

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

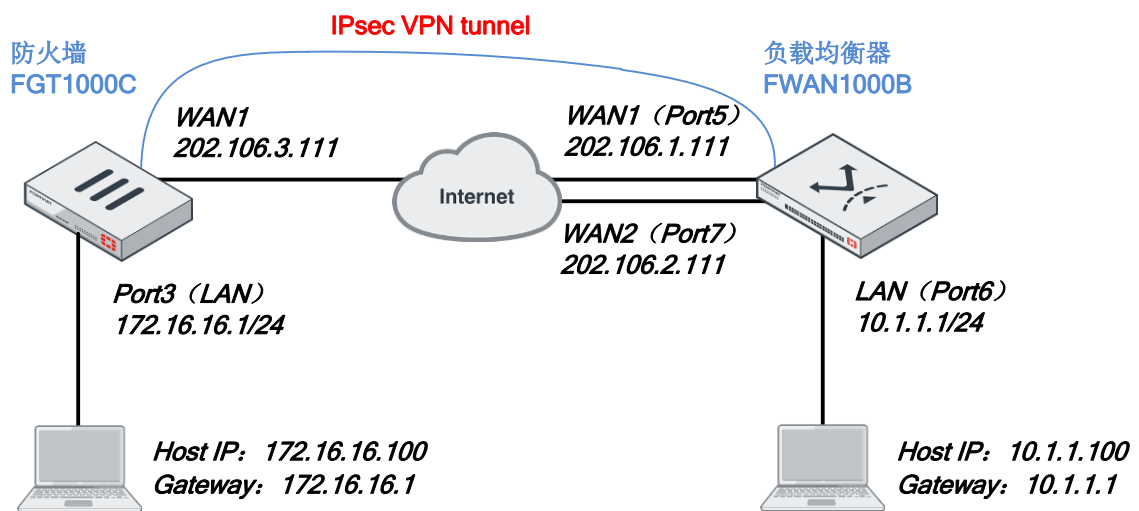
目录

简介.....	3
环境拓扑图.....	3
FortiGate1000C IPsec VPN 配置.....	4
FortiWAN1000B IPsec VPN 配置.....	7
结果查看.....	10

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



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
```

用户名 TO-FWN
注释

网络		 
IP 版本	IPv4	
远程网关	<input type="text" value="静态IP地址"/>	
IP地址	<input type="text" value="202.106.1.111"/>	
接口	<input type="text" value="wan1"/>	
模式配置	<input type="checkbox"/>	
NAT穿越	<input checked="" type="button" value="启用"/> <input type="button" value="禁用"/> <input type="button" value="强制的"/>	
保持存活频率	<input type="text" value="10"/>	
对等体状态探测	<input type="button" value="禁用"/> <input type="button" value="空闲"/> <input checked="" type="button" value="按需"/>	

认证		 编辑
认证方法	预共享密钥	
IKE版本	1, 模式: 主模式(ID保护)	
接受Peer	peertype_	

阶段 1 Proposal		 编辑
算法	AES256-SHA256	
Diffie-Hellman 组	5	

✓ IPsec VPN 第二阶段配置

```

config vpn ipsec phase2-interface
    edit "TO-FWN"
        set phaselname "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
    
