

## 使用 ADVPN(Auto Discovery VPN) 建立 Full-Mesh 方式的 Hub\_and\_Spoke

版本	1.2
时间	2016 年 5 月
支持的版本	FortiGate 5.4. x
作者	刘康明
状态	已审核
反馈	<a href="mailto:support_cn@fortinet.com">support_cn@fortinet.com</a>

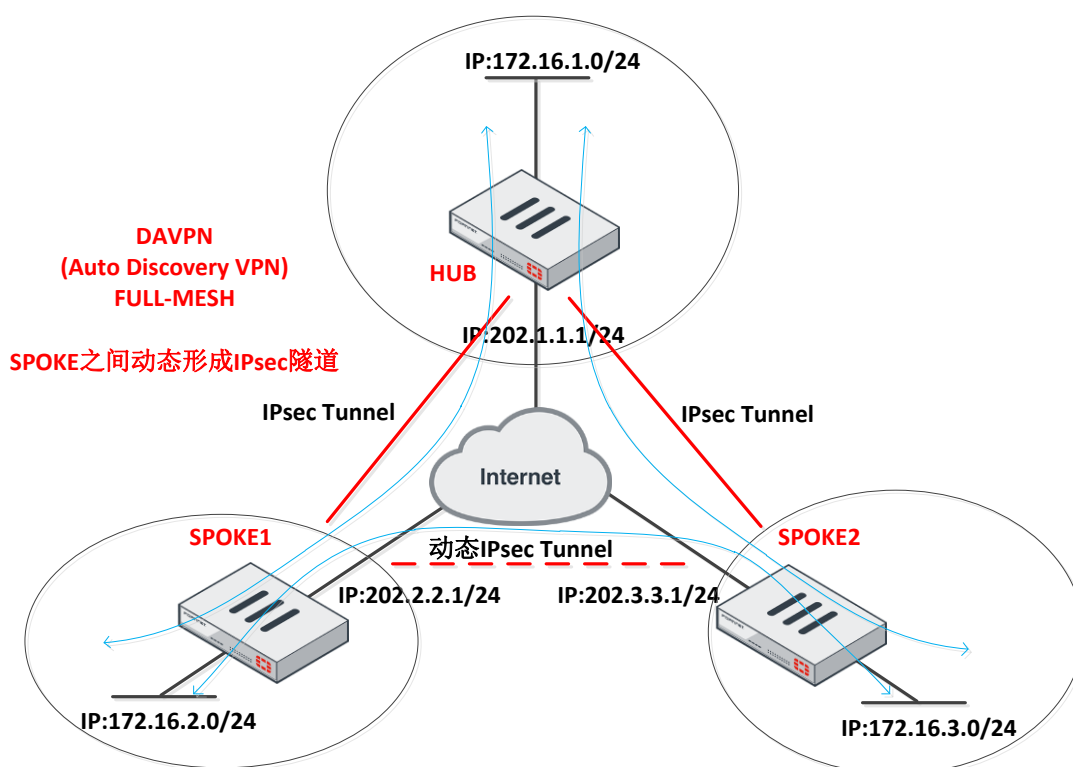
## 目录

简介.....	3
ADVPN 配置举例.....	6
拓扑说明.....	6
总部 HUB FortiGate 配置.....	7
配置 IPsec VPN 第一阶段.....	7
配置 IPsec VPN 第二阶段.....	7
配置 IPsec VPN 隧道 IP.....	7
配置 BGP 和路由反射器.....	8
策略配置.....	9
分部 Spoke1 FortiGate 配置.....	10
配置 IPsec VPN 第一阶段.....	10
配置 IPsec VPN 第二阶段.....	10
配置 IPsec VPN 隧道 IP.....	11
配置 BGP 并发布业务路由.....	11
配置打通 IBGP 路由下一跳的静态路由.....	12
策略配置.....	13
分部 Spoke2 FortiGate 配置.....	14
配置 IPsec VPN 第一阶段.....	14
配置 IPsec VPN 第二阶段.....	14
配置 IPsec VPN 隧道 IP.....	14
配置 BGP 并发布业务路由.....	15
配置打通 IBGP 路由下一跳的静态路由.....	16
策略配置.....	16
Spoke 之间业务互访前设备状态观察.....	17
HUB 状态.....	17
SPOKE1 状态.....	18
SPOKE2 状态.....	18
Spoke 之间业务互访后设备状态观察.....	19
HUB 状态.....	20
SPOKE1 状态.....	20
SPOKE2 状态.....	21
业务访问测试.....	23
RIP v2 方式的 ADVPN（补充）.....	26
HUB、Spoke1、Spoke2 之间使用 RIP v2.....	26
Spoke 之间业务互访前设备状态观察（RIP v2）.....	29
Spoke 之间业务互访后设备状态观察（RIP v2）.....	30
FAQ.....	32

## 简介

ADVPN (Auto Discovery VPN) 是一种基于 IETF RFC draft 的 IPsec VPN 技术。  
(<https://tools.ietf.org/html/draft-sathyanarayan-ipsecme-advpn-03>) 简单来说，ADVPN 允许在传统的 Hub-and-Spoke VPN 网络中的 Spokes 之间相互建立动态的、按需连接的 VPN 隧道，从而达到整网 Full-Mesh 的效果。

传统的 Hub-Spoke 方式中，Spoke 只能和 Hub 建立永久隧道，Spoke 之间的流量需要通过 Hub 来转发，这种方式减轻了 Spoke 的负担，增加了 Hub 的性能要求，同时利于总部对分支间流量的监控；使用 ADVPN 技术实现的 Full-Mesh 方式中，Spoke 之间可以建立动态直连隧道，分支间的流量可以直接转发。相比而言，Hub 负担减轻，同时减少分支间流量的延迟，更有利于 VOIP 等实时流量的传输，在实际使用的过程中可按照自身需求进行选择。ADVPN 实现总部和分部之间 Full-Mesh 如下图所示：

