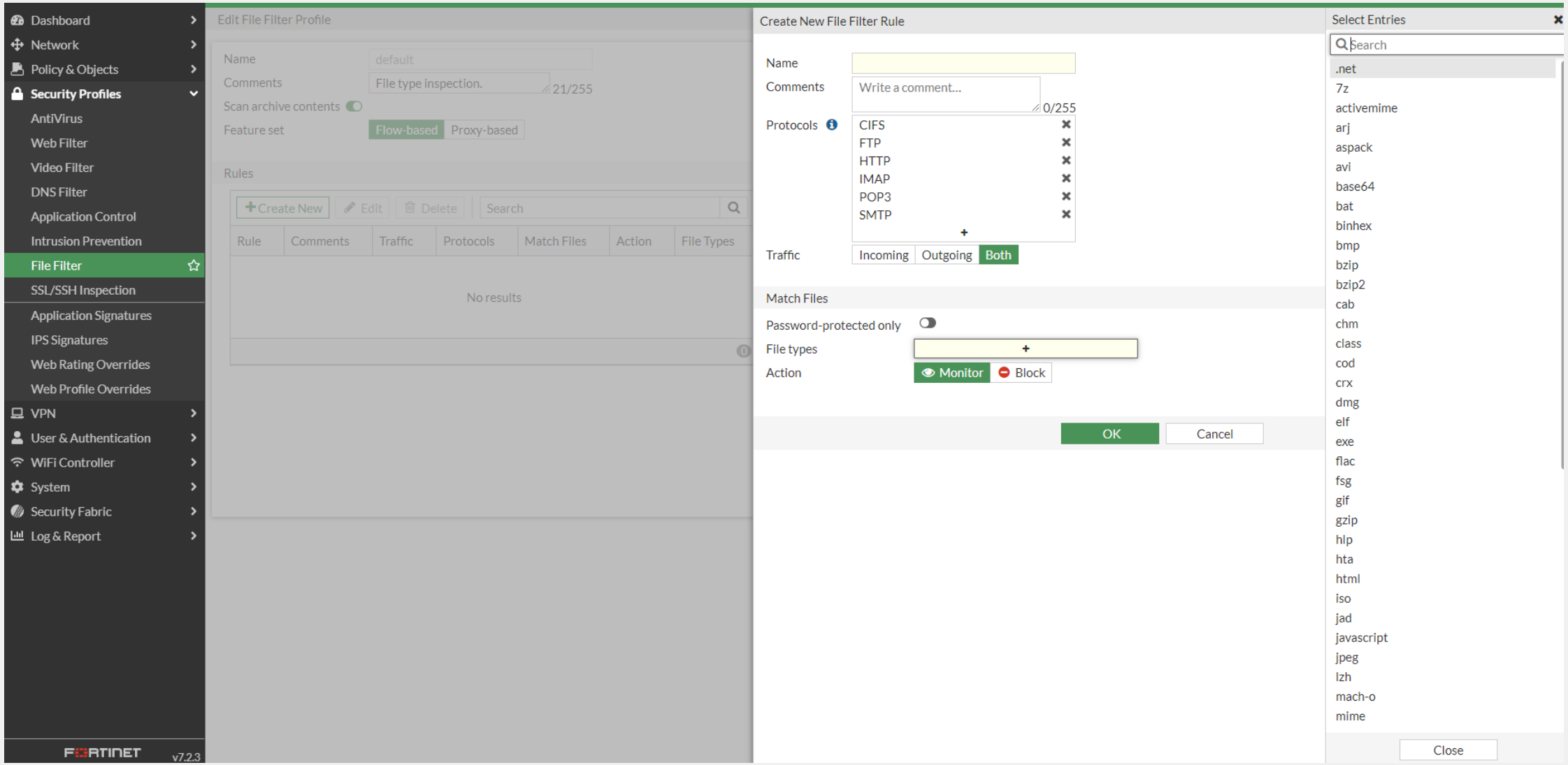
可基于应用分类设置监控、允许、阻止、隔离的动作

可设置应用黑白名单



安全策略——文件过滤

文件过滤分两种：一种是只对文件类型做过滤的**File Filter**，另一种是针对文件大小和文件内容的**DLP**



安全策略——DLP：数据防泄漏

DLP只支持命令行配置，配置举例：过滤关键字

1. Configure the DLP dictionary:

```
config dlp dictionary
    edit "dic-case2-keyword-regex-hex"
        config entries
            edit 1
                set type "keyword"
                set pattern "demo"
                set repeat enable
            next
            edit 2
                set type "regex"
                set pattern "demo(regex){1,5}"
                set repeat enable
            next
            edit 3
                set type "hex"
                set pattern "e6b58be8af95"
                set repeat enable
            next
        end
    next
end
```

2. Configure the DLP sensor:

```
config dlp sensor
    edit "sensor-case2-keyword-regex-hex"
        config entries
            edit 1
                set dictionary "dic-case2-keyword-regex-hex"
                set count 5
            next
        end
    next
end
```

3. Configure the DLP profile:

```
config dlp profile
    edit "profile-case2-keyword-regex-hex"
        config rule
            edit 1
                set proto ftp
                set sensor "sensor-case2-keyword-regex-hex"
                set action log-only
            next
        end
    next
end
```

4. Add the DLP profile to a firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "custom-deep-inspection"
        set dlp-profile "profile-case2-keyword-regex-hex"
        set logtraffic all
        set nat enable
```

安全策略——DLP：数据防泄漏

DLP只支持命令行配置，配置举例：阻止下载exe文件并记录大于500k的exe文件日志

1. Configure the DLP file pattern:

```
config dlp filepattern
    edit 3
        set name "case3-exe"
        config entries
            edit "exe"
                set filter-type type
                set file-type exe
            next
        end
    next
end
```

2. Configure the DLP profile:

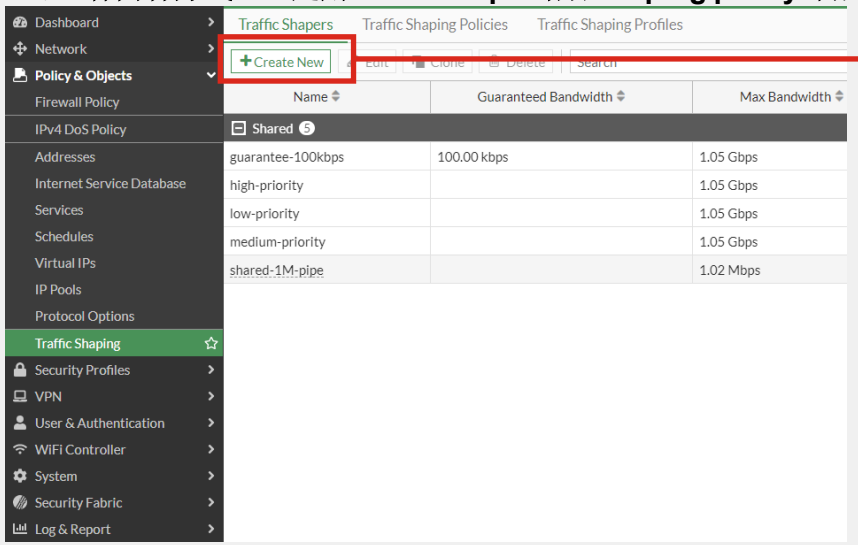
```
config dlp profile
    edit "profile-case3-type-size"
        config rule
            edit 1
                set proto http-get
                set filter-by none
                set file-type 3
                set action block
            next
            edit 2
                set proto http-get
                set filter-by none
                set file-size 500
                set action log-only
            next
        end
    next
end
```

3. Add the DLP profile to a firewall policy:

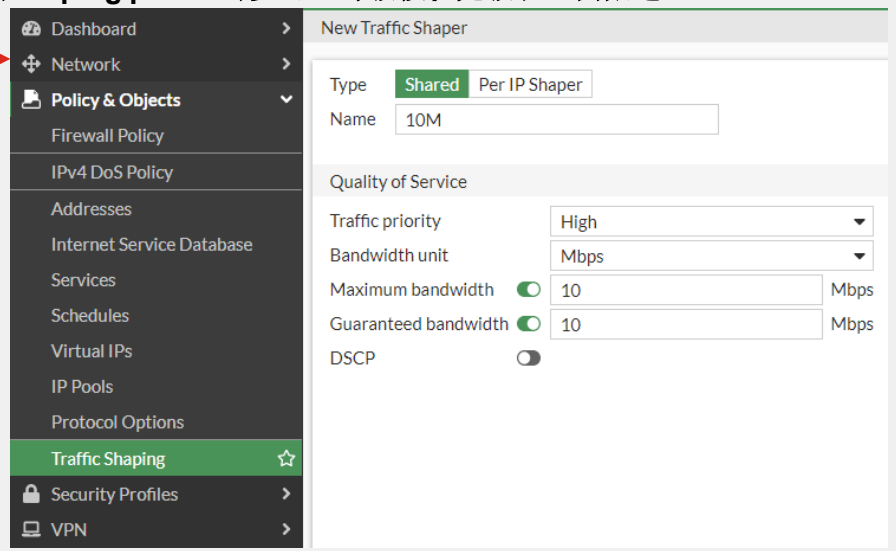
```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "custom-deep-inspection"
        set dlp-profile "profile-case3-type-size"
        set logtraffic all
        set nat enable
    next
end
```

QoS——shaper + shaping policy

QoS有两种方式：一是用traffic shaper结合shaping policy对流量做限速，二是用shaping profile对多QoS等级按优先级和比例限速



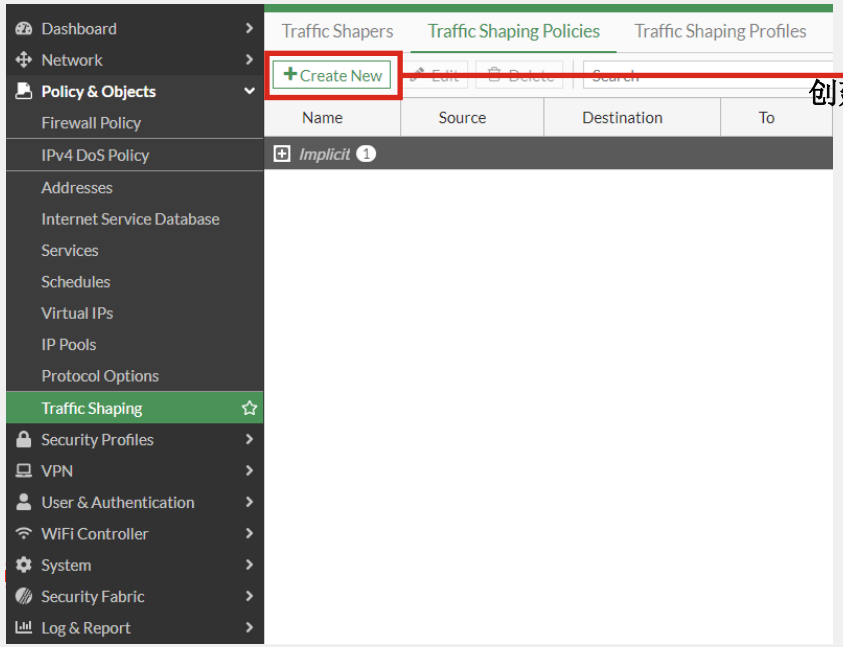
创建shaper



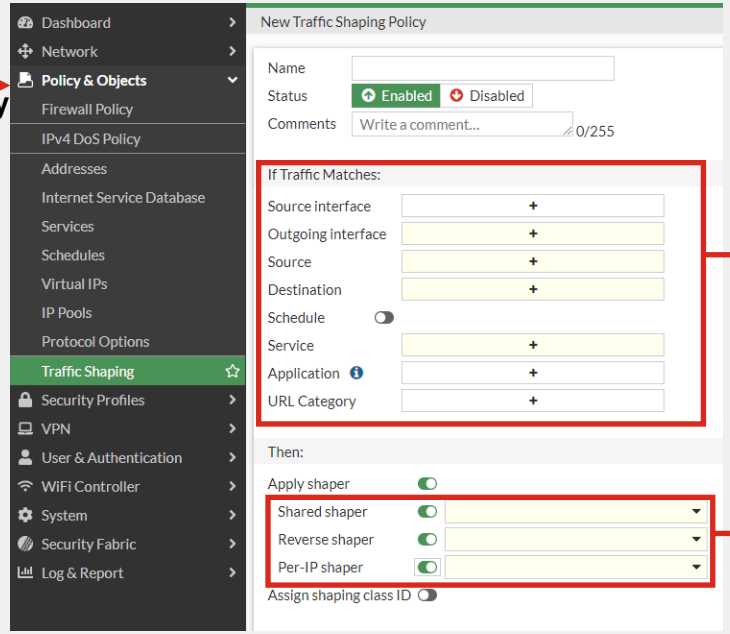
Shaper命令行：