```

阶段 2 选择器

用户名	本地地址	远端地址
TO-FWN	172.16.16.0/255.255.255.0	10.1.1.0/255.255.255.0

编辑 Phase 2

用户名: TO-FWN

注释:

本地地址: 172.16.16.0/255.255.255.0

远端地址: 10.1.1.0/255.255.255.0

高级

阶段 2 Proposal

加密: 认证:

启用重播检测

启用完全前向保密 (PFS)

Diffie-Hellman 组: 21 20 19 18 17 16
 15 14 5 2 1

本地端口: 全部

远端端口: 全部

协议: 全部

自动协商:

自动密钥保持存活:

密钥周期(秒/kb):

秒:

✓ 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 日志

隧道模式

+ 阶段 1	
名称	TO-FGT-PH1 隐藏详细设定
本地 IP	202.106.1.111 远端 IP 202.106.3.111
验证方法	预共享密钥 *****
网路密钥交换	<input checked="" type="checkbox"/> v1 <input type="checkbox"/> v2
模式	主模式 (ID保护)
端点失效检测	<input checked="" type="checkbox"/> 启用 延迟 30 秒
安全提议	加密 <input type="checkbox"/> DES <input type="checkbox"/> 3DES <input type="checkbox"/> AES128 <input type="checkbox"/> AES192 <input checked="" type="checkbox"/> AES256
	认证 <input type="checkbox"/> MD5 <input type="checkbox"/> SHA1 <input checked="" type="checkbox"/> SHA256 <input type="checkbox"/> SHA384 <input type="checkbox"/> SHA512
	DH 群组 <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 14
密钥有效期	28800 秒

✓ IPsec VPN 第二阶段配置

+ 阶段 2	
名称	TO-FGT-PH2-1 隐藏详细设定
安全提议	加密 <input type="checkbox"/> NULL <input type="checkbox"/> DES <input type="checkbox"/> 3DES <input type="checkbox"/> AES128 <input type="checkbox"/> AES192 <input checked="" type="checkbox"/> AES256
	认证 <input type="checkbox"/> NULL <input type="checkbox"/> MD5 <input type="checkbox"/> SHA1 <input checked="" type="checkbox"/> SHA256 <input type="checkbox"/> SHA384 <input type="checkbox"/> SHA512
	PFS 群组 <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 14
密钥有效期	1800 秒
快速模式	来源 10.1.1.0/255.255.255.0 端口 任何端口
	目的地 172.16.16.0/255.255.255.0 端口 任何端口
	协议 任何协议

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 RVhNemR5TmxOPU1I
}
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



The screenshot shows the Fortinet FortiGate configuration interface. On the left is a navigation menu with options like '系统总览', '网络设定', and 'IP 群组设定'. The main area displays the 'IP 群组设定' (IP Group Settings) for a group named 'VPN_Remote_Group'. The group is enabled. Under the 'IPv4 规则设定' (IPv4 Rule Settings) section, there is a table with columns for '启用' (Enabled), 'IP 地址' (IP Address), and '动作' (Action). A rule is listed with '172.16.16.0/255.255.255.0' as the IP address and '属于' (Belongs to) as the action. Red circles highlight the group name and the IP address in the screenshot.

IP 群组设定			
群组名称		VPN_Remote_Group	启用此群组 <input checked="" type="checkbox"/>
IPv4 规则设定			
+	启用	IP 地址	动作
+ 音 4 4	<input checked="" type="checkbox"/>	172.16.16.0/255.255.255.0	属于
IPv6 规则设定			


```

        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

The screenshot shows the NAT configuration page for WAN1. A table of NAT rules is displayed with the following columns: 启用 (Enabled), 时段 (Time), 内部地址 (Internal Address), 目的地 (Destination), 服务 (Service), 转换为 (Translate To), and 日志 (Log). The first rule is highlighted with a red box:

+	启用	时段	内部地址	目的地	服务	转换为	日志
+	<input checked="" type="checkbox"/>	所有时段	任何地址	群组:VPN_Remote_Group	任何服务	不做NAT	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	所有时段	202.106.10/255.255.0	任何地址	任何服务	不做NAT	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	所有时段	任何地址	任何地址	任何服务	202.106.1.111	<input type="checkbox"/>

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

刷新	用户名	远程网关	状态	Proxy ID源	代理ID	持续时间	超时
	TO-FWN	202.106.1.111	启用	• 0:172.16.16.0/255.255.255.0:0	• 0:10.1.1.0/255.255.255.0:0	2分钟 42秒	43015

```
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 encaps=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_rgw=202.106.1.111 npu_lgw=202.106.3.111 npu_selid=2
```

✓ FWN1000B 结果

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

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

```
C:\> 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
```