FortiWAN 如何与 FortiGate 建立 IPsec VPN

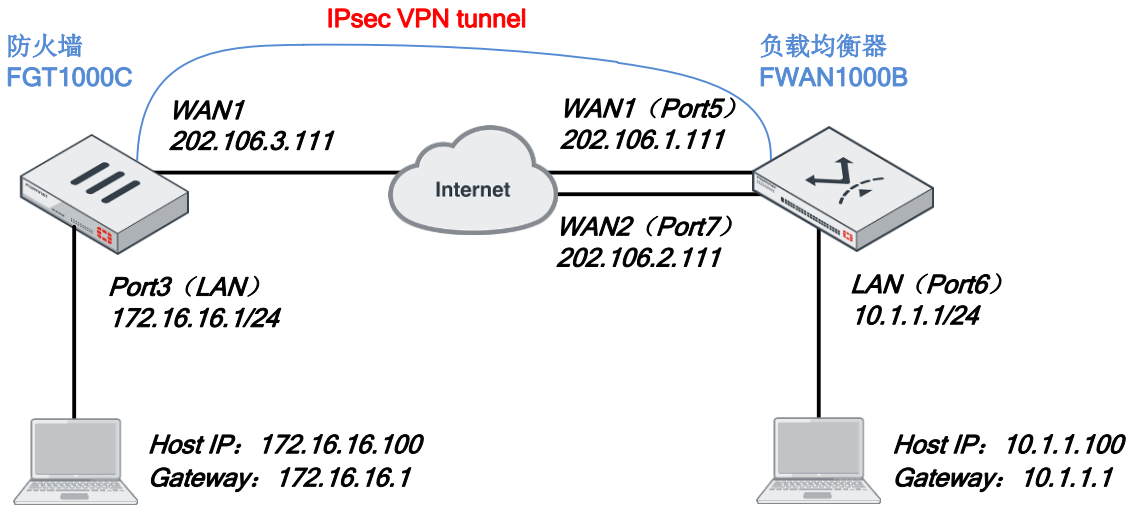
版本	1.0
时间	2017 年 9 月 1 日星期五
支持的版本	FortiWAN v4.4.1/FortiGate v5.4.5
作者	刘康明
状态	已审核
反馈	support_cn@fortinet.com

目录

简介

FortiWAN 设备的 IPsec VPN 使用起来和 FortiGate 有很多不一样的地方，在配置 FortiWAN 的 IPsec VPN 的时候可能会遇到一些思路上的问题，本文将针对 FortiWAN 与 FortiGate 建立一次 IPsec VPN，让大家熟悉一下二者 IPsec VPN 配置上的区别。

环境拓扑图



FortiGate V5.4.5

WAN1 WAN Port 202.106.3.111 GW:202.106.3.2
Port3 LAN Port 172.16.16.1/24
测试 PC：172.16.16.100

FortiWAN V4.4.1

Port5 WAN1 Port 202.106.1.111 GW：202.106.1.2
Port7 WAN2 Port 202.106.2.111 GW：202.106.2.2
Port6 LAN Port 10.1.1.1/24
测试 PC:10.1.1.100

FGT1000C----------IPsec Tunnel----------FWN1000B
WAN1（202.106.3.111） WAN1（202.106.1.111）

FortiGate1000C IPsec VPN 配置

✓ IPsec VPN 第一阶段配置

```
config vpn ipsec phase1-interface
    edit "TO-FWN"
        set interface "wan1"
        set peertype any
        set proposal aes256-sha256
        set dhgrp 5
        set remote-gw 202.106.1.111
        set psksecret FortiNet
    next
end
```

✓ IPsec VPN 第二阶段配置

```
config vpn ipsec phase2-interface
    edit "TO-FWN"
        set phase1name "TO-FWN"
        set proposal aes256-sha256
        set dhgrp 5
        set auto-negotiate enable
        set src-subnet 172.16.16.0 255.255.255.0
        set dst-subnet 10.1.1.0 255.255.255.0
    next
end
```