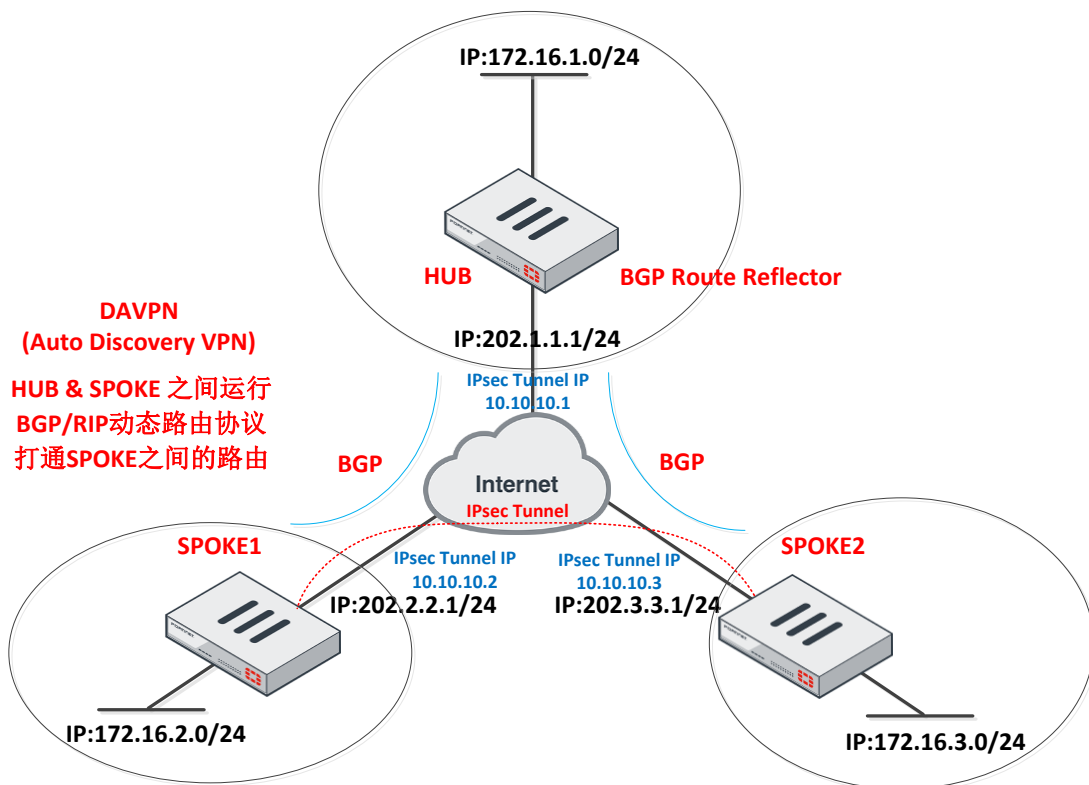


我们都知道思科的 DMVPN，DMVPN 通过多点的 GRE-Over-IPsec 加上 NHRP 注册协议实现总部和分部之间的全互联（Full-Mesh），而 Fortinet 的 ADVPN 与 DMVPN 的实现方式完全不一样，ADVPN 只基于 IKE（携带 ADVPN 报文）& IPsec（通过 IKE 消息触发 advpn 内核通知）就能实现，不需要 GRE-Over-IPsec，也不需要 NHRP 注册服务，以更加简单

的方式实现总部和分部之间全互联（Full-Mesh）。

目前只有 FortiOS5.4 的版本才支持 ADVPN，同时 ADVPN 需要与动态路由协议（BGP/RIP v2）配合使用。相对较大的 Hub\_and\_Spoke 组网，推荐使用 BGP 协议，因为 BGP 有着丰富的路由选路特性，同时 BGP 的路由反射功能与 ADVPN 能够完美的契合，二者的实现原理都围绕着简化 Full-Mesh 进行，HUB 设备充当 BGP 的 RR 反射器角色，所有的 Spoke 都只需要与 Hub 建立起 BGP 邻居（就像所有 Spoke 也只需要与 Hub 建立起 IPsec VPN 一样），Hub 就像一面反射的镜子，将这个 Spoke 学习而来的 BGP 路由传递给其他所有的 Spokes，Hub 通过 BGP RR 负责整网的路由动态更新。

当新加入一个 Spoke 的时候，只需要与 Hub 建立 IPsec VPN 隧道以及 BGP 邻居，则这个新的 Spoke 的路由信息就可被传递到其他的 Spoke，同时其他的 Spoke 通过触发 ADVPN 可以动态地与新 Spoke 建立起直连的 IPsec VPN 隧道，二者的业务网段 BGP 路由将迭代到这条直连 IPsec VPN 隧道上，从而实现 Spoke 之间数据和路由的直接转发，如下图：Spoke1 的 172.16.2.0 网段发起去往 Spoke2 的 172.16.3.0 网段的访问，ADVPN 会被动态触发，形成一条动态的 Spoke1 到 Spoke2 的直连隧道，而相应的 BGP 路由也会被路由迭代到这条直连的隧道上去。



在实际使用过程中为了简化 BGP 的配置，可以使用 BGP 动态邻居特性，该特性中，在 Hub 节点 BGP 配置中，配置一个特定网段，Hub 可以接受来自该网段内的所有邻居的连接请求，并与其建立对等体关系，本地不再一一配置到每个对端的 peer 命令。在大规模组网中，该特性既简化了配置，又大大降低了维护和升级成本。为了防止非法邻居接入，建议动态邻居所在的对等体组需要配置 MD5 认证功能。

而对于较小型的组网（Spoke 不超过 10 个），可以选择使用简单的 RIP v2，RIP v2 使用组播 224.0.0.9 定期更新路由，最开始 Spoke 学到的 RIP 业务网段路由的下一跳全部来自 HUB，但当 ADVPN 被触发后，将会建立一条 Spoke\_X 到 Spoke\_Y 之间的直连 IPsec 隧道，RIP v2 就会在这条直连隧道上通告 RIP 路由，于是 Spoke 之间可以学习到相互的业务网段的路由下一跳直接指向这条直连的 IPsec 隧道（因为发布的 RIP 路由的跳数更少，路由更优），此后 Spoke 之间的业务数据访问就走都这条直连的 IPsec VPN 隧道了。

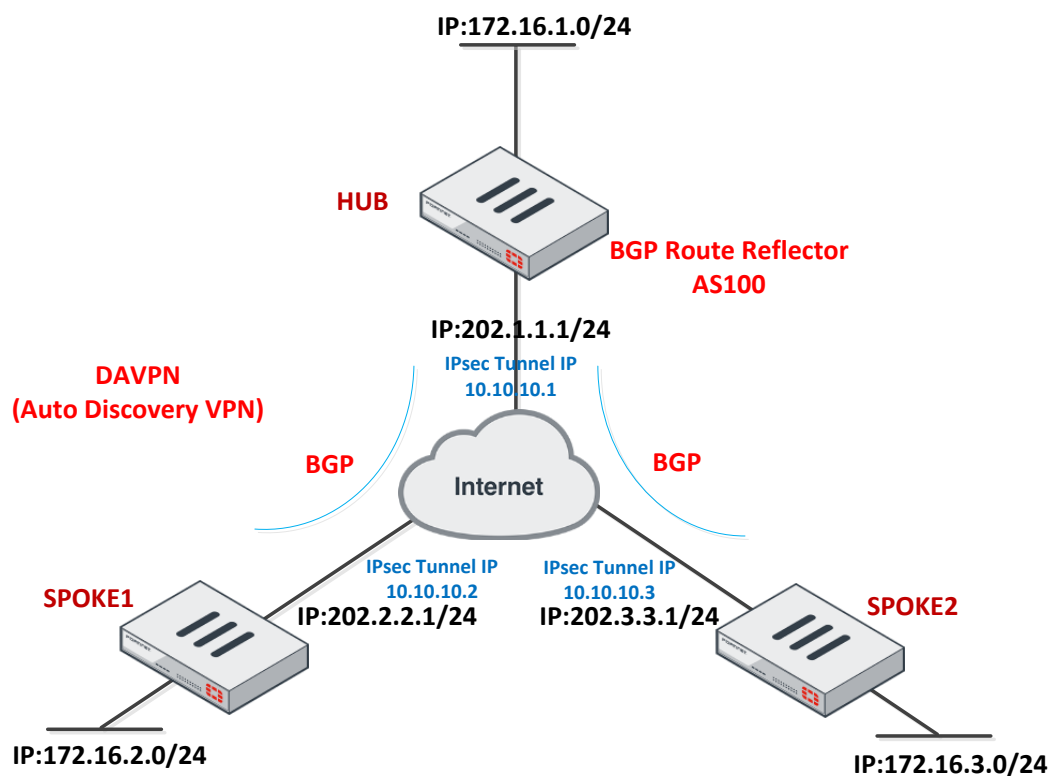
**Key word:** *IPsec VPN、ADVPN、BGP Route-Reflector、Full-Mesh、HUB-and-SPOKE*

**FortiOS Version:** *v5.4.0,build1045,160429 (Interim)*

## ADVPN 配置举例

本章节将重点演示利用 BGP 路由反射器机制作为动态路由协议的 ADVPN 解决方案，最后将简单演示 RIP 路由实现的 ADVPN。

### 拓扑说明



角色	公网 IP	私网网段	VPN 隧道 IP	BGP 信息
HUB	202.1.1.1	172.16.1.0/24	10.10.10.1	AS 100 RR 反射器
SPOKE1	202.2.2.1	172.16.2.0/24	10.10.10.2	AS 100 RR Client
SPOKE2	202.3.3.1	172.16.3.0/24	10.10.10.3	AS 100 RR Client
SPOKE3				
SPOKExyz.				

在配置 BGP 和 ADVPN 的时候最好选择使用 CLI 进行配置，我们假设基本的 IP 以及路由信息已按照拓扑图配置完毕。

## 总部 HUB FortiGate 配置

### 配置 IPsec VPN 第一阶段

```
config vpn ipsec phase1-interface
    edit "ADVPN"
        set type dynamic
        set interface "wan1"
        set psksecret fortinet
        set add-route disable
        set auto-discovery-sender enable
```

注意：

1. 由于总部需要与各种不通类型（静态 IP/PPPOE）的 SPOKE 之间建立 IPsec VPN，因此 HUB 需选择 dynamic 模式
2. ADVPN 不支持 aggressive 模式，只能选择主模式
3. HUB 侧需要开启“auto-discovery-sender enable”，以便接收与发送 Spoke 之间的直连隧道互联信息。（Hub 响应信息，让 Spoke 知道它应该去连接哪个公网 IP 的动态隧道）
4. 由于使用了 BGP 动态路由协议，因此需要关闭自动添加路由的功能“add-route disable”


### 配置 IPsec VPN 第二阶段

```
config vpn ipsec phase2-interface
    edit "ADVPN"
        set phase1name "ADVPN"
    next
end
```

### 配置 IPsec VPN 隧道 IP

```
config system interface
    edit "ADVPN"
        set vdom "root"
        set ip 10.10.10.1 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 10.10.10.254      (10.10.10.254 并非真实存在的一个 IP)
        set interface "wan1"
    next
end
```

## Edit Interface

Interface Name	ADVPN
Type	Tunnel Interface
Interface	wan1
Role 	Undefined ▼

### Address

Addressing mode	Manual
IP	10.10.10.1
Network Mask	255.255.255.255
Remote IP	10.10.10.254

未被使用的IP

注意: 1.remote-ip 10.10.10.254 是不被 Spoke 所使用的预留 IP, IPsec Tunnel 是一个点对点的隧道,但是 ADVPN 中这条隧道需要同时对应多个 SPOKE,因此不能将 Remote IP 写成一个存在的 SPOKE 端 IP。

## 配置 BGP 和路由反射器

```
config router bgp
    set as 100
    set router-id 10.10.10.1
    config neighbor-group -neighbor-group 特性
        edit "ADVPN-PEERS"
            set remote-as 100
            set route-reflector-client enable -设置 RR (路由反射器)
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.10.0 255.255.255.0
            set neighbor-group "ADVPN-PEERS"
        next
    end
    config network
        edit 1
            set prefix 172.16.1.0 255.255.255.0 -发布路由
        next
    end
```



注意：1.利用 BGP neighbor-group 特性，只要匹配前缀列表 10.10.10.0/24 的 BGP-Peer 均可以和 HUB 建立 BGP 邻居。

2.将邻居设置为 Route-Reflector-Client，自己即为路由反射器（Route-Reflector），通过路由反射器原理实时同步整网路由。

## 策略配置

```
config firewall policy
  edit 1
    set name "OUT ADVPN"
    set srcintf "lan"
    set dstintf "ADVPN"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set status enable
  next

  edit 2
    set name "IN ADVPN"
    set srcintf "ADVPN"
    set dstintf "lan"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set status enable
  next

  edit 3
    set name "ADVPNtoADVPN"
    set srcintf "ADVPN"
    set dstintf "ADVPN"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set status enable
```

```
next
end
```

<div> <div>+ Create New</div> <div>Edit</div> <div>Delete</div> <div>Policy Lookup</div> <div>Search</div> </div>								
Seq.#	Name	Source	Destination	Schedule	Service	Action	NAT	S
ADVPN - ADVPN (1 - 1)								
1	ADVPNtoADVPN	all	all	always	ALL	ACCEPT	Disabled	
ADVPN - lan (2 - 2)								
2	IN ADVPN	all	all	always	ALL	ACCEPT	Disabled	+
lan - ADVPN (3 - 3)								
3	OUT ADVPN	all	all	always	ALL	ACCEPT	Disabled	

注意：一定注意配置 ADVPN 到 ADVPN 之间（SPOKE 之间）的放通策略

## 分部 Spoke1 FortiGate 配置

### 配置 IPsec VPN 第一阶段

```
config vpn ipsec phase1-interface
    edit "ADVPN"
        set interface "wan1"
        set remote-gw 202.1.1.1
        set psksecret fortinet
        set add-route disable
        set auto-discovery-receiver enable
    next
end
```

注意：

1. 由于总部 HUB 的公网 IP 是固定的，因此分部配置静态的 IPsec VPN
2. Spoke 侧需要开启“auto-discovery-receiver enable”，以便接收 Hub 的 ADVPN 信息
3. 同样由于 Spoke 需要使用 BGP 动态路由协议，因此需要关闭自动添加路由属性（add-route disable）

### 配置 IPsec VPN 第二阶段

```
config vpn ipsec phase2-interface
    edit "ADVPN"
        set phase1name "ADVPN"
        set auto-negotiate enable
    next
end
```

end

## 配置 IPsec VPN 隧道 IP

```
config system interface
    edit "ADVPN"
        set vdom "root"
        set ip 10.10.10.2 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 10.10.10.1 // 指向 HUB 的隧道 IP 地址
        set interface "wan1"
    next
end
```

Interface Name	ADVPN
Type	Tunnel Interface
Interface	wan1
Role	Undefined

### Address

Addressing mode	Manual
IP	10.10.10.2
Network Mask	255.255.255.255
Remote IP	10.10.10.1

## 配置 BGP 并发布业务路由

Local As	100	(1-4294967295)
Router ID	10.10.10.2	(IP)

Apply

Neighbors		IP:	Remote As:	Add / Edit
<input type="checkbox"/>	Neighbor			
<input type="checkbox"/>	10.10.10.1		100	

Networks		IP/Netmask:	Add
<input type="checkbox"/>	Network		
<input type="checkbox"/>	172.16.2.0/255.255.255.0		

```
config router bgp
    set as 100
```

```
set router-id 10.10.10.2
config neighbor
    edit "10.10.10.1"
        set remote-as 100
    next
end
config network
    edit 1
        set prefix 172.16.2.0 255.255.255.0
    next
end
```

\\只需要与 HUB 建立 BGP 邻居即可

## 配置打通 IBGP 路由下一跳的静态路由

```
config router static
    edit 2
        set dst 10.10.10.0 255.255.255.0
        set device "ADVPN"
    next
end
```

Edit Static Route

Destination ⓘ

Subnet
Named Address
Internet Service

10.10.10.0/255.255.255.0

Device
ADVPN

Administrative Distance ⓘ
10

Comments
0/255

Status
Enabled Disabled

+ Advanced Options

OK Cancel

### 注意:

这是非常重要的一步，Spoke 都需要写 10.10.10.0/24 下一跳指向 ADVPN，要记住 BGP 的路由是建立在 IGP 之上的，首先需要保障 IGP 路由可达，以防止出现路由黑洞。（由于 SPOKE1 学习到 SPOKE2 的 BGP 路由 172.16.3.0/24 下一跳是指向 10.10.10.3，而 SPOKE1 去往 10.10.10.3 去走默认路由的，将会被递归转发到运营商的设备上，此时 SPOKE 间的业务数据转发将异常，同时会导致无法触发 ADVPN，因此需要手动添加一条静态的去往 10.10.10.0/24 网段的路由指向 ADVPN 隧道，避免上述问题。

## 策略配置

```
config firewall policy
  edit 0
    set name "OUT ADVPN"
    set srcintf "internal"
    set dstintf "ADVPN"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set status enable
  next

  edit 0
    set name "IN ADVPN"
    set srcintf "ADVPN"
    set dstintf "internal"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set status enable
  next
end
```

Create New		Edit	Delete	Policy Lookup	Search		
Seq.#	Name	Source	Destination	Schedule	Service	Action	NAT
ADVPN - internal (1 - 1)							
1	1	all	all	always	ALL	ACCEPT	Disabled
internal - ADVPN (2 - 2)							
2	2	all	all	always	ALL	ACCEPT	Disabled

## 分部 Spoke2 FortiGate 配置

### 配置 IPsec VPN 第一阶段

```
config vpn ipsec phase1-interface
    edit "ADVPN"
        set interface "wan1"
        set remote-gw 202.1.1.1
        set psksecret fortinet
        set add-route disable
        set auto-discovery-receiver enable
    next
end
```


### 配置 IPsec VPN 第二阶段

```
config vpn ipsec phase2-interface
    edit "ADVPN"
        set phase1name "ADVPN"
        set auto-negotiate enable
    next
end
```

### 配置 IPsec VPN 隧道 IP

```
config system interface
    edit "ADVPN"
        set vdom "root"
        set ip 10.10.10.3 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 10.10.10.1
        set interface "wan1"
    next
end
```

## Edit Interface

Interface Name ADVPN  
 Type Tunnel Interface  
 Interface wan1  
 Role  Undefined ▼

### Address

Addressing mode Manual  
 IP 10.10.10.3  
 Remote IP 10.10.10.1

### Restrict Access

Administrative Access ☐ HTTPS ☒ PING [ ☐ SNMP ☐ RADIUS Accour

## 配置 BGP 并发布业务路由

Local As 100 (1-4294967295)  
 Router ID 10.10.10.3 (IP)

Neighbors		IP: <input type="text"/>	Remote As: <input type="text"/>	<input type="button" value="Add / Edit"/>
<input type="checkbox"/>	Neighbor			
<input type="checkbox"/>	10.10.10.1		100	

Networks		IP/Netmask: <input type="text"/>	<input type="button" value="Add"/>
<input type="checkbox"/>	Network		
<input type="checkbox"/>	172.16.3.0/255.255.255.0		

```
config router bgp
  set as 100
  set router-id 10.10.10.3
  config neighbor
    edit "10.10.10.1"
      set remote-as 100
    next
  end
  config network
    edit 1
      set prefix 172.16.3.0 255.255.255.0
```

next

## 配置打通 IBGP 路由下一跳的静态路由

```
config router static
  edit 2
    set dst 10.10.10.0 255.255.255.0
    set device "ADVPN"
  next
end
```

Edit Static Route

Destination

Subnet
Named Address
Internet Service

10.10.10.0/255.255.255.0

Device

ADVPN

Administrative Distance

10

Comments

0/255

Status

Enabled
Disabled

+ Advanced Options

OK

Cancel

## 策略配置

<div> + Create New Edit Delete Policy Lookup Search </div>							
Seq.#	Name	Source	Destination	Schedule	Service	Action	NAT
ADVPN - lan (1 - 1)							
1	IN ADVPN	all	all	always	ALL	ACCEPT	Disabled
lan - ADVPN (2 - 2)							
2	OUT ADVPN	all	all	always	ALL	ACCEPT	Disabled

```
config firewall policy
  edit 0
    set name "OUT ADVPN"
    set srcintf "lan"
    set dstintf "ADVPN"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
```



```

set schedule "always"
set service "ALL"
set status enable
next
edit 0
set name "IN ADVPN"
set srcintf "ADVPN"
set dstintf "lan"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set status enable
next
end

```

以上 HUB/Spoke1/Spoke2 全部配置完毕。

## Spoke 之间业务互访前设备状态观察

SPOKE1 和 SPOKE2 之间无任何流量访问的时候，HUB/SPOKE1/SPOKE2 状态观察：

### HUB 状态

HUB IPsec VPN 建立情况：

Monitor--->IPsec Monitor

Refresh							
Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2 Selector
ADVPN_0	Custom	202.2.2.1		Up	71.97 kB	34.61 kB	ADVPN
ADVPN_1	Custom	202.3.3.1		Up	37.74 kB	18.21 kB	ADVPN

HUB 路由学习情况：

Monitor--->Routing Monitor

Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	202.1.1.254	wan1	
Connected		10.10.10.1/32	0.0.0.0	ADVPN_0	
Connected		10.10.10.1/32	0.0.0.0	ADVPN_1	
Connected		10.10.10.2/32	0.0.0.0	ADVPN_0	
Connected		10.10.10.3/32	0.0.0.0	ADVPN_1	
Connected		172.16.1.0/24	0.0.0.0	lan	
BGP		172.16.2.0/24	10.10.10.2	ADVPN_0	0 04:21:28
BGP		172.16.3.0/24	10.10.10.3	ADVPN_1	0 02:13:07
Connected		202.1.1.0/24	0.0.0.0	wan1	

```
FG240D3913801860 # get router info routing-table all
```

```
S*    0.0.0.0/0 [10/0] via 202.1.1.254, wan1
C     10.10.10.1/32 is directly connected, ADVPN_0
           is directly connected, ADVPN_1
C     10.10.10.2/32 is directly connected, ADVPN_0
C     10.10.10.3/32 is directly connected, ADVPN_1
C     172.16.1.0/24 is directly connected, lan
B     172.16.2.0/24 [200/0] via 10.10.10.2, ADVPN_0, 04:22:02
B     172.16.3.0/24 [200/0] via 10.10.10.3, ADVPN_1, 02:13:41
C     202.1.1.0/24 is directly connected, wan1
```

## SPOKE1 状态

SPOKE1 IPsec VPN 建立情况（只和 HUB 建立 IPsec）：



Monitor--->IPsec Monitor

Refresh

Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2 Selector
ADVPN	 Custom	202.1.1.1		 Up	73.43 kB	35.35 kB	ADVPN

SPOKE1 路由学习情况：

Monitor--->Routing Monitor

 Refresh		 Route Lookup			
Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	202.2.2.254	wan1	
Static		10.10.10.0/24	10.10.10.1	ADVPN	
Connected		10.10.10.1/32	0.0.0.0	ADVPN	
Connected		10.10.10.2/32	0.0.0.0	ADVPN	
BGP		172.16.1.0/24	10.10.10.1	ADVPN	0 04:26:10
Connected		172.16.2.0/24	0.0.0.0	internal	
BGP		172.16.3.0/24	10.10.10.3		0 02:17:24
Connected		202.2.2.0/24	0.0.0.0	wan1	

```
FGT60D4614022596 # get router info routing-table all
```

```
S*    0.0.0.0/0 [10/0] via 202.2.2.254, wan1
S     10.10.10.0/24 [10/0] via 10.10.10.1, ADVPN
C     10.10.10.1/32 is directly connected, ADVPN
C     10.10.10.2/32 is directly connected, ADVPN
B     172.16.1.0/24 [200/0] via 10.10.10.1, ADVPN, 04:26:51
C     172.16.2.0/24 is directly connected, internal
B     172.16.3.0/24 [200/0] via 10.10.10.3 (recursive via 10.10.10.1), 02:18:05
C     202.2.2.0/24 is directly connected, wan1
```

## SPOKE2 状态

SPOKE2 IPsec VPN 建立情况（只和 HUB 建立 IPsec）：

Monitor--->IPsec Monitor

Refresh							
Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2 Selector
ADVPN	Custom	202.1.1.1		Up	40.27 kB	19.39 kB	ADVPN

SPOKE2 路由学习情况:

Monitor--->Routing Monitor

Refresh

Route Lookup

Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	202.3.3.254	wan1	
Static		10.10.10.0/24	10.10.10.1	ADVPN	
Connected		10.10.10.1/32	0.0.0.0	ADVPN	
Connected		10.10.10.3/32	0.0.0.0	ADVPN	
BGP		172.16.1.0/24	10.10.10.1	ADVPN	0 02:20:10
BGP		172.16.2.0/24	10.10.10.2		0 02:14:22
Connected		172.16.3.0/24	0.0.0.0	lan	
Connected		202.3.3.0/24	0.0.0.0	wan1	

```
FG240D4614802169 # get router info routing-table all
```

```
S*      0.0.0.0/0 [10/0] via 202.3.3.254, wan1
S       10.10.10.0/24 [10/0] via 10.10.10.1, ADVPN
C       10.10.10.1/32 is directly connected, ADVPN
C       10.10.10.3/32 is directly connected, ADVPN
B       172.16.1.0/24 [200/0] via 10.10.10.1, ADVPN, 02:20:55
B       172.16.2.0/24 [200/0] via 10.10.10.2 (recursive via 10.10.10.1), 02:15:07
C       172.16.3.0/24 is directly connected, lan
C       202.3.3.0/24 is directly connected, wan1
```

注意 Spoke1 学到的 Spoke2 的业务路由(B 172.16.3.0/24 [200/0] via 10.10.10.3 (recursive via 10.10.10.1))，下一跳是指向 10.10.10.3 的，并路由递归到了 HUB (10.10.10.1)，这是由于 BGP RR 在传递路由信息的时候，不改变 net-hop 信息，因此这条静态路由 || "S 10.10.10.0/24 [10/0] via 10.10.10.1, ADVPN" || 在此时发挥了重要的作用，SPOKE1 和 SPOKE2 之间互访的时候，需要触发 ADVPN 机制，而如果没有这条静态路由，总部 HUB 根本无法收到 SPOKE1 与 SPOKE2 之间的互访的流量（报文会被递归到缺省路由，丢到 Internet 上去了），也不会触发 ADVPN 机制让 SPOKE1 和 SPOKE2 之间动态建立 IPsec VPN 邻居。因此在 IBGP 的环境下这条路由必不可少，否则将出现业务不通。

## Spoke 之间业务互访后设备状态观察

一旦发起 SPOKE1 与 SPOKE2 之间的互访将立马触发 ADVPN 机制，使得 SPOKE1 和 SPOKE2 之间动态协商出一条直连的 IPsec VPN 隧道。接下来我们观察一下，SPOKE1 和 SPOKE2 有流量访问并触发建立了动态 IPsec VPN 隧道时 HUB/SPOKE1/SPOKE2 的状态：

## HUB 状态

HUB IPsec VPN 建立情况:

Monitor--->IPsec Monitor

Refresh

Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2
ADVPN_0	Custom	202.2.2.1		Up	78.10 kB	37.56 kB	ADVPN
ADVPN_1	Custom	202.3.3.1		Up	44.00 kB	21.22 kB	ADVPN

HUB 路由学习情况:

Monitor--->Routing Monitor

Refresh Route Lookup

Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	202.1.1.254	wan1	
Connected		10.10.10.1/32	0.0.0.0	ADVPN_0	
Connected		10.10.10.1/32	0.0.0.0	ADVPN_1	
Connected		10.10.10.2/32	0.0.0.0	ADVPN_0	
Connected		10.10.10.3/32	0.0.0.0	ADVPN_1	
Connected		172.16.1.0/24	0.0.0.0	lan	
BGP		172.16.2.0/24	10.10.10.2	ADVPN_0	0 04:42:25
BGP		172.16.3.0/24	10.10.10.3	ADVPN_1	0 02:34:04
Connected		202.1.1.0/24	0.0.0.0	wan1	

```
FG240D3913801860 # get router info routing-table all
```

```
S*    0.0.0.0/0 [10/0] via 202.1.1.254, wan1
C     10.10.10.1/32 is directly connected, ADVPN_0
           is directly connected, ADVPN_1
C     10.10.10.2/32 is directly connected, ADVPN_0
C     10.10.10.3/32 is directly connected, ADVPN_1
C     172.16.1.0/24 is directly connected, lan
B     172.16.2.0/24 [200/0] via 10.10.10.2, ADVPN_0, 04:42:50
B     172.16.3.0/24 [200/0] via 10.10.10.3, ADVPN_1, 02:34:29
C     202.1.1.0/24 is directly connected, wan1
```

可以看出 HUB 端没有任何变化。变化主要在 SPOKE 端。

## SPOKE1 状态

SPOKE1 IPsec VPN 建立情况:

Monitor--->IPsec Monitor

Refresh

SPOKE1与SPOKE2动态建立起的IPsec VPN隧道

Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2
ADVPN_0	Custom	202.3.3.1		Up	78.00 kB	38.00 kB	ADVPN
ADVPN	Custom	202.1.1.1		Up	78.91 kB	38.01 kB	ADVPN

SPOKE1 路由学习情况:

Monitor--->Routing Monitor

	Route Lookup				
Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	202.2.2.254	wan1	
Static		10.10.10.0/24	10.10.10.1	ADVPN	
Connected		10.10.10.1/32	0.0.0.0	ADVPN	
Connected		10.10.10.2/32	0.0.0.0	ADVPN	
Connected		10.10.10.2/32	0.0.0.0	ADVPN_0	
Connected		10.10.10.3/32	0.0.0.0	ADVPN_0	
BGP		172.16.1.0/24	10.10.10.1	ADVPN	0 04:47:20
Connected		172.16.2.0/24	0.0.0.0	internal	
BGP		172.16.3.0/24	10.10.10.3	ADVPN_0	0 00:12:19
Connected		202.2.2.0/24	0.0.0.0	wan1	

```
FGT60D4614022596 # get router info routing-table all
```

```
S*    0.0.0.0/0 [10/0] via 202.2.2.254, wan1
S     10.10.10.0/24 [10/0] via 10.10.10.1, ADVPN
C     10.10.10.1/32 is directly connected, ADVPN
C     10.10.10.2/32 is directly connected, ADVPN
      is directly connected, ADVPN_0
C    10.10.10.3/32 is directly connected, ADVPN_0
B    172.16.1.0/24 [200/0] via 10.10.10.1, ADVPN, 04:48:05
C     172.16.2.0/24 is directly connected, internal
B    172.16.3.0/24 [200/0] via 10.10.10.3, ADVPN_0, 00:13:04
C     202.2.2.0/24 is directly connected, wan1
```

注意 IPsecVPN 和路由都变化了! 去往 SPOKE2 的 172.16.3.0/24 网段 BGP 路由的下一跳还是 10.10.10.3, 但是此时由于动态建立了一条直连的 IPsec VPN 隧道, 10.10.10.3 变成了 SPOKE2 的直连路由, 因此此时直连路由 (C 10.10.10.3/32 is directly connected, ADVPN\_0) 优先于静态路由 (S 10.10.10.0/24 [10/0] via 10.10.10.1, ADVPN), 因此去往 SPOKE2 的下一跳直接递归指向了 ADVPN\_0, 也就是与 SPOKE1 和 SPOKE2 之间建立起来的 IPsec VPN 隧道, 如此就实现了 SPOKE 之间数据直接转发。

## SPOKE2 状态

SPOKE2 IPsec VPN 建立情况:

Monitor--->IPsec Monitor

	SPOKE2和SPOKE1之间动态建立起来的IPsec VPN隧道						
Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2
ADVPN_0	Custom	202.2.2.1		Up	170.28 kB	85.14 kB	ADVPN
ADVPN	Custom	202.1.1.1		Up	48.33 kB	23.27 kB	ADVPN

SPOKE2 路由学习情况:

Monitor--->Routing Monitor

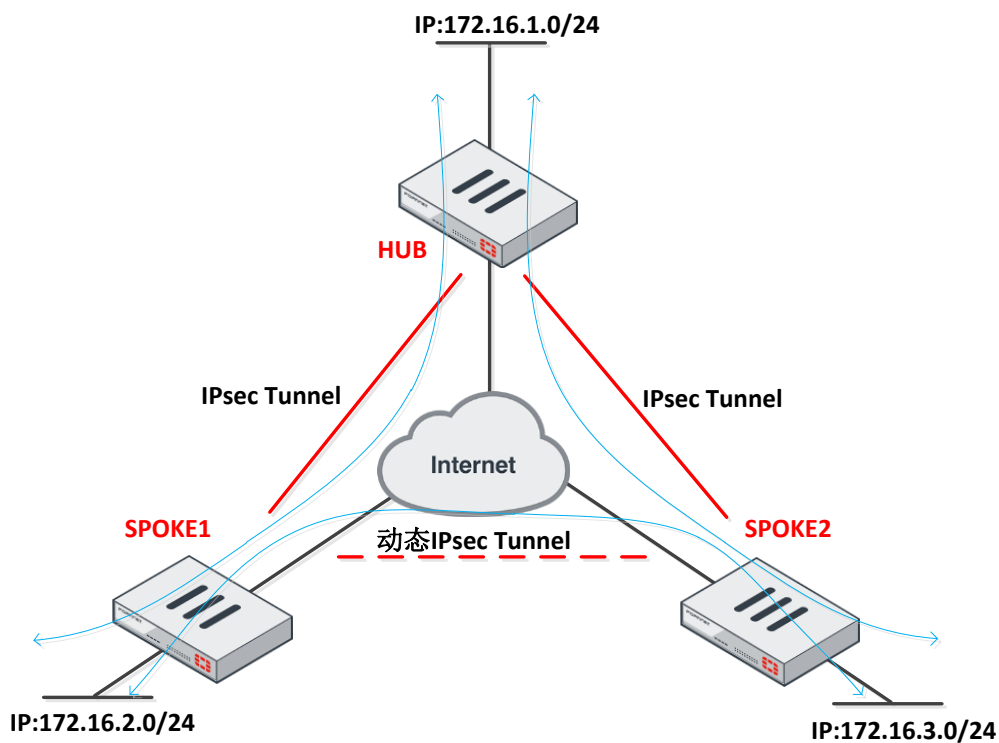
Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	202.3.3.254	wan1	
Static		10.10.10.0/24	10.10.10.1	ADVPN	
Connected		10.10.10.1/32	0.0.0.0	ADVPN	
Connected		10.10.10.2/32	0.0.0.0	ADVPN_0	
Connected		10.10.10.3/32	0.0.0.0	ADVPN	
Connected		10.10.10.3/32	0.0.0.0	ADVPN_0	
BGP		172.16.1.0/24	10.10.10.1	ADVPN	0 02:50:39
BGP		172.16.2.0/24	10.10.10.2	ADVPN_0	0 00:23:51
Connected		172.16.3.0/24	0.0.0.0	lan	
Connected		202.3.3.0/24	0.0.0.0	wan1	

FG240D4614802169 # get router info routing-table all

```

S*      0.0.0.0/0 [10/0] via 202.3.3.254, wan1
S       10.10.10.0/24 [10/0] via 10.10.10.1, ADVPN
C       10.10.10.1/32 is directly connected, ADVPN
C       10.10.10.2/32 is directly connected, ADVPN_0
C       10.10.10.3/32 is directly connected, ADVPN
              is directly connected, ADVPN_0
B       172.16.1.0/24 [200/0] via 10.10.10.1, ADVPN, 02:51:03
B       172.16.2.0/24 [200/0] via 10.10.10.2, ADVPN_0, 00:24:15
C       172.16.3.0/24 is directly connected, lan
C       202.3.3.0/24 is directly connected, wan1
  
```

IPsec VPN 和路由的变化与 SPOKE1 同理。此时的 HUB-SPOKE 之间的数据转发为 FULL-MESH 模式，如下图所示：



## 业务访问测试

在 ADVPN 触发前，Spoke1 访问 Spoke2 的数据实际上被转发到了 HUB 上，HUB 感知到了是可以走 ADVPN 的数据流，ADVPN 被触发发送 IKE 消息告知 Spoke1 去 IPsec 连接 Spoke2，让他们之间形成一条直连的 IPsec 隧道，然后相互的业务流量就直接走这条动态协商出来的隧道了，不再经过 HUB。

SPOKE1 (172.16.2.2) 访问 HUB (172.16.1.2)：

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 172.16.2.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.2.1

C:\>ping 172.16.1.2 -t      Spoke1访问Hub网段

Pinging 172.16.1.2 with 32 bytes of data:

Reply from 172.16.1.2: bytes=32 time=2ms TTL=126
Reply from 172.16.1.2: bytes=32 time=2ms TTL=126
Reply from 172.16.1.2: bytes=32 time=1ms TTL=126
```

SPOKE1 (172.16.2.2) 访问 SPOKE2 (172.16.3.2)

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 172.16.2.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.2.1

C:\>ping 172.16.3.2 -t      Spoke1访问Spoke2网段

Pinging 172.16.3.2 with 32 bytes of data:

Reply from 172.16.3.2: bytes=32 time=2ms TTL=126
Reply from 172.16.3.2: bytes=32 time=2ms TTL=126
Reply from 172.16.3.2: bytes=32 time=2ms TTL=126
```

Debug Flow 一下 SPOKE1 (172.16.2.2) 访问 SPOKE2 (172.16.3.2)：

//

diagnose debug flow filter addr 172.16.2.2

```
diagnose debug flow filter proto 1
diagnose debug flow show console enable
diagnose debug flow show function-name enable
diagnose debug flow trace start 1
diagnose debug enable
//

FGT60D4614022596 # id=20085 trace_id=1 func=print_pkt_detail line=4743
msg="vd-root received a packet(proto=1, 172.16.2.2:512->172.16.3.2:2048) from
internal. type=8, code=0, id=512, seq=38664."
id=20085 trace_id=1 func=init_ip_session_common line=4894 msg="allocate a new
session-0000c6d9"
id=20085 trace_id=1 func=vf_ip4_route_input line=1597 msg="find a route:
flags=00000000 gw-10.10.10.3 via ADVPN_0"
id=20085 trace_id=1 func=fw_forward_handler line=700 msg="Allowed by Policy-3:"
id=20085 trace_id=1 func=ipsecdev_hard_start_xmit line=122 msg="enter IPsec
interface-ADVPN_0" (数据从动态建立的 ADVPN_0 转发出去)
id=20085 trace_id=1 func=esp_output4 line=1152 msg="IPsec encrypt/auth"
id=20085 trace_id=1 func=ipsec_output_finish line=519 msg="send to 202.2.2.254
via intf-wan1"
id=20085 trace_id=2 func=print_pkt_detail line=4743 msg="vd-root received a
packet(proto=1, 172.16.3.2:512->172.16.2.2:0) from ADVPN_0. type=0, code=0,
id=512, seq=38664."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=4807 msg="Find an existing
session, id-0000c6d9, reply direction"
id=20085 trace_id=2 func=vf_ip4_route_input line=1597 msg="find a route:
flags=00000000 gw-172.16.2.2 via internal"
id=20085 trace_id=2 func=npu_handle_session44 line=904 msg="Trying to offloading
session from ADVPN_0 to internal, skb.npu_flag=00000000 ses.state=00010200
ses.npu_state=0x00000000"
```

**SPOKE2 (172.16.3.2) 访问 HUB (172.16.1.2) :**



```
Ethernet adapter Internet_Card:

Connection-specific DNS Suffix  . :
IP Address. . . . . : 172.16.3.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.3.1

C:\>ping 172.16.1.2    Spoke2访问Hub网段

Pinging 172.16.1.2 with 32 bytes of data:

Reply from 172.16.1.2: bytes=32 time=1ms TTL=126
Reply from 172.16.1.2: bytes=32 time=1ms TTL=126
Reply from 172.16.1.2: bytes=32 time=1ms TTL=126
```

SPOKE2 (172.16.3.2) 访问 SPOKE1 (172.16.2.2)

```
Ethernet adapter Internet_Card:

Connection-specific DNS Suffix  . :
IP Address. . . . . : 172.16.3.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.3.1

C:\>ping 172.16.2.2    Spoke2访问Spoke1网段

Pinging 172.16.2.2 with 32 bytes of data:

Reply from 172.16.2.2: bytes=32 time=2ms TTL=126
Reply from 172.16.2.2: bytes=32 time=1ms TTL=126
Reply from 172.16.2.2: bytes=32 time=2ms TTL=126
```

Debug Flow 一下 SPOKE2 (172.16.3.2) 访问 SPOKE1 (172.16.2.2):

```
//
diagnose debug flow filter addr 172.16.3.2
diagnose debug flow filter proto 1
diagnose debug flow show console enable
diagnose debug flow show function-name enable
diagnose debug flow trace start 1
diagnose debug enable
//
FG240D4614802169 # id=20085 trace_id=1 func=print_pkt_detail line=4743
msg="vd-root received a packet(proto=1, 172.16.3.2:768->172.16.2.2:2048) from
lan. type=8, code=0, id=768, seq=37961."
id=20085 trace_id=1 func=init_ip_session_common line=4894 msg="allocate a new
session-469269fc"
id=20085 trace_id=1 func=vf_ip4_route_input line=1597 msg="find a route:
flags=00000000 gw-10.10.10.2 via ADVPN_0"
id=20085 trace_id=1 func=fw_forward_handler line=700 msg="Allowed by Policy-2:"
id=20085 trace_id=1 func=ipsecdev_hard_start_xmit line=122 msg="enter IPsec
```

```
interface-ADVPN_0"      (数据从动态建立的 ADVPN_0 转发出去)
id=20085 trace_id=1 func=esp_output4 line=1152 msg="IPsec encrypt/auth"
id=20085 trace_id=1 func=ipsec_output_finish line=519 msg="send to 202.3.3.254
via intf-wan1"
id=20085 trace_id=2 func=print_pkt_detail line=4743 msg="vd-root received a
packet(proto=1, 172.16.2.2:768->172.16.3.2:0) from ADVPN_0. type=0, code=0,
id=768, seq=37961."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=4807 msg="Find an existing
session, id=469269fc, reply direction"
id=20085 trace_id=2 func=vf_ip4_route_input line=1597 msg="find a route:
flags=00000000 gw=172.16.3.2 via lan"
id=20085 trace_id=2 func=npu_handle_session44 line=904 msg="Trying to offloading
session from ADVPN_0 to lan, skb.npu_flag=00000000 ses.state=00010200
ses.npu_state=0x00000000"
```

## RIP v2 方式的 ADVPN（补充）

### HUB、Spoke1、Spoke2 之间使用 RIP v2

在之前描述的基础上，IPsec VPN 等配置均不需要修改，只需要将 BGP 改成 RIP 即可。

#### **HUB 删除 BGP 配置：**

```
config router bgp
    unset as
    unset router-id
    config network
        purge
        Do you want to continue? (y/n)y
    end
config neighbor-range
    purge
    Do you want to continue? (y/n)y
    end
config neighbor-group
    purge
    Do you want to continue? (y/n)y
    end
```

#### **SPOKE1 删除 BGP 配置：**

```
config router bgp
    unset as
```

```
unset router-id
config network
    purge
    Do you want to continue? (y/n)y
end
config neighbor
    purge
    Do you want to continue? (y/n)y
End
```

**SPOKE2 删除 BGP 配置:**

```
config router bgp
    unset as
    unset router-id
config network
    purge
    Do you want to continue? (y/n)y
end
config neighbor
    purge
    Do you want to continue? (y/n)y
end
```

// Spoke1 和 Spoke2 上的关于 10.10.10.0/24 这条静态路由在 RIPv2 的环境中可以不需要，可以选择性删除。

```
config router static
    edit 2
        set dst 10.10.10.0 255.255.255.0
        set device "ADVPN" //
```

**HUB 配置 RIP:**

```
config router rip
    config network
        edit 1
            set prefix 10.10.10.0 255.255.255.0
        next
        edit 2
            set prefix 172.16.1.0 255.255.255.0
        next
    end
```

RIP Version ☐ 1 ☒ 2

▶ **Advanced Options**(Defaults, Timers, Route Redistribution)

Apply

Networks		