```
config firewall shaper traffic-shaper
    edit "10M"
        set guaranteed-bandwidth 10
        set maximum-bandwidth 10
        set bandwidth-unit mbps
        set priority high
        set per-policy disable
        set diffserv disable
        set overhead 0
    next
end
```

Per-policy默认disable，若存在多个shaping policy调用同一个shaper的情况，则带宽是共享这个shaper的，enable之后则是每个policy独享



创建shaping policy

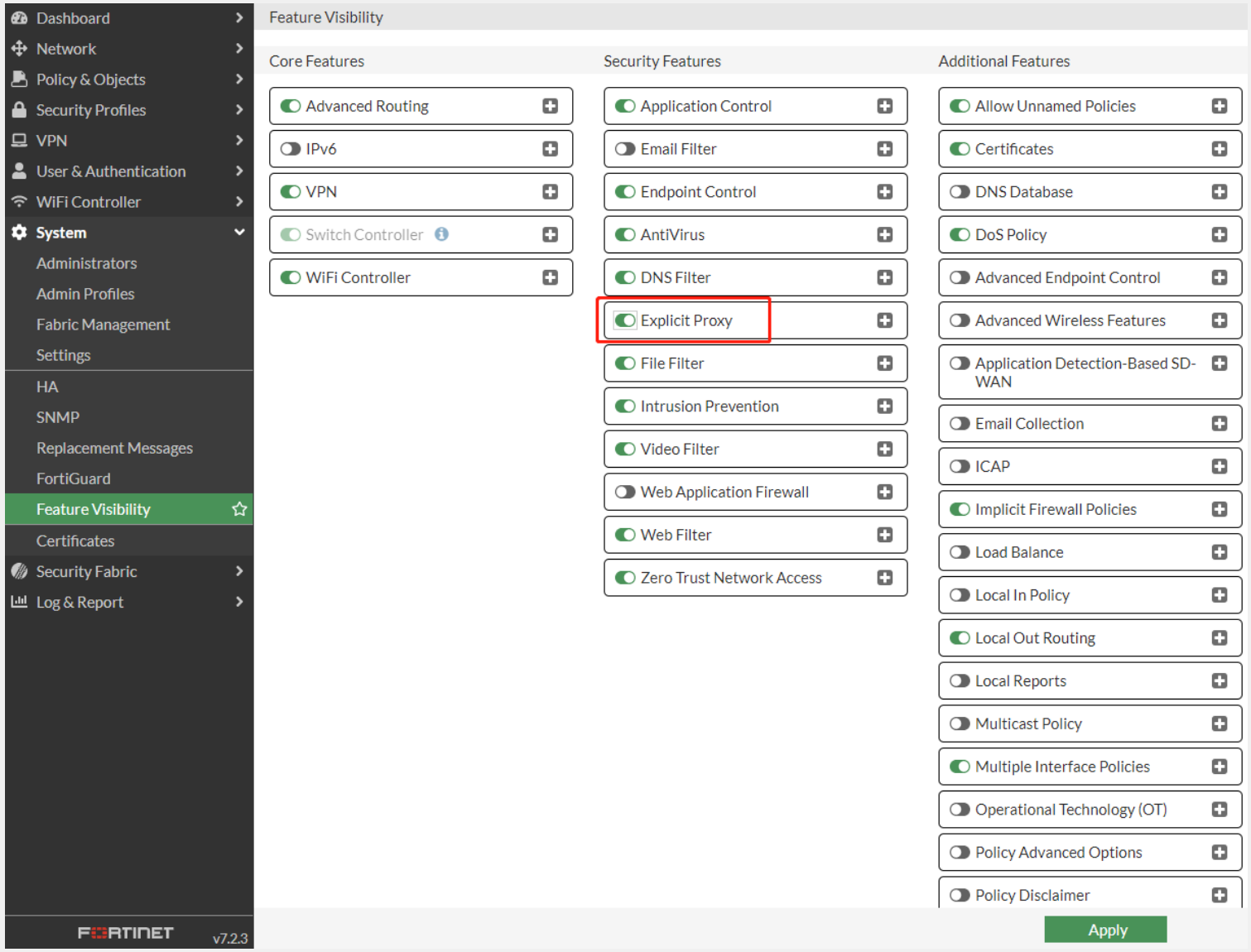


设置匹配条件

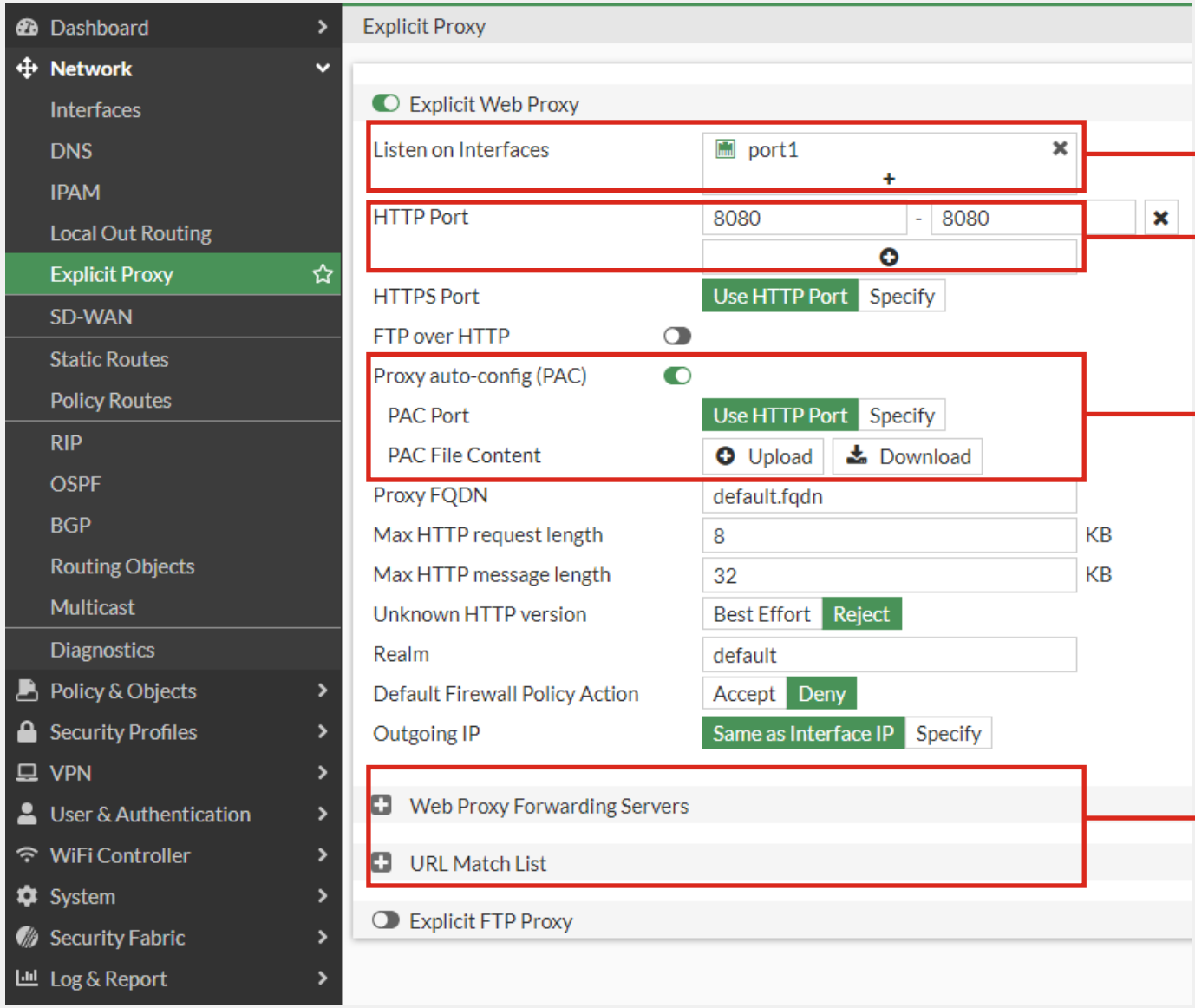
调用shaper

Proxy——功能开启

可在功能可见列表中开启**Explicit Proxy**功能



Proxy——接口设置



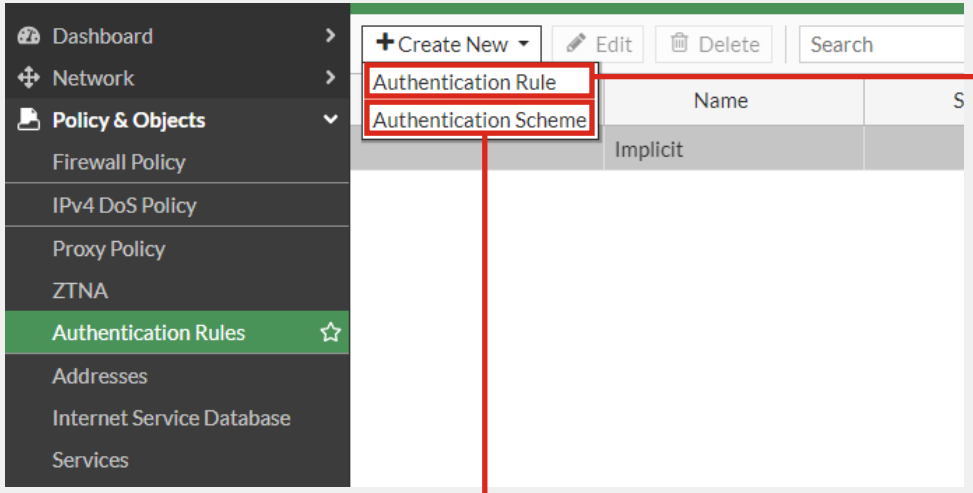
设置监听接口

设置监听端口

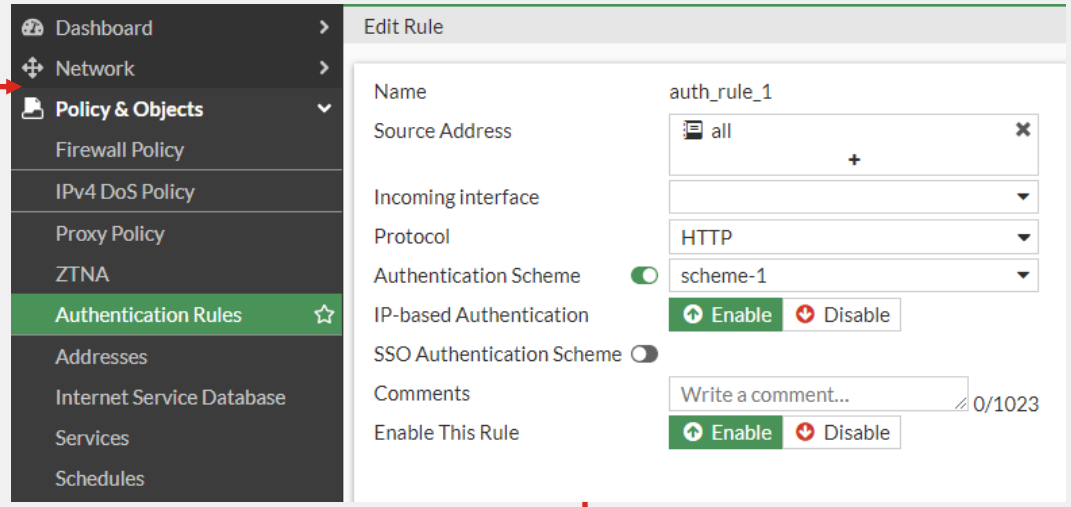
设置PAC文件，若不设置，则所有http流量都被代理
若设置了PAC文件，则文件地址为
http://port1_IP:8080/文件名.pac

可设置某些URL的流量转发给下一级代理

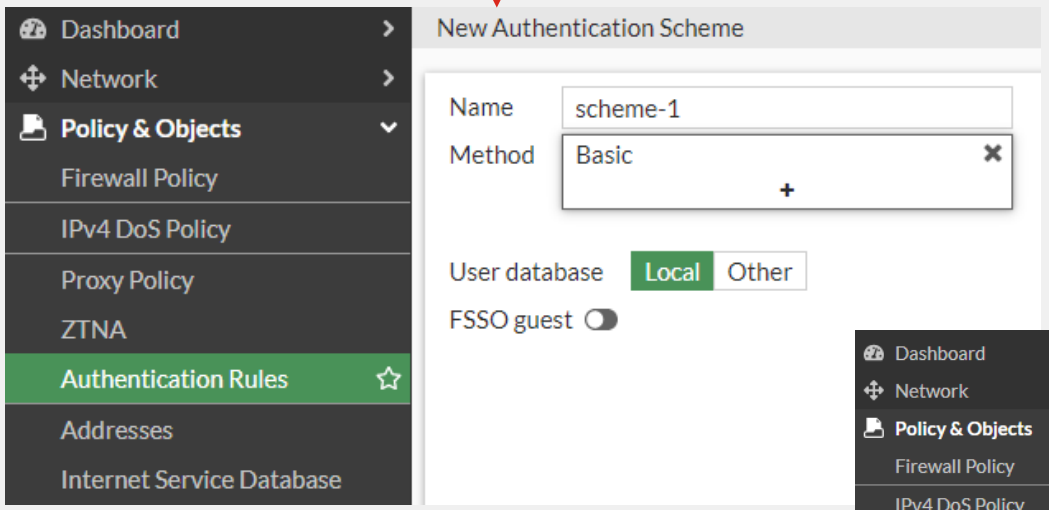
Proxy——认证设置



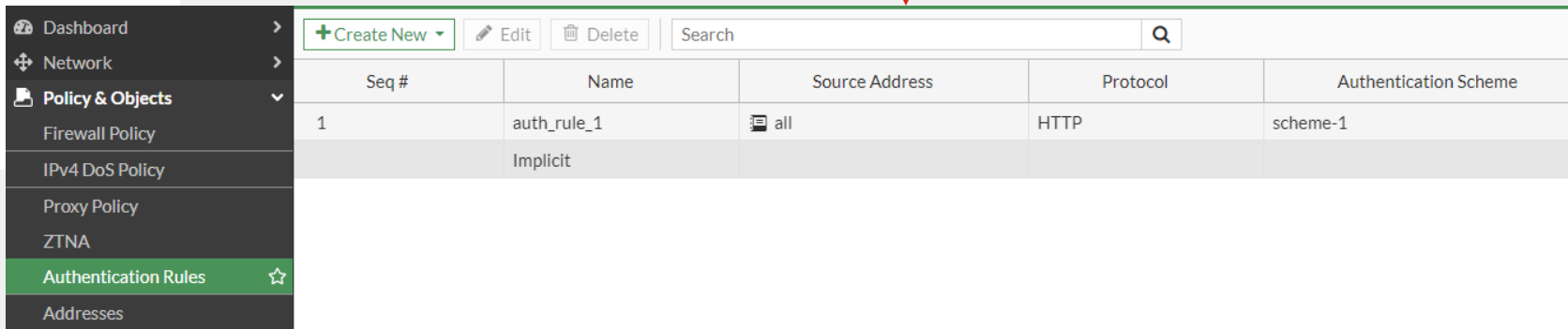
2、设置认证规则



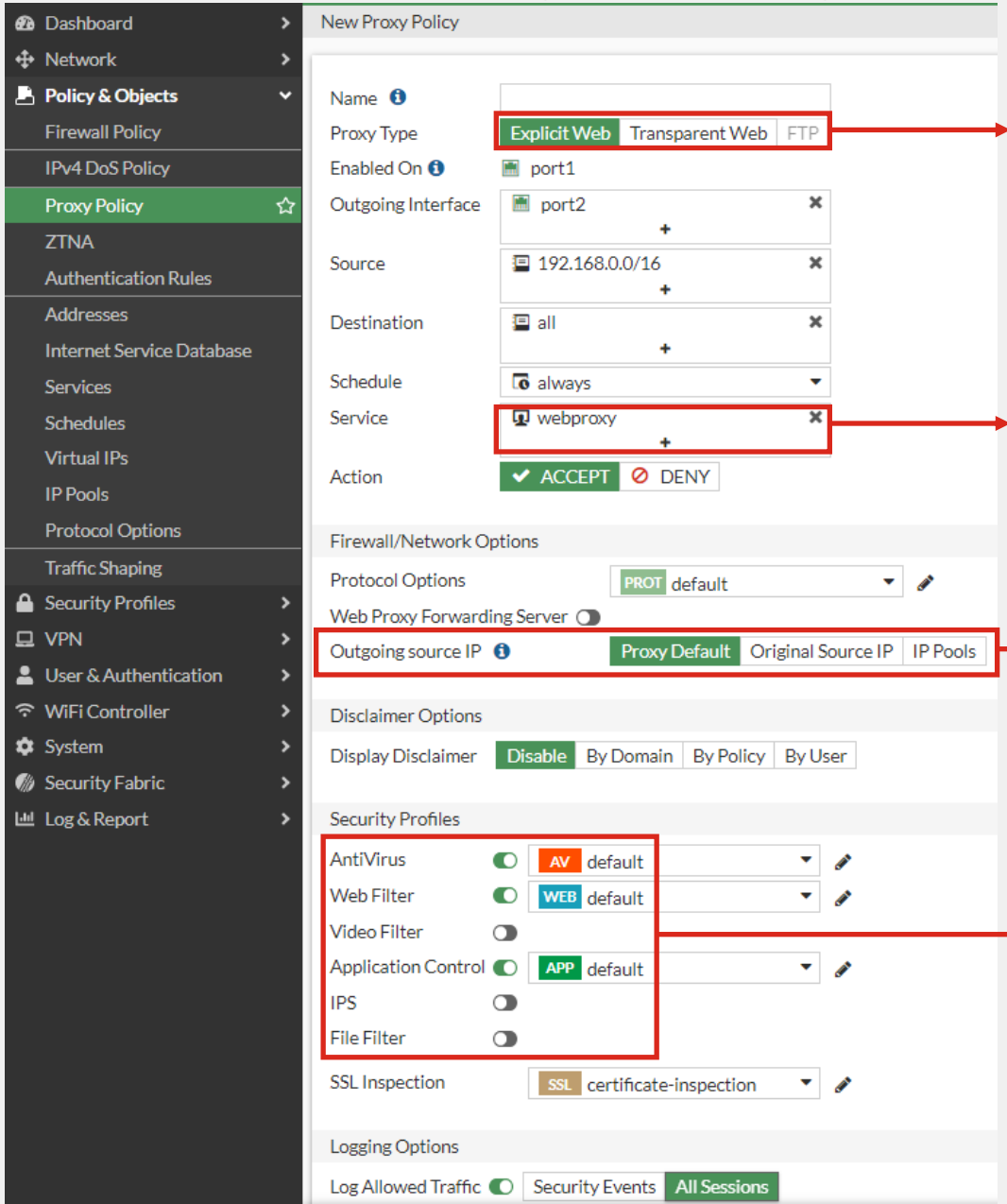
1、创建认证方案



3、设置完成



Proxy——设置Proxy Policy



Proxy类型默认为显示web代理，此方式在客户端需要手动设置代理网关，若选择透明代理，客户端网关指向FortiGate，则代理对用户无感，透明代理需要结合Firewall Policy

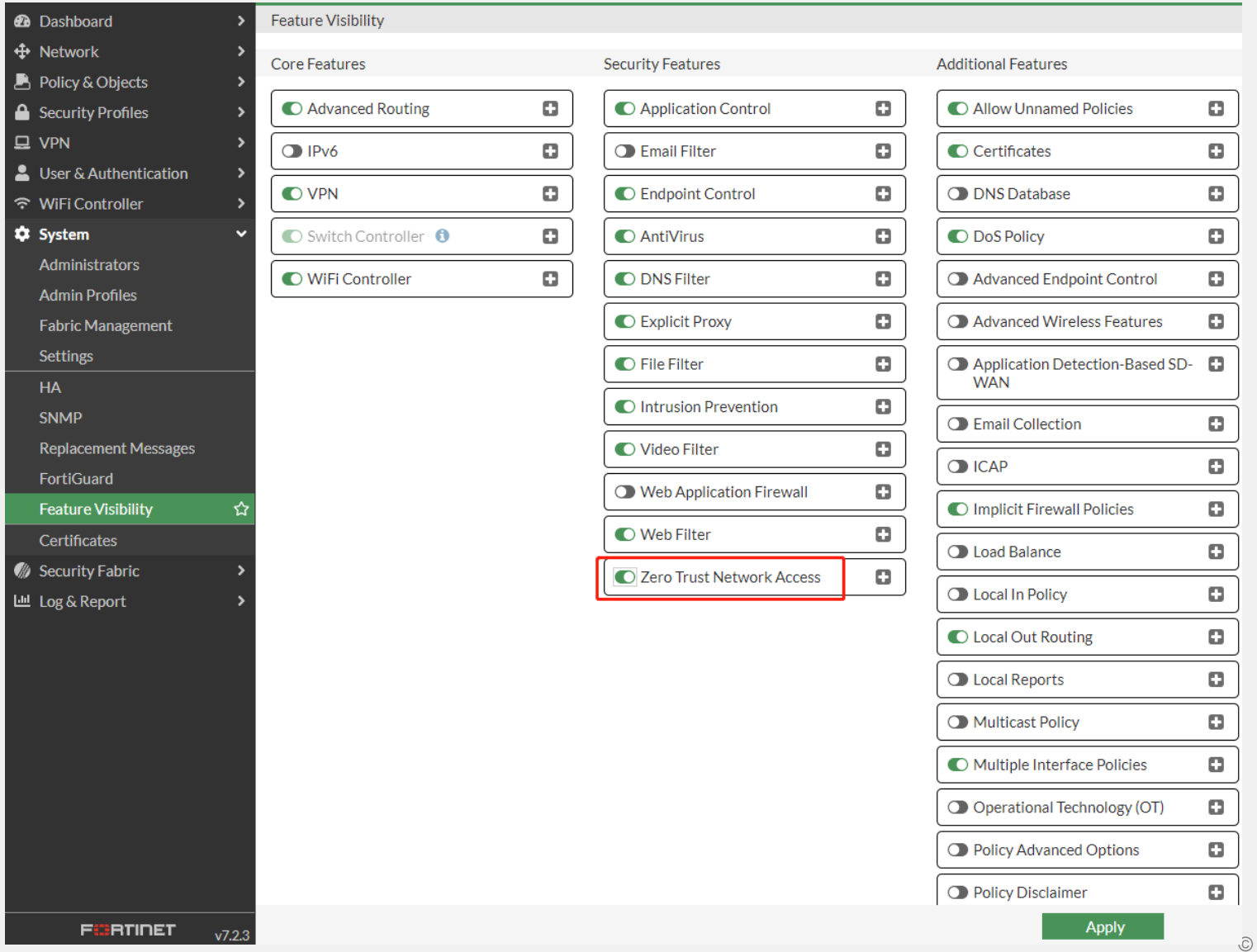
默认选项

设置代理流量从FortiGate以什么源IP出去

可设置security profile

ZTNA

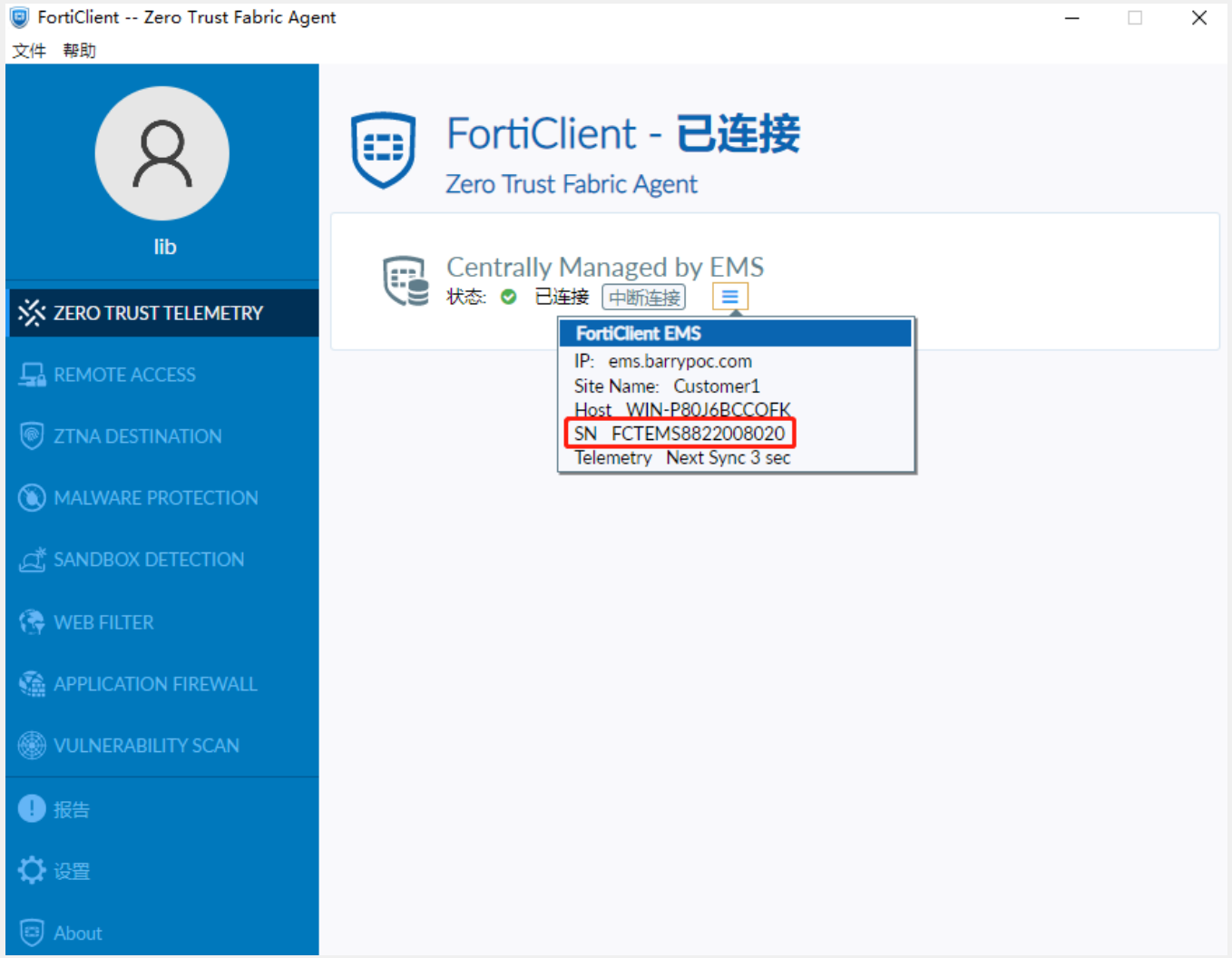
可在功能可见列表中开启**Zero Trust Network Access**功能

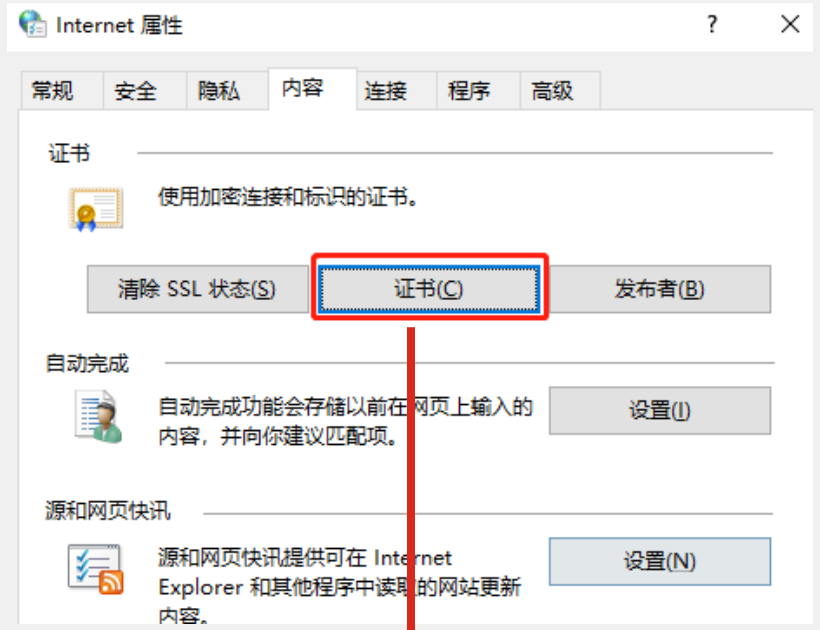


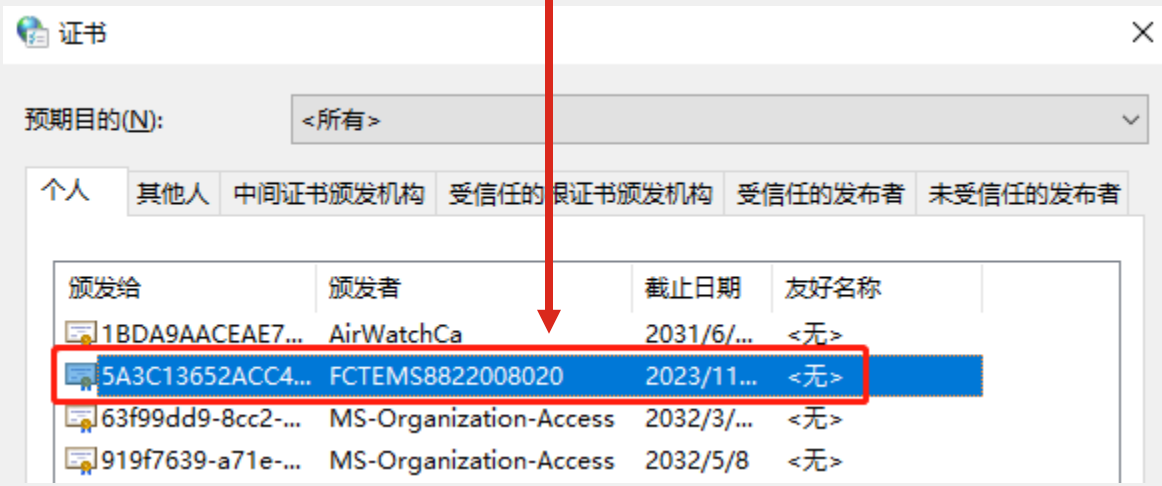
ZTNA规则简介

- 通过设置ZTNA Server及ZTNA规则，客户端在不需要拨VPN的情况下，也可以安全的连接企业内部应用；
- EMS会给每个FortiClient终端下发一张个人证书，该证书包含了FortiClient UID，客户端在发起ZTNA访问时，FortiGate将验证客户端证书及从EMS获取的其它终端信息，并授予终端相应访问权限；
- ZTNA Server有以下两种类型：
  - ✓ HTTP/HTTPS方式：在FortiGate配置HTTP/HTTPS方式的ZTNA Server及规则，FortiGate作为HTTP服务器的反向代理，客户端访问web服务器域名，域名解析为FortiGate设置的代理IP地址，FortiGate 代理连接并采取步骤对用户进行身份验证，它会提示用户在浏览器上确认他们的证书，并验证从 EMS 同步的 ZTNA 终端记录，如果通过，则允许流量基于在 ZTNA 规则上将网页返回给客户端。
  - ✓ TCP Forwarding方式：在FortiGate配置TCP Forwarding方式的ZTNA Server及规则，通过EMS将ZTNA规则下发至FortiClient，该规则指定了它想要到达的真实目标主机以及指向的代理网关（FortiGate），在客户端访问真实目标主机时，FortiClient会自动匹配该流量并与FortiGate建立HTTPS连接，FortiGate验证客户端证书并根据 ZTNA 规则授予访问权限；为了减少开销，您可以禁用在客户端访问代理加密，因为某些 TCP 协议（如 RDP）已经是安全的。

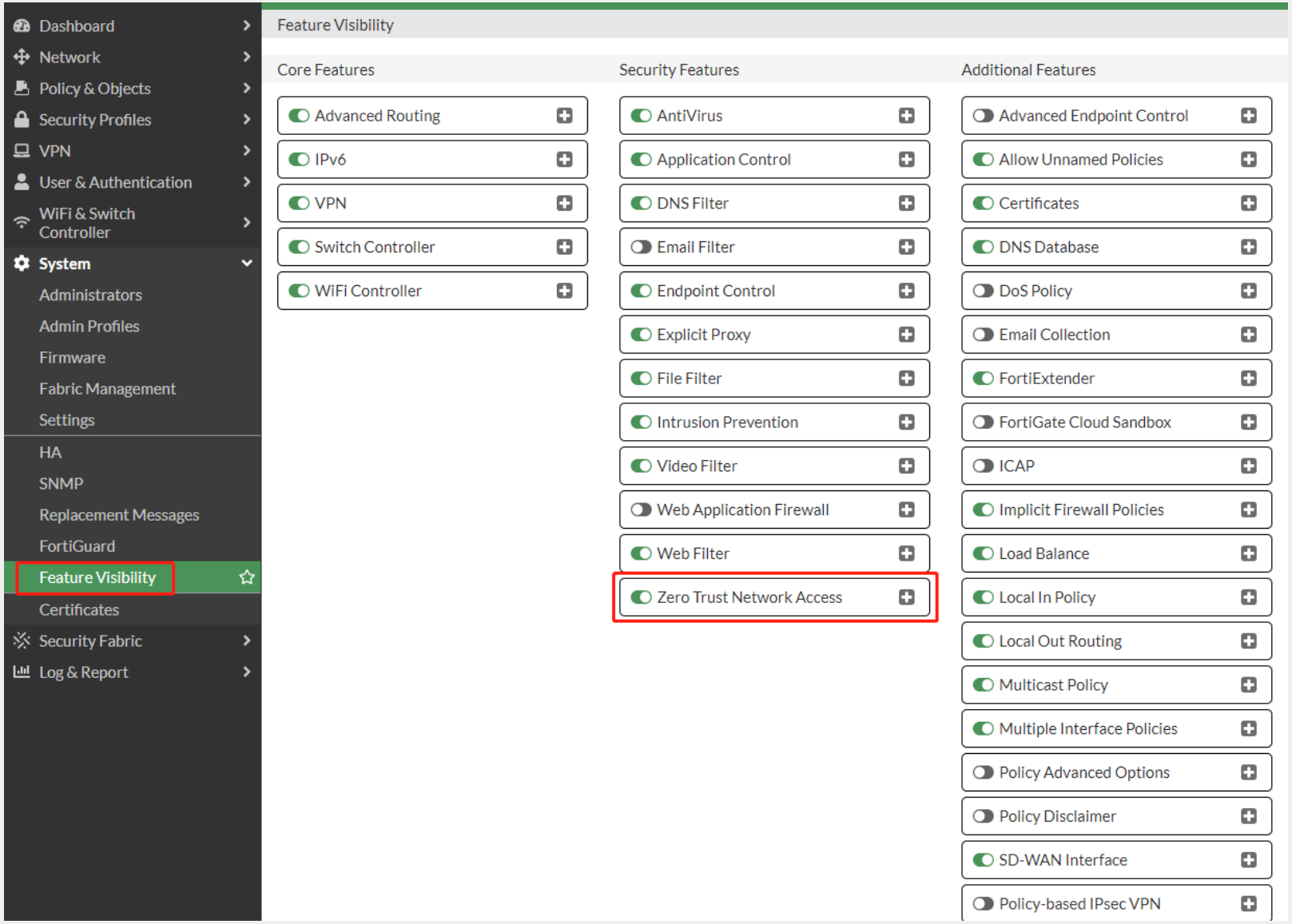
客户端证书查看



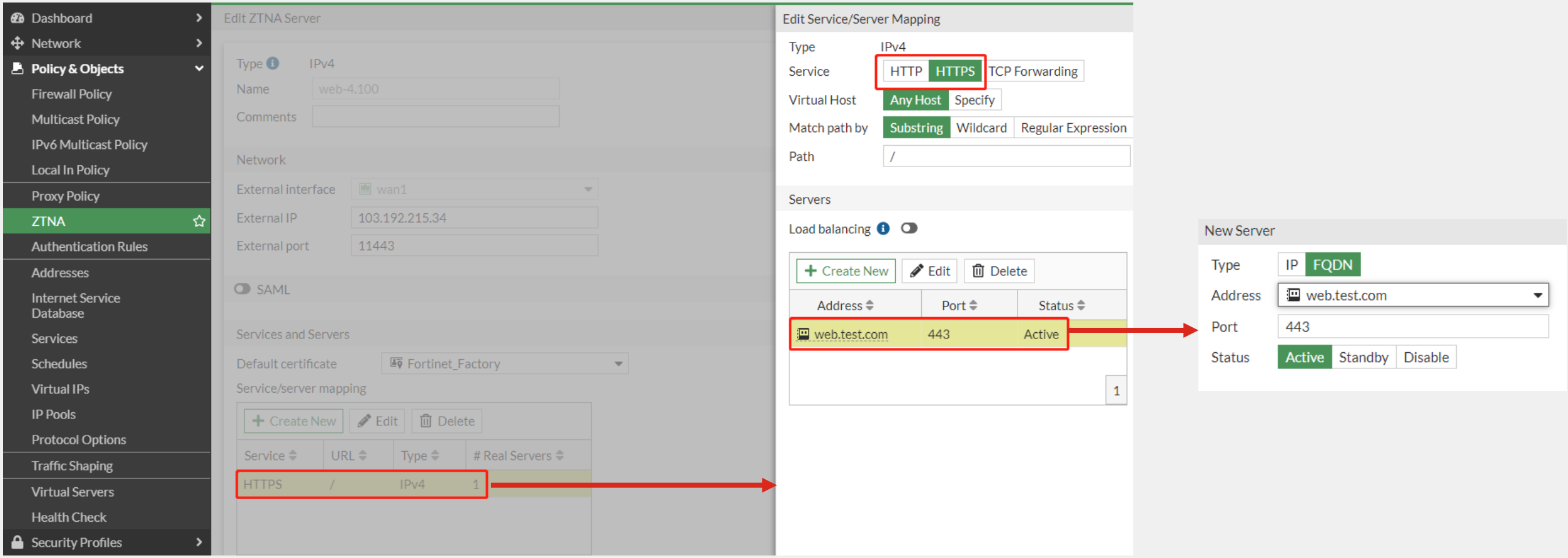




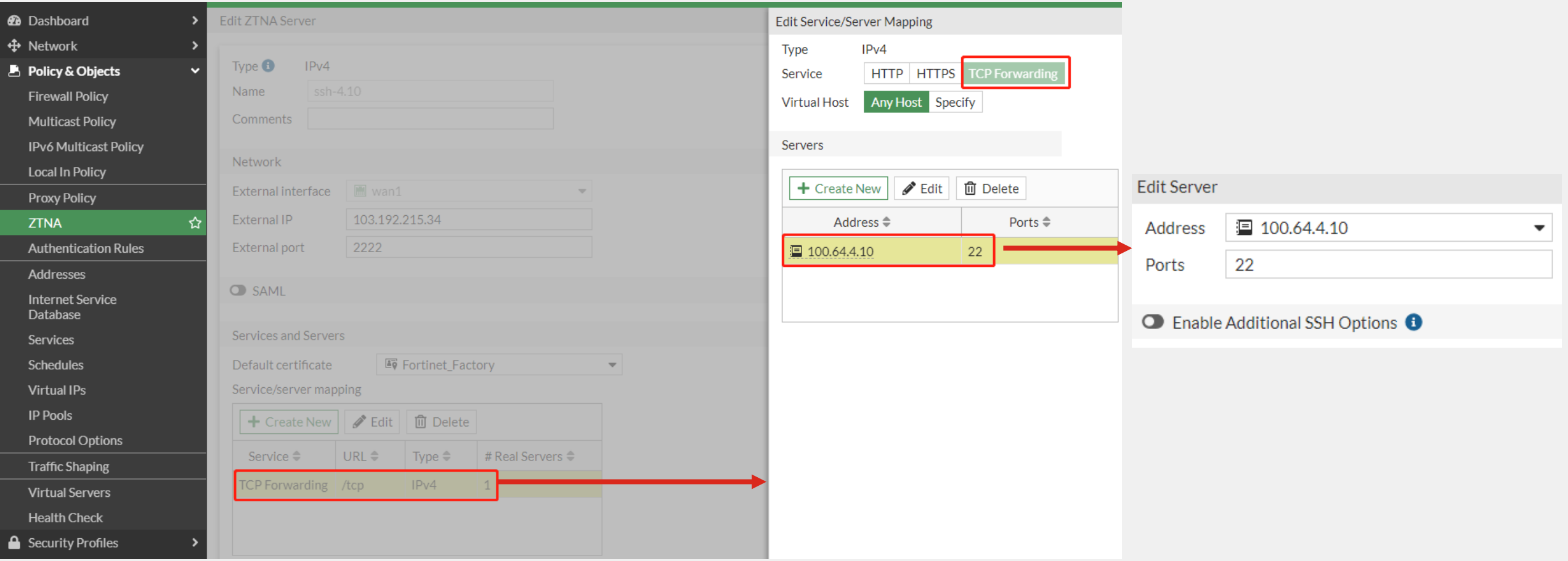
FortiGate上ZTNA功能显示开关



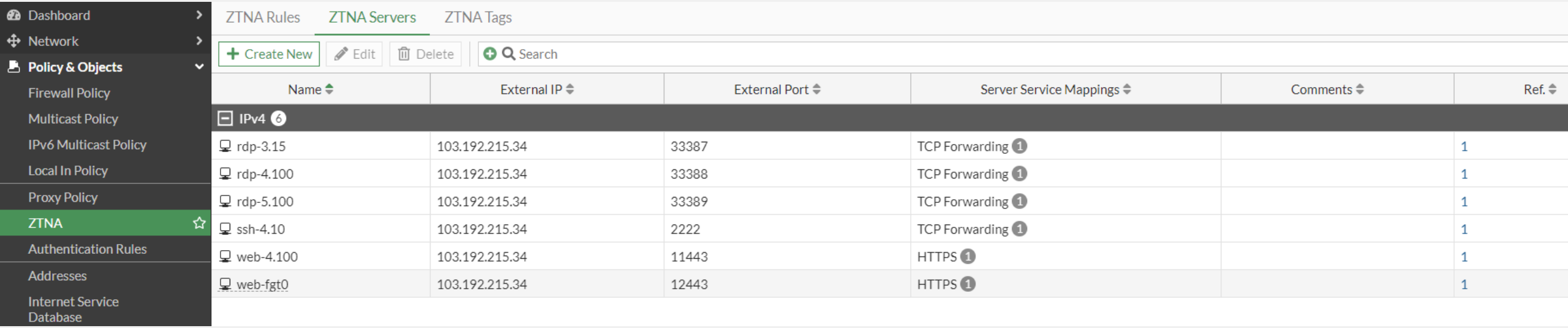
FortiGate配置ZTNA HTTP/HTTPS方式Server

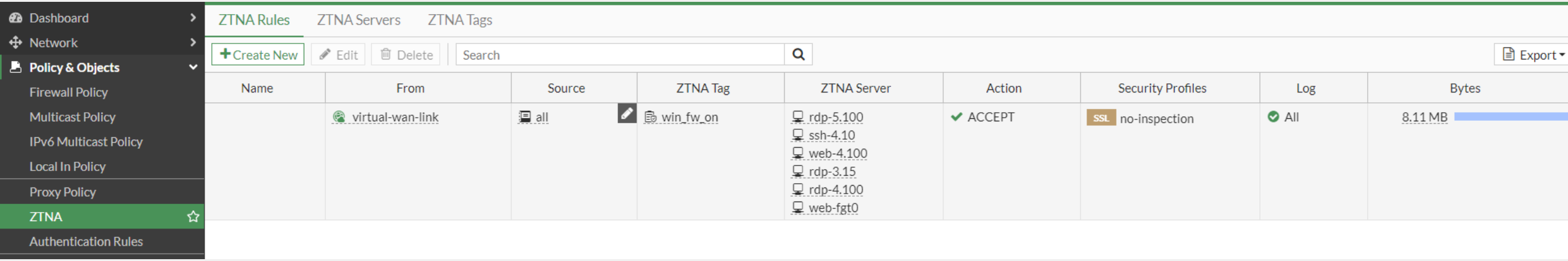


FortiGate配置ZTNA TCP Forwarding方式 Server



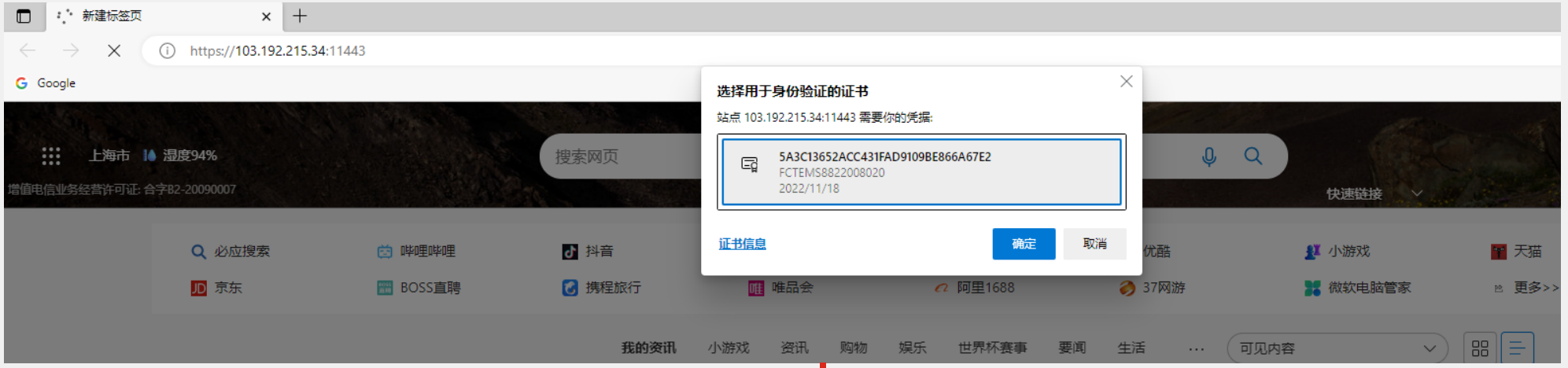
FortiGate配置

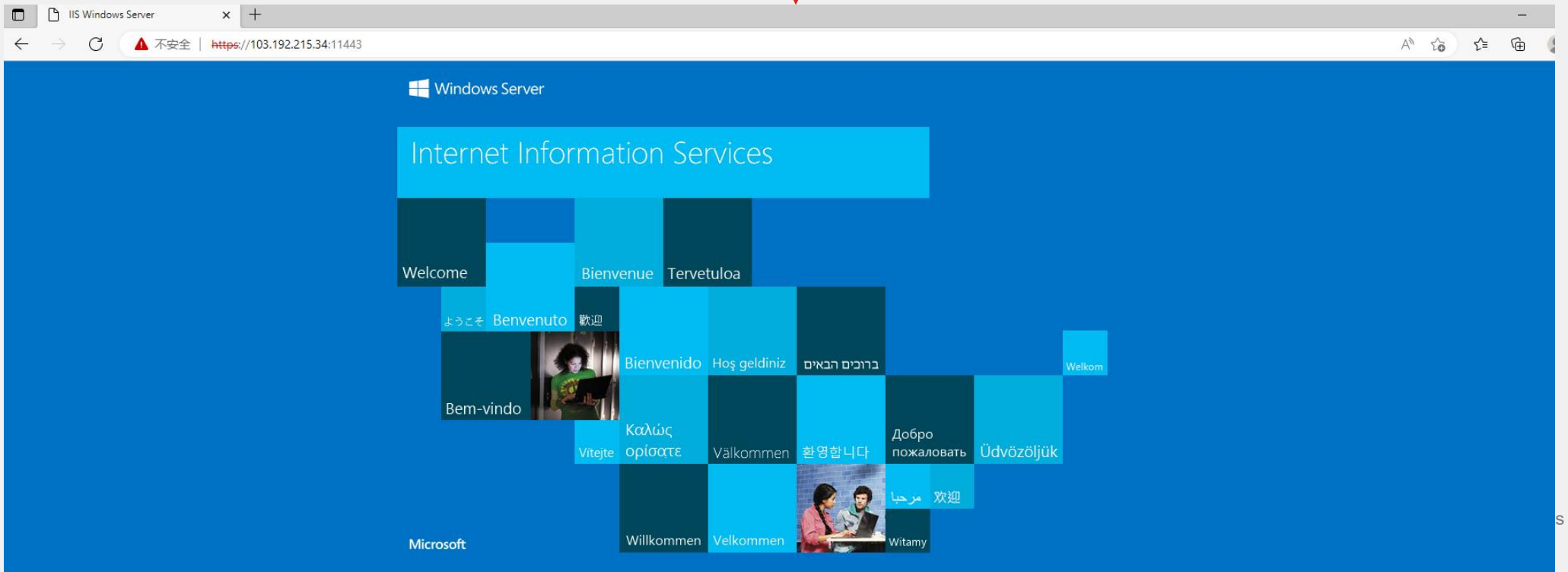




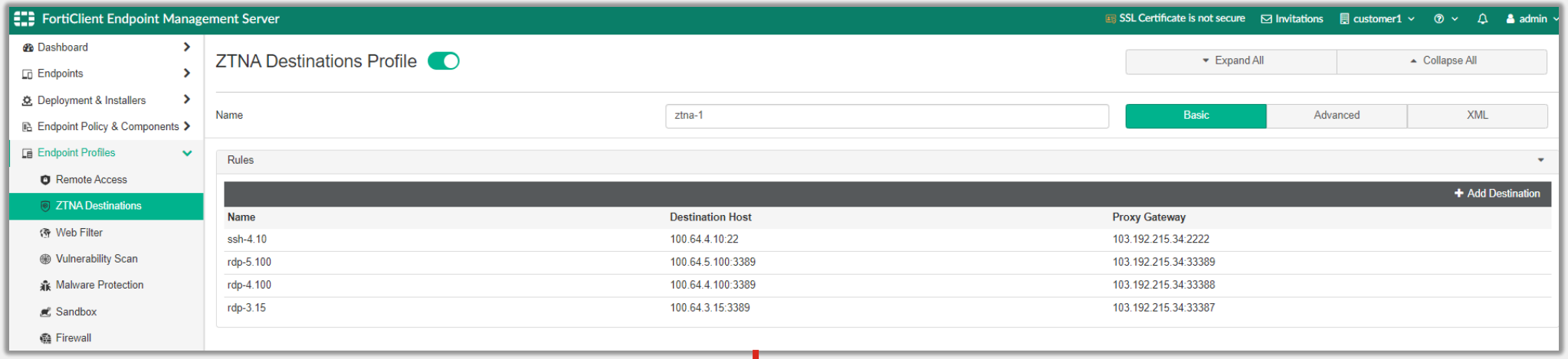
客户端访问ZTNA HTTP/HTTPS Server

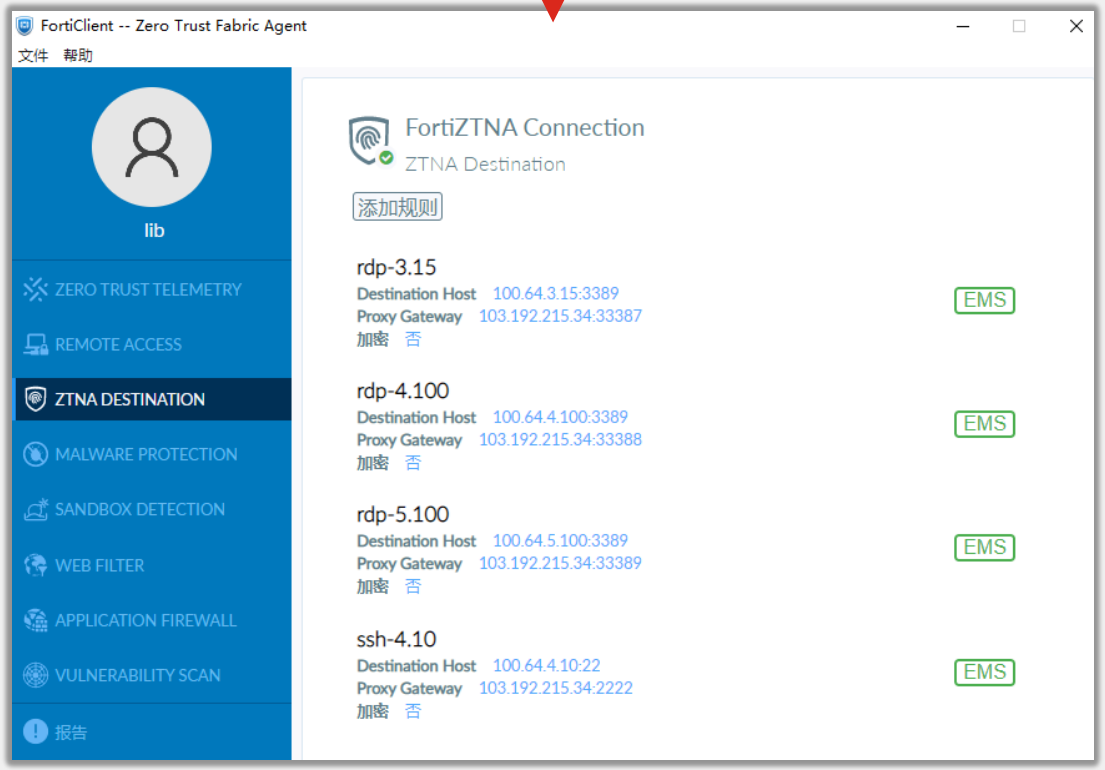
终端访问FortiGate的代理地址（域名的话需要将DNS A记录指向FortiGate上的代理IP），弹出证书选择，选择正确的证书认证通过后可正常访问后端服务





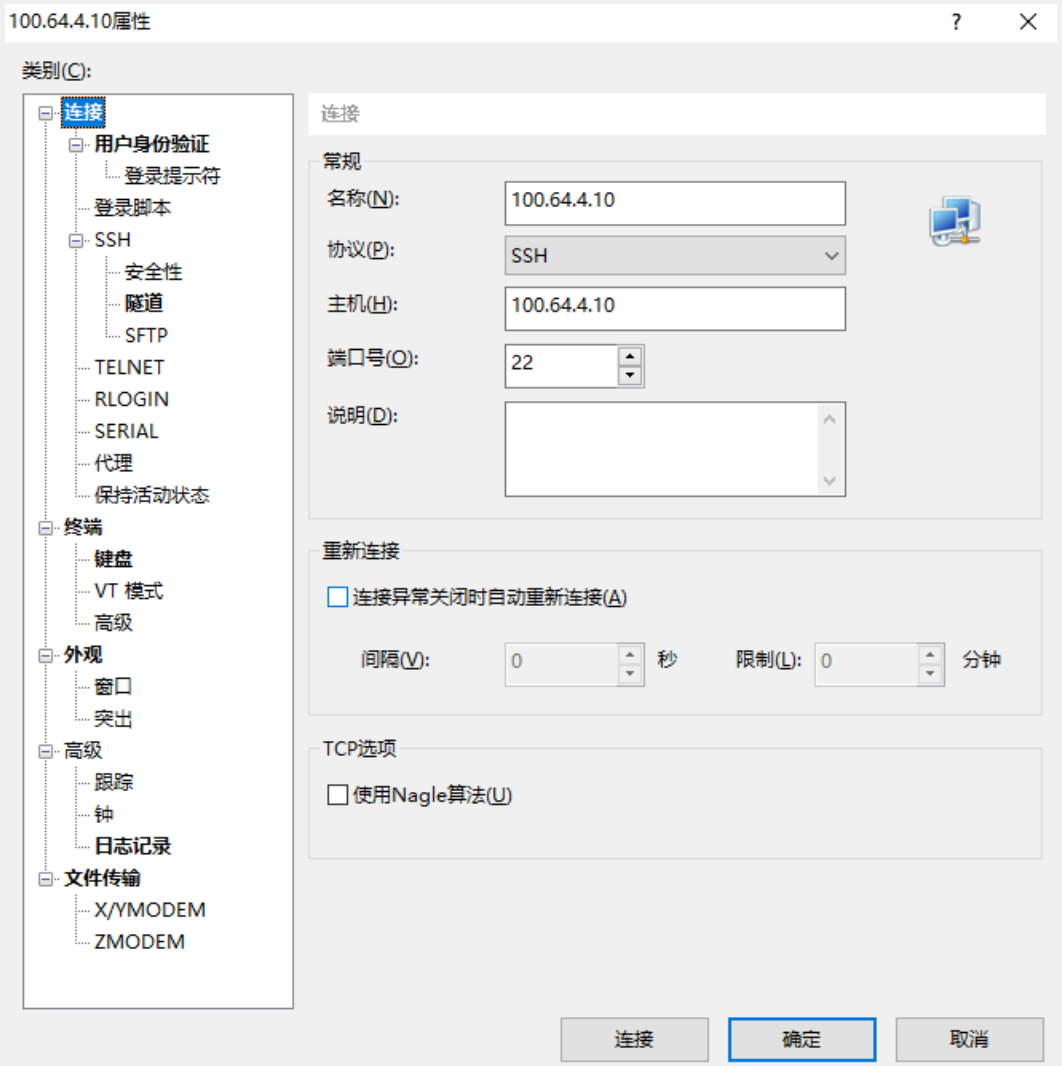
EMS上配置ZTNA TCP Forwarding规则，自动下发给FortiClient

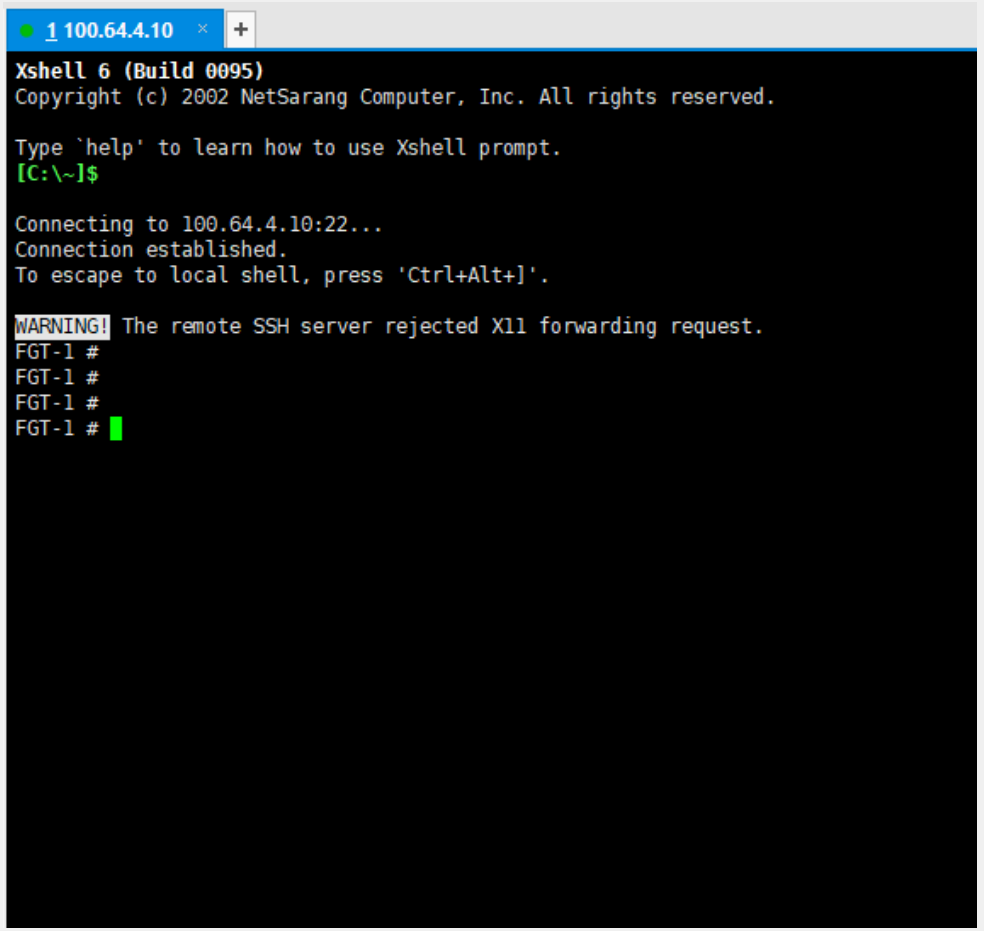




客户端访问ZTNA TCP Forwarding Server

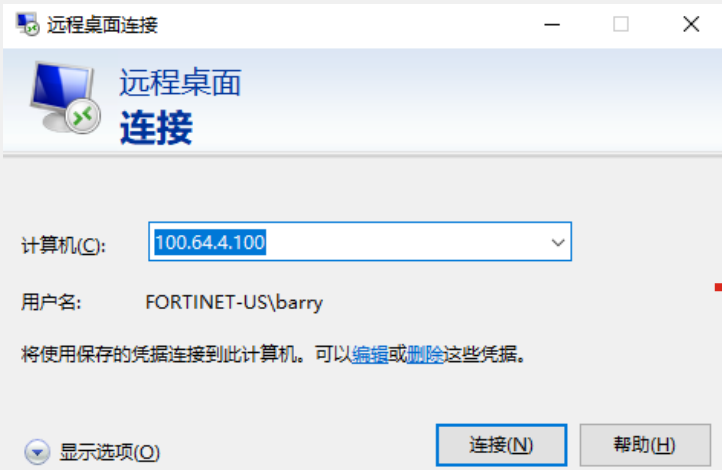
终端访问Destination Host（100.64.1.10），该地址位于企业内网，而终端处于外网，FortiClient通过ZTNA规则与Proxy Gateway建立隧道HTTPS隧道，通过FortiGate和100.64.1.10建立SSH连接

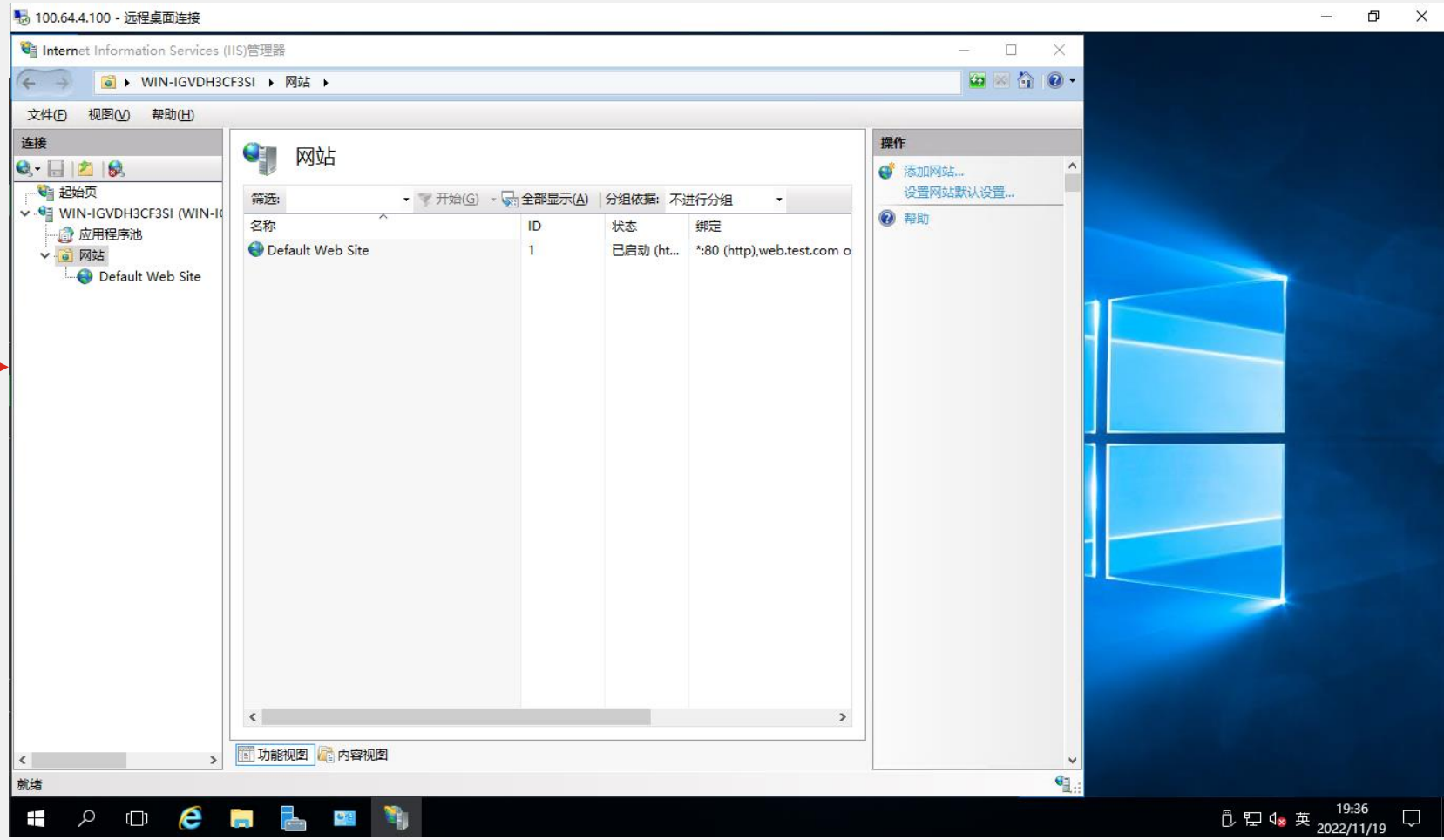




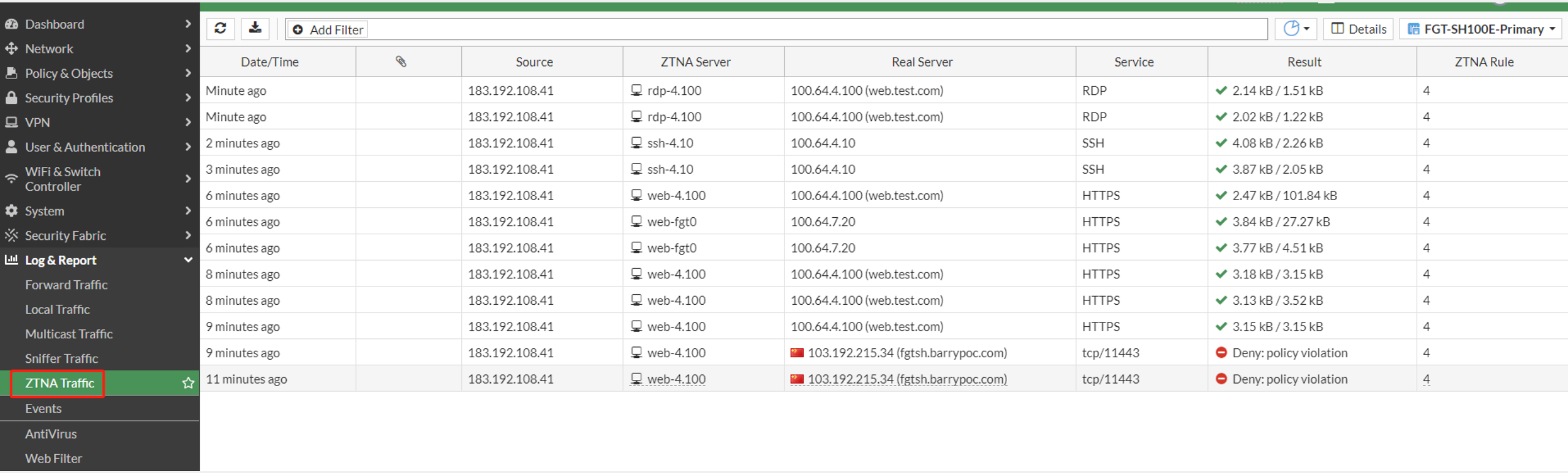
客户端访问ZTNA TCP Forwarding Server

终端访问Destination Host（100.64.4.100），该地址位于企业内网，而终端处于外网，FortiClient通过ZTNA规则与Proxy Gateway建立隧道HTTPS隧道，通过FortiGate和100.64.4.100建立远程桌面连接





FortiGate上ZTNA流量日志查看



Date/Time		Source	ZTNA Server	Real Server	Service	Result	ZTNA Rule
Minute ago		183.192.108.41	rdp-4.100	100.64.4.100 (web.test.com)	RDP	2.14 kB / 1.51 kB	4
Minute ago		183.192.108.41	rdp-4.100	100.64.4.100 (web.test.com)	RDP	2.02 kB / 1.22 kB	4
2 minutes ago		183.192.108.41	ssh-4.10	100.64.4.10	SSH	4.08 kB / 2.26 kB	4
3 minutes ago		183.192.108.41	ssh-4.10	100.64.4.10	SSH	3.87 kB / 2.05 kB	4
6 minutes ago		183.192.108.41	web-4.100	100.64.4.100 (web.test.com)	HTTPS	2.47 kB / 101.84 kB	4
6 minutes ago		183.192.108.41	web-fgt0	100.64.7.20	HTTPS	3.84 kB / 27.27 kB	4
6 minutes ago		183.192.108.41	web-fgt0	100.64.7.20	HTTPS	3.77 kB / 4.51 kB	4
8 minutes ago		183.192.108.41	web-4.100	100.64.4.100 (web.test.com)	HTTPS	3.18 kB / 3.15 kB	4
8 minutes ago		183.192.108.41	web-4.100	100.64.4.100 (web.test.com)	HTTPS	3.13 kB / 3.52 kB	4
9 minutes ago		183.192.108.41	web-4.100	100.64.4.100 (web.test.com)	HTTPS	3.15 kB / 3.15 kB	4
9 minutes ago		183.192.108.41	web-4.100	103.192.215.34 (fgtsh.barrypoc.com)	tcp/11443	Deny: policy violation	4
11 minutes ago		183.192.108.41	web-4.100	103.192.215.34 (fgtsh.barrypoc.com)	tcp/11443	Deny: policy violation	4

6、HA、VDOM等配置

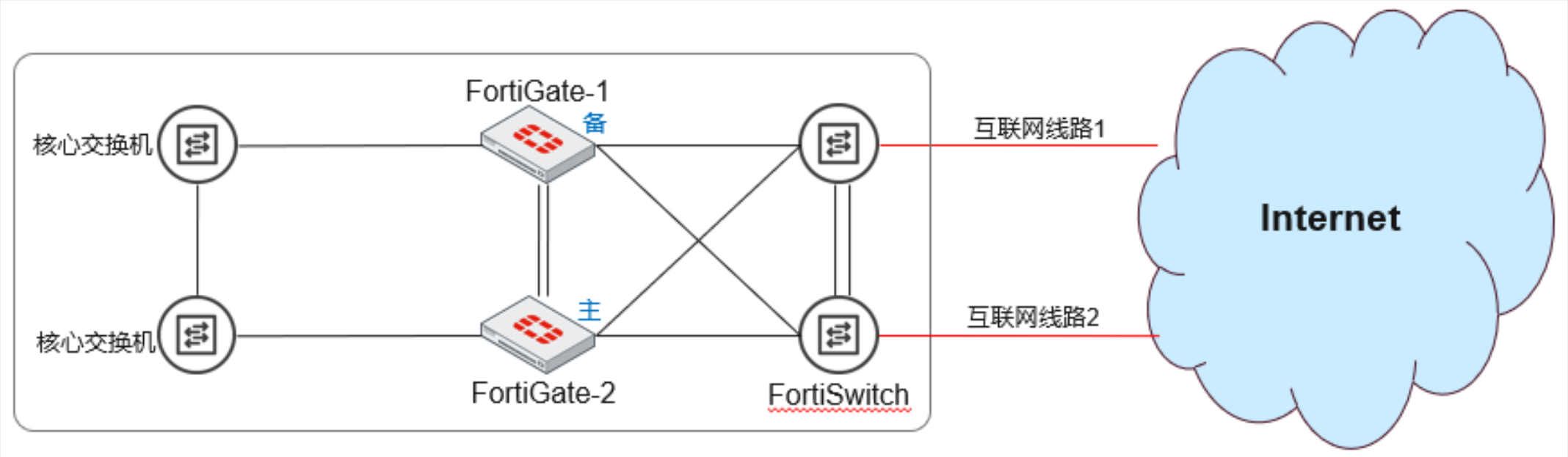
HA建立及切换条件

进行HA 的配置需满足如下要求：

1. 防火墙型号相同
2. 软件版本相同
3. 硬件配置相同（cpu,内存,硬盘等）

HA切换情况：

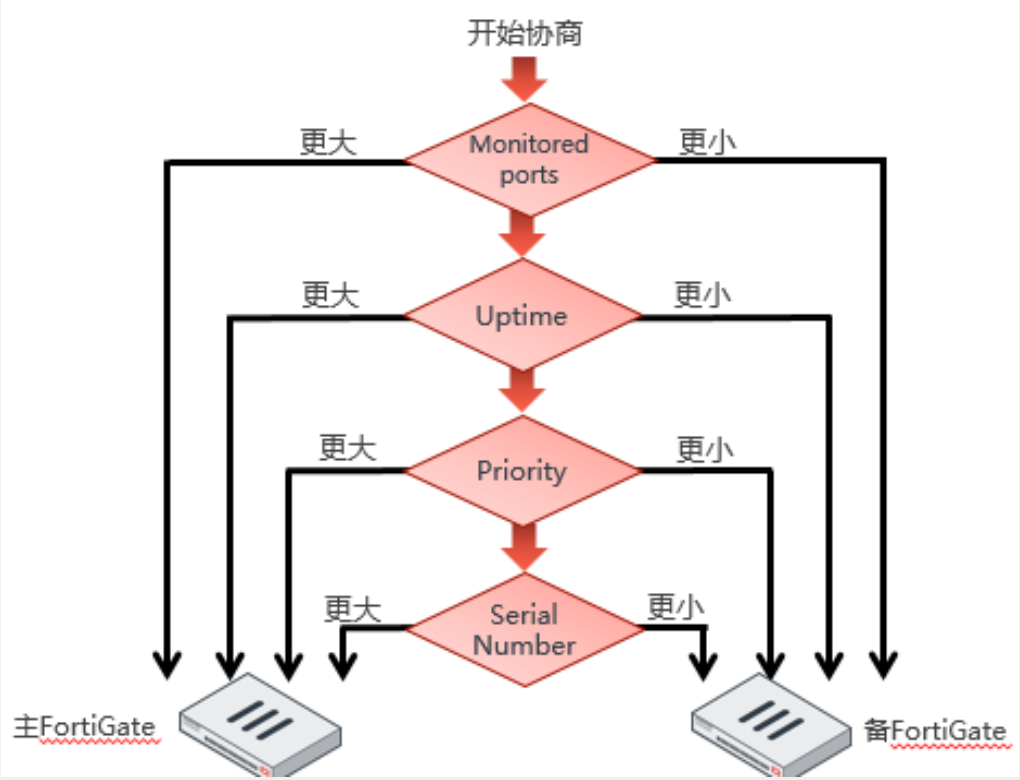
1. 链路中断（接口down，需要设置监听接口）
2. 设备掉电
3. 硬盘损坏
4. 内存使用率超过阈值一定时间（需要配置）



HA主备选举规则

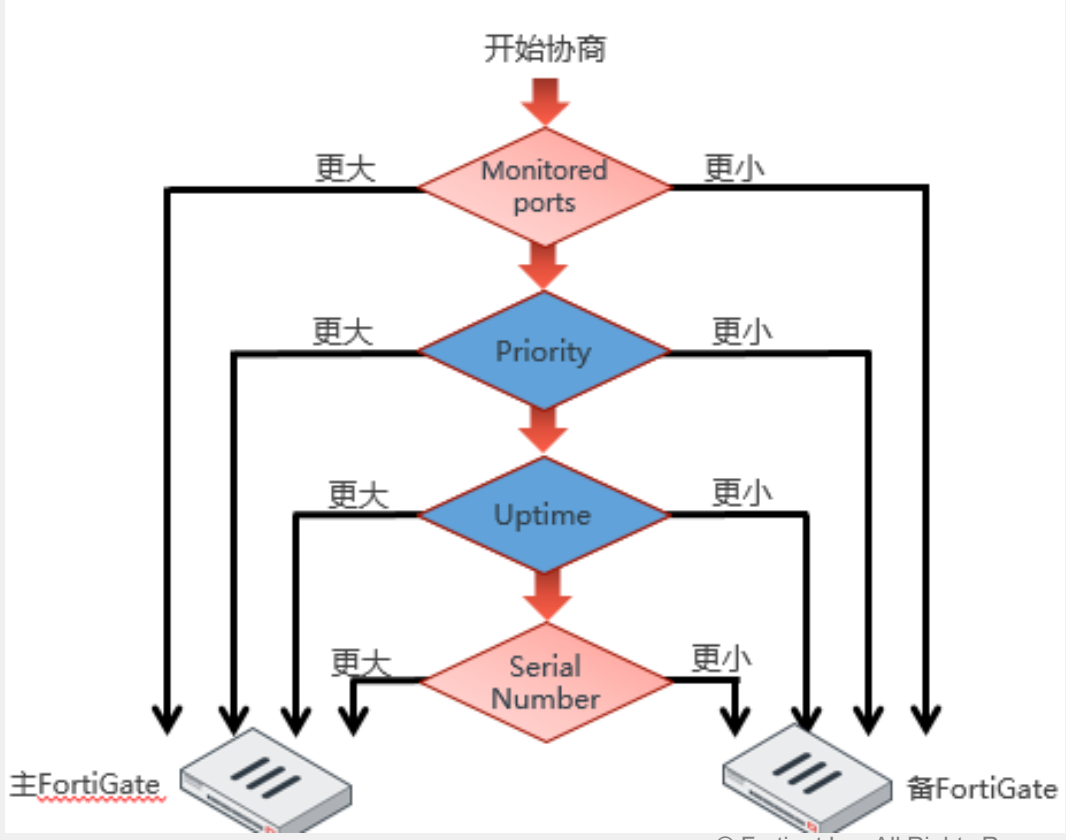
非抢占模式

- Override disabled (默认)
- 强制切换
  - diagnose sys ha reset-uptime



抢占模式

- Override enabled
  config system ha
  set override enable
  end
- 强制切换
  - 改变HA *priority*

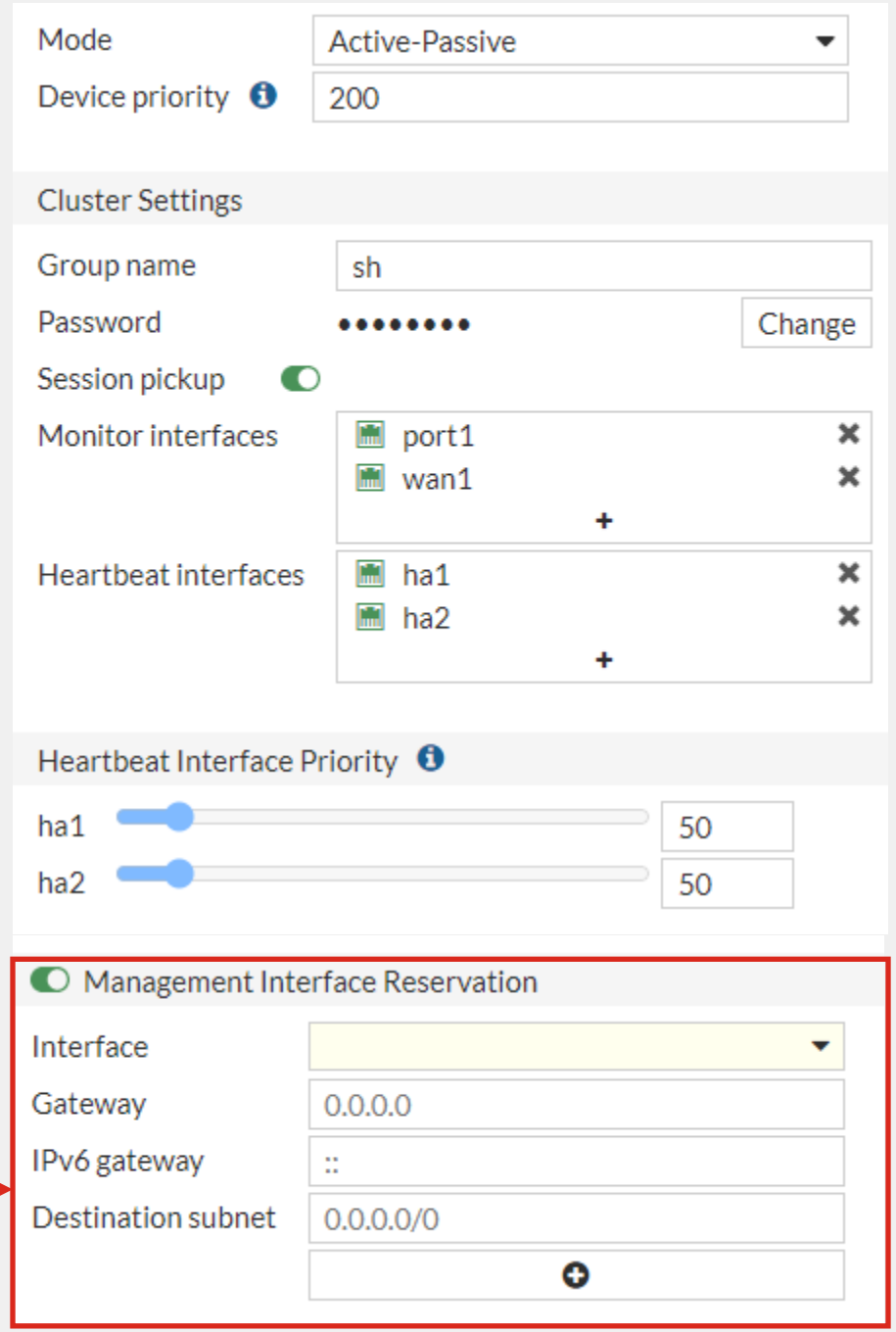


HA配置

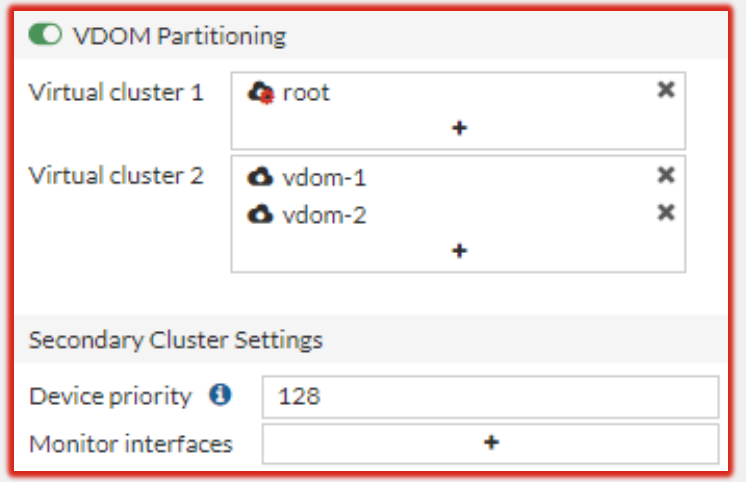
常用配置：

```
config system ha
    set group-id 1
    set group-name "sh"
    set mode a-p
    set password xxxxxx
    set hbdev "ha1" 50 "ha2" 50
    set session-sync-dev "ha2"
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1" "wan1"
end
```

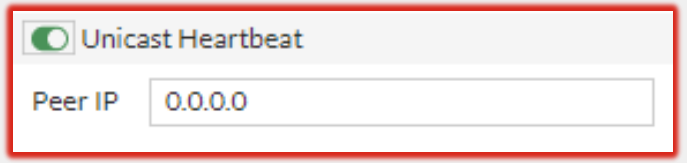
```
config system ha
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface port8
            set gateway 10.11.101.2
        next
    end
end
```



在多vdom的情况下，可根据需要设置多vdom的互为主备



云上部署的FGT需要用到单播进行心跳通信



HA配置——设置配置不同步等命令

硬件和虚机上可以设置以下配置不同步:

log.fortianalyzer.setting
log.fortianalyzer.override-setting
log.fortianalyzer2.setting
log.fortianalyzer2.override-setting
log.fortianalyzer3.setting
log.fortianalyzer3.override-setting
log.fortianalyzer-cloud.setting
log.fortianalyzer-cloud.override-setting
log.syslogd.setting
log.syslogd.override-setting
log.syslogd2.setting
log.syslogd2.override-setting
log.syslogd3.setting
log.syslogd3.override-setting
log.syslogd4.setting
log.syslogd4.override-setting
system.gre-tunnel
system.central-management
system.csf
user.radius

虚机上还可以设置以下配置不同步:

system.interface
vpn.ipsec.phase1-interface
vpn.ipsec.phase2-interface
router.bgp
router.route-map
router.prefix-list
firewall.ippool
firewall.ippool6
router.static
router.static6
firewall.vip
firewall.vip6
system.sdwan
system.saml
router.policy
router.policy6

配置示例:

```
config system vdom-exception
    edit 1
        set object system.interface
    next
    edit 2
        set object router.static
    next
end
```

通过主机命令行管理备机命令:
exe ha manage (id) admin

查看ha状态命令:
get system ha status

HA配置——设置配置不同步

硬件和虚机上可以设置以下配置不同步:

log.fortianalyzer.setting
log.fortianalyzer.override-setting
log.fortianalyzer2.setting
log.fortianalyzer2.override-setting
log.fortianalyzer3.setting
log.fortianalyzer3.override-setting
log.fortianalyzer-cloud.setting
log.fortianalyzer-cloud.override-setting
log.syslogd.setting
log.syslogd.override-setting
log.syslogd2.setting
log.syslogd2.override-setting
log.syslogd3.setting
log.syslogd3.override-setting
log.syslogd4.setting
log.syslogd4.override-setting
system.gre-tunnel
system.central-management
system.csf
user.radius

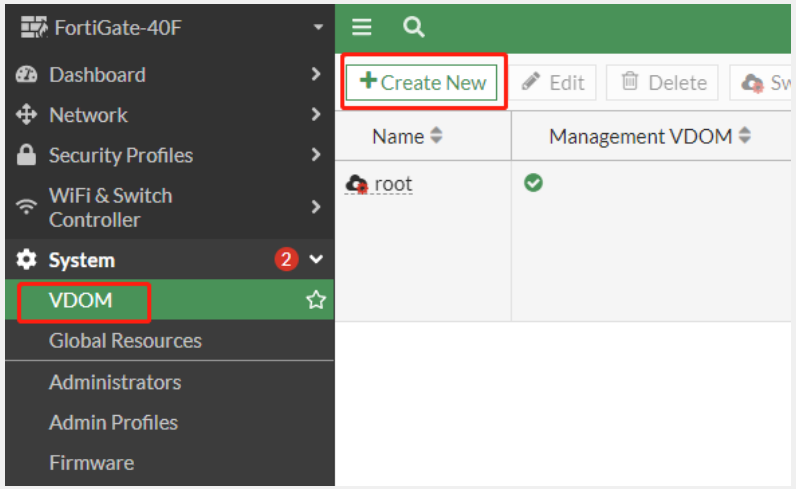
虚机上还可以设置以下配置不同步:

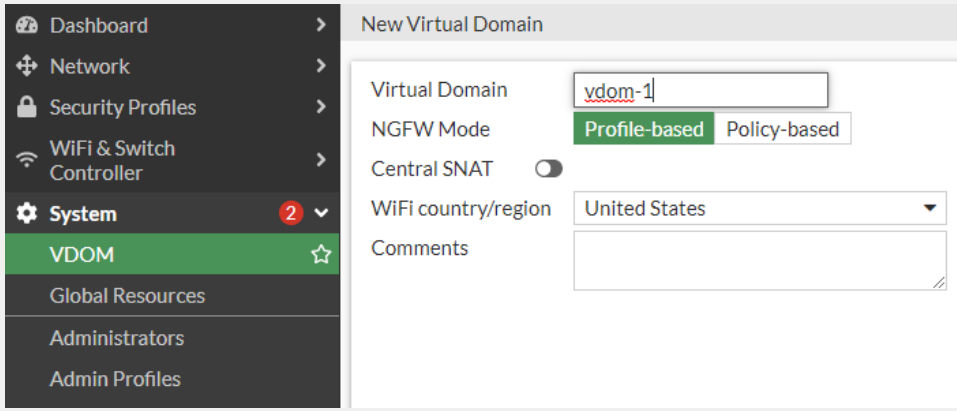
system.interface
vpn.ipsec.phase1-interface
vpn.ipsec.phase2-interface
router.bgp
router.route-map
router.prefix-list
firewall.ippool
firewall.ippool6
router.static
router.static6
firewall.vip
firewall.vip6
system.sdwan
system.saml
router.policy
router.policy6

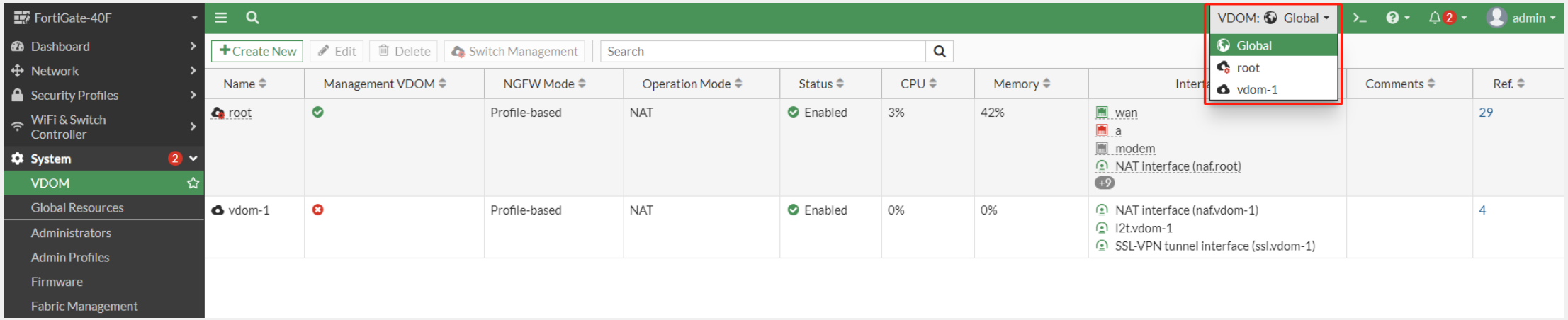
VDOM配置

CLI Console (1)

```
FortiGate-40F # config sys global

FortiGate-40F (global) # set vdom-mode
no-vdom       Disable split/multiple VDOMs mode.
split-vdom    Enable split VDOMs mode.
multi-vdom    Enable multiple VDOMs mode.

FortiGate-40F (global) # set vdom-mode multi-vdom

FortiGate-40F (global) # end
You will be logged out for the operation to take effect.
Do you want to continue? (y/n)
```







7、常用排错命令

常用排错命令

```
# get system status                          //查看系统状态
# get router info routing-table all          //查看路由表
# get system arp                             //查看ARP表
# diagnose ip address list                   //查看接口IP list
# get system performance status              //查看设备运行性能状态（CPU/MEM/新建/并发）
# get system performance top                 //查看系统允许top进程
```

Ping: exe ping-option source x.x.x.x

exe ping x.x.x.x

Traceroute: exe traceroute-option source x.x.x.x

exe traceroute x.x.x.x

diagnose debug application <程序><Debug level>

例：Diagnose debug application sslvpn -1

Diagnose debug enable

查看会话信息

diagnose system session filter (过滤条件)

Diagnose system session list

查看接口错包以及接口MAC地址：

diagnose netlink device list

get hardware nic wan1

常用排错命令

Sniffer 常用抓包命令

```
diagnose sniffer packet port1 “host 172.16.1.100” 1                          //抓port1上172.16.1.100的包
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 172.16.1.100 or host 172.16.1.101 and port 1701” 4    //and和or组合
diagnose sniffer packet internal "tcp[13]&2!=0 and port 23" 4                          //SYN置位包
diagnose sniffer packet internal "tcp[13]&4!=0" 4                                     //RST置位
diagnose sniffer packet internal "net 4.2.2.0/24" 4                                  //抓某一网段的包
diagnose sniffer packet internal "(ether[6:4]=0x00090f89) and (ether[10:2]=0x10ea)“ //根据MAC源地址抓包
diagnose sniffer packet any "ip[2:2] > 1500" 4                                      //观察大于1500的帧
```

如果以上命令都无法满足抓包过滤要求，可参考tcpdump命令的语法！

有道在线笔记会不定期更新
https://note.youdao.com/ynoteshare/index.html?id=e9d0c97cce36b87069536d819567c789&type=note&_time=1672059461019

Fortinet资源链接

Fortinet资源链接

FORTINET知识库	https://community.fortinet.com
FORTINET文档中心	https://docs.fortinet.com
FORTINET(中国)官方网站	https://www.fortinet.com/cn
FORTINET(全球)技术支持	https://support.fortinet.com
FORTINET(中国)合作伙伴	https://partnerportal.fortinet.com
FORTINET 配置视频指导	https://video.fortinet.com
FORTINET博客	https://blog.fortinet.com
FORTIGUARD中心	http://www.fortiguard.com
FORTINET培训与认证	http://www.fortinet.com/training
FortiGate实施一本通	https://handbook.fortinet.com.cn/


FORTINET