✓ 策略配置

```
config firewall policy
    edit 2
        set name "VPN-IN"
        set srcintf "TO-FWN"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "VPN-OUT"
        set srcintf "port3"
        set dstintf "TO-FWN"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

Seq.#	Name	源	目的	源	目的地址	时间表	服务	动作	NAT
2	VPN-IN	TO-FWN	LAN (port3)	all	all	always	ALL	ACCEPT	已禁用
3	VPN-OUT	LAN (port3)	TO-FWN	all	all	always	ALL	ACCEPT	已禁用

✓ 路由配置

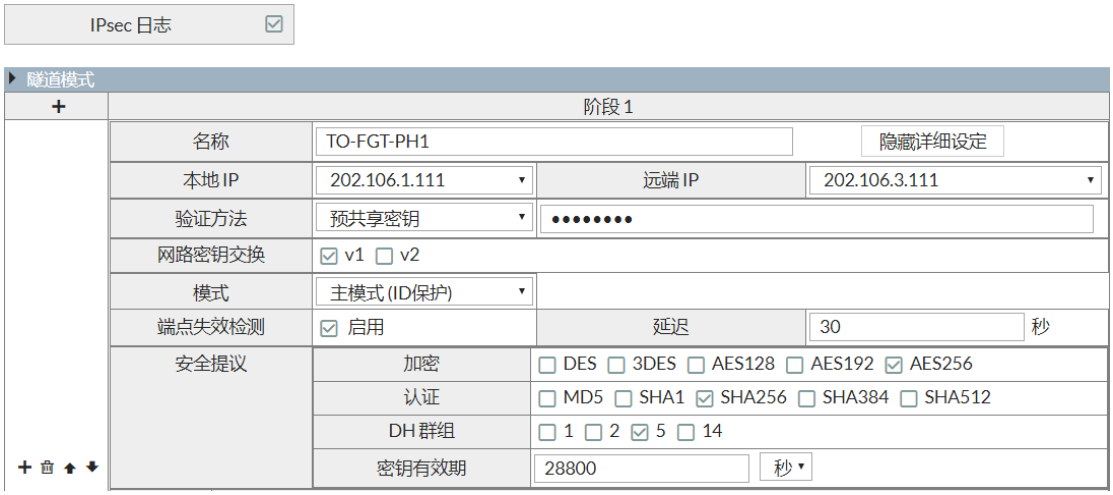
```
config router static
    edit 2
        set dst 10.1.1.0 255.255.255.0
        set device "TO-FWN"
    next
    edit 3
        set dst 10.1.1.0 255.255.255.0
        set distance 254
        set blackhole enable
    next
end
```

新建 | 编辑 | 克隆 | 删除

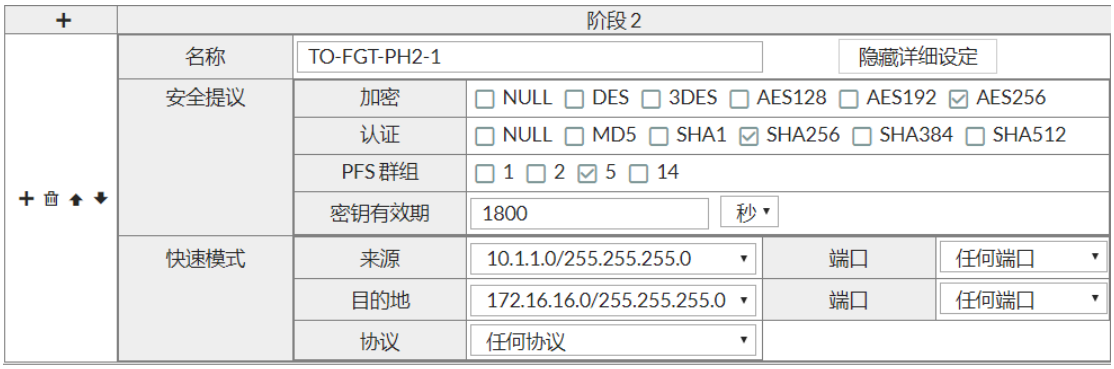
目标地址	网关	接口
0.0.0.0/0	202.106.3.2	wan1
10.1.1.0/24		TO-FWN
10.1.1.0/24		无(黑洞)

FortiWAN1000B IPsec VPN 配置

✓ IPsec VPN 第一阶段配置



✓ IPsec VPN 第二阶段配置

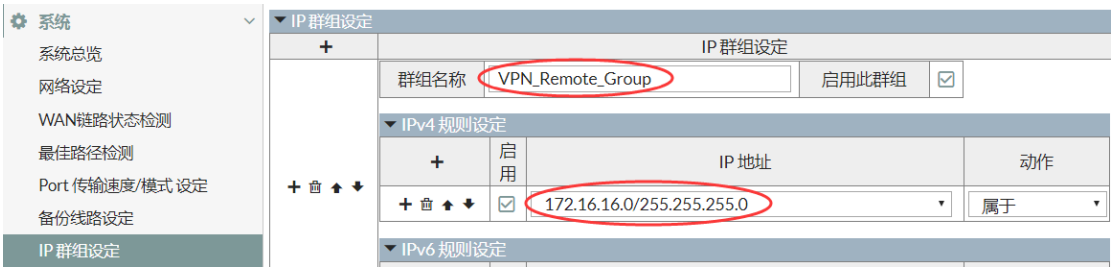


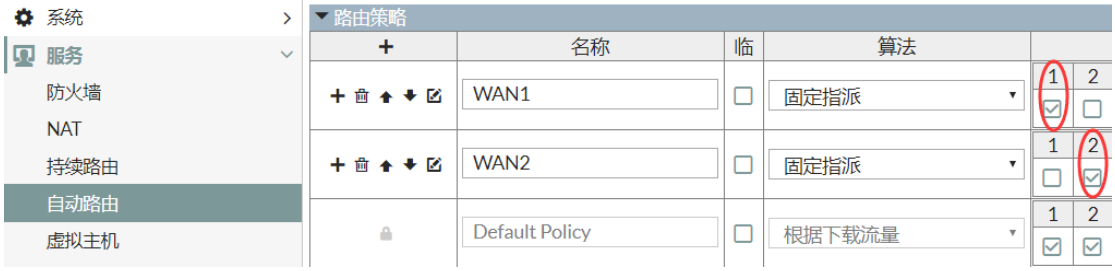
命令行：

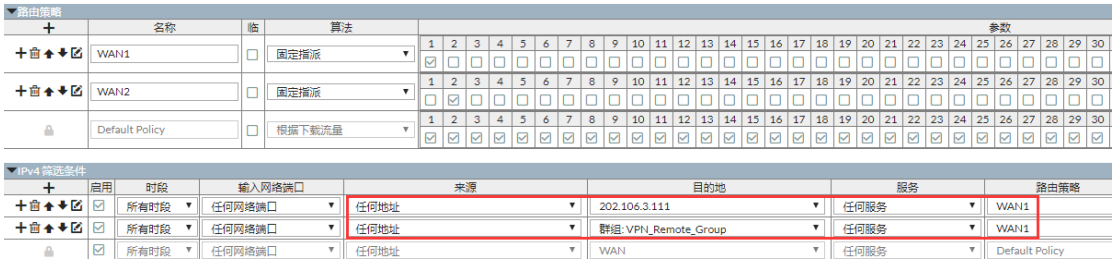
```
ipsec {
log 1
tunnel {
    p1-rule-array {
        rule { # 1
            name TO-FGT-PH1
            local 202.106.1.111
            remote 202.106.3.111
```

```
                method {
                    password RVhNemR5TmxOPUlI
                }
                dpd {
                    enable 1
                }
                proposal {
                    encryption aes256
                    authentication sha256
                }
                p2-rule-array {
                    rule { # 1
                        name TO-FGT-PH2-1
                        proposal {
                            encryption aes256
                            authentication sha256
                        }
                        quick-mode {
                            source {
                                ip 10.1.1.0/255.255.255.0
                            }
                            destination {
                                ip 172.16.16.0/255.255.255.0
                            }
                        }
                    }
                }
            }
        }
    }
    }
```

✓ 自动路由将 202.106.3.111/32&172.16.16.0/24 强制指向 WAN1







命令行：

```
ip-group {
group-array {
    group { # 1
        name VPN_Remote_Group
        rule-array {
            rule { # 1
                ip 172.16.16.0/255.255.255.0
            }
        }
    }
}
}
auto-routing {
policy-array {
    policy { # 1
        label WAN1
        algorithm Fixed
        parameter 1
    }
    policy { # 2
        label WAN2
        algorithm Fixed
        parameter 2
    }
}
filter-array {
    filter { # 1
        destination 202.106.3.111
```

```
            routing-policy WAN1
        }
        filter { # 2
            destination Group:VPN_Remote_Group
            routing-policy WAN1
        }
    }
}
```

✓ WAN1 的 NAT 排除掉 IPsec VPN 的感兴趣流，既针对去往 172.16.16.0/24 的流量不做 SNAT

命令行：

```
    nat {
    wan-array {
        wan@1 {
            rule-array {
                rule { # 1
                    destination Group:VPN_Remote_Group
                    translated "No NAT"
                }
            }
        }
    }
    }
```

IPsec VPN 总结:

FWN 的 IPsec VPN 和思科路由器的 IPsec VPN 配置有些类似，需要注意的两点：

1. 路由一定要明确的指向到 WAN1（包括公网 IP、感兴趣流目的 IP 的路由）
2. SNAT 需要将第二阶段中的感兴趣流排除掉，因为 FWN 先 NAT 再 IPsec VPN，如果不排除，将匹配不到 IPsec VPN 的感兴趣流，导致 VPN 业务异常。

结果查看

✓ FGT1000C 结果


```
    FGT1KC3912800033 # diagnose vpn ike gateway list
    vd: root/0
    name: TO-FWN
    version: 1
    interface: wan1 5
    addr: 202.106.3.111:500 -> 202.106.1.111:500
    created: 268s ago
    auto-discovery: 0
    IKE SA: created 1/1  established 1/1  time 6010/6010/6010 ms
    IPsec SA: created 1/1  established 1/1  time 6020/6020/6020 ms

      id/spi: 4 4df30f8238d70fc7/269d0dfdce7c9d92
      direction: initiator
      status: established 268-262s ago = 6010ms
      proposal: aes256-sha256

key:fa70f1bc25bc0faa-4f2c10a2cfb9bae0-7b8b723293966530-d1aefd28a7c3691d
      lifetime/rekey: 86400/85837
      DPD sent/recv: 00000000/00000000

    FGT1KC3912800033 # diagnose vpn tunnel list
    list all ipsec tunnel in vd 0
    ------------------------------------------------------
    name=TO-FWN ver=1 serial=1 202.106.3.111:0->202.106.1.111:0
    bound_if=5 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/8
options[0008]=npu
    proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=0 auto-discovery=0
    stat: rxp=271 txp=271 rxb=33604 txb=16260
    dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=2
    natt: mode=none draft=0 interval=0 remote_port=0
    proxyid=TO-FWN proto=0 sa=1 ref=2 serial=3 auto-negotiate
      src: 0:172.16.16.0/255.255.255.0:0
      dst: 0:10.1.1.0/255.255.255.0:0
      SA: ref=4 options=2f type=00 soft=0 mtu=1438 expire=42895/0B
replaywin=2048 seqno=110 esn=0 replaywin_lastseq=0000010f
      life: type=01 bytes=0/0 timeout=43172/43200
      dec: spi=8bf29dc0 esp=aes key=32
c22aeb28d9e30a59548758be18936e57259db4c59aaa8c52d8d8a09fde3cfc2f
          ah=sha256 key=32
```

```
8cd06df23f2d6f7f2cb9bf4df7c3d074927aee1b841b9014c0e9d4da454550d1
     enc: spi=cb9664fe esp=aes key=32
9204dc8ad70ad537b2016e2105a95ad97565e648b9abc9f5841bb2e8bc60f03b
         ah=sha256 key=32
803303ec0f4879075e2d8e4d7c9377233f979cd42489c0722ddf49e6f34da578
     dec:pkts/bytes=271/16260, enc:pkts/bytes=271/33604
     npu_flag=20 npu_rgwy=202.106.1.111 npu_lgwy=202.106.3.111 npu_selid=2
```

✓ FWN1000B 结果

模式 Tunnel 阶段1名称 TO-FGT-PH1 更新

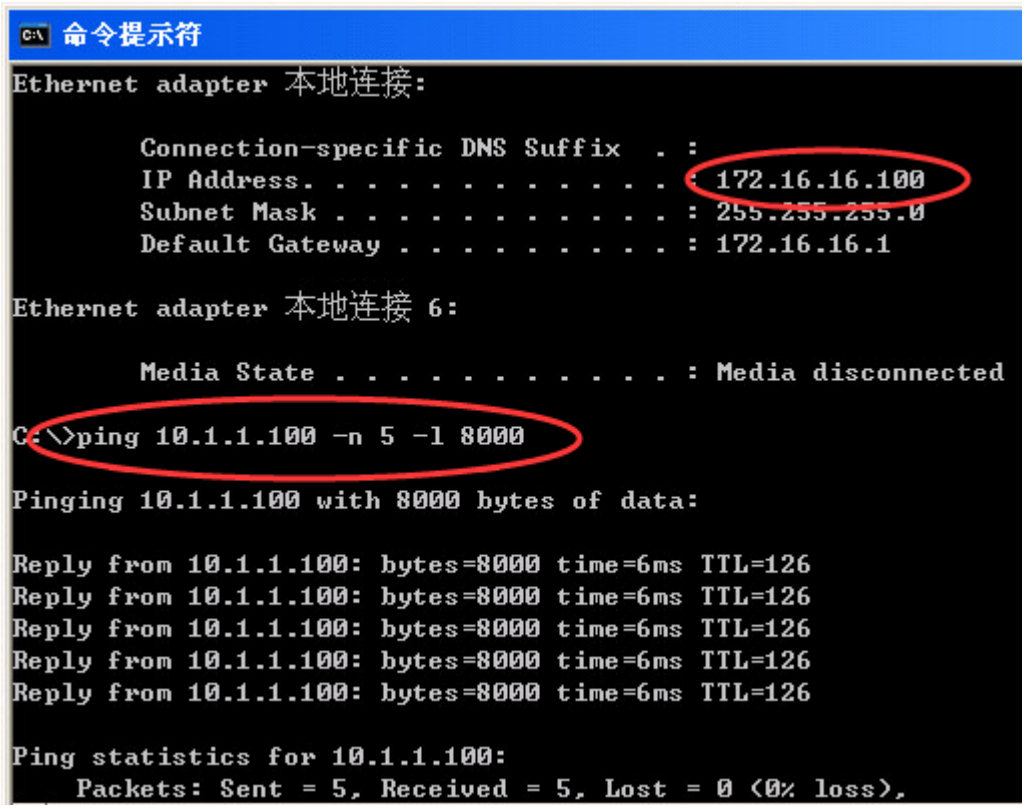
安全关联数据库

本地 IP	远端 IP	加密	认证	使用时间(秒)	生存时间(秒)	更改时间(秒)	状态
202.106.1.111	202.106.3.111	aes-cbc	hmac-sha256	694	1800	1756	mature

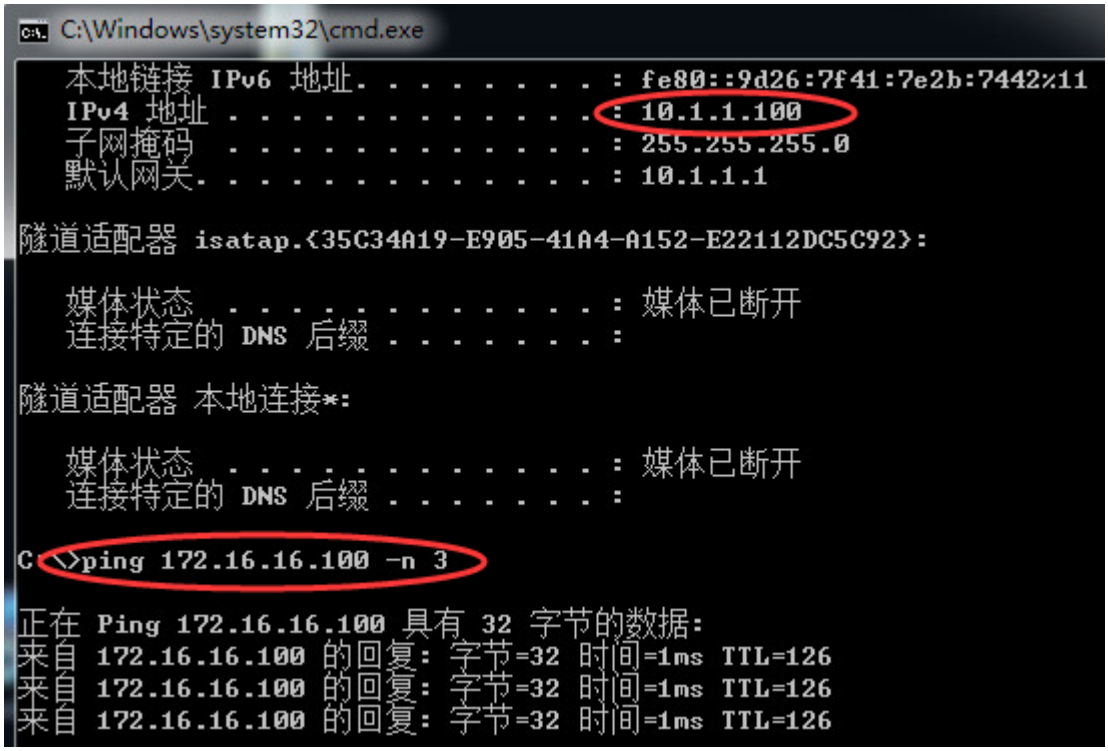
安全策略数据库

名称	来源[端口]	目的地[端口]	协议	创建时间	最后使用时间
TO-FGT-PH2-1	10.1.1.0/24[any]	172.16.16.0/24[any]	any	Sep 3 19:46:12 2017	Sep 3 19:57:46 2017

✓ 业务测试结果



```
命令提示符
Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.16.16.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.16.1

Ethernet adapter 本地连接 6:

        Media State . . . . . . . . . . . : Media disconnected

C:\>ping 10.1.1.100 -n 5 -l 8000

Pinging 10.1.1.100 with 8000 bytes of data:

Reply from 10.1.1.100: bytes=8000 time=6ms TTL=126
Reply from 10.1.1.100: bytes=8000 time=6ms TTL=126
Reply from 10.1.1.100: bytes=8000 time=6ms TTL=126
Reply from 10.1.1.100: bytes=8000 time=6ms TTL=126
Reply from 10.1.1.100: bytes=8000 time=6ms TTL=126

Ping statistics for 10.1.1.100:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
```


C:\Windows\system32\cmd.exe
本地链接 IPv6 地址. . . . . : fe80::9d26:7f41:7e2b:7442%11
IPv4 地址 . . . . . : 10.1.1.100
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 10.1.1.1
隧道适配器 isatap.{35C34A19-E905-41A4-A152-E22112DC5C92}:
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
隧道适配器 本地连接*:
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
C:\>ping 172.16.16.100 -n 3
正在 Ping 172.16.16.100 具有 32 字节的数据:
来自 172.16.16.100 的回复: 字节=32 时间=1ms TTL=126
来自 172.16.16.100 的回复: 字节=32 时间=1ms TTL=126
来自 172.16.16.100 的回复: 字节=32 时间=1ms TTL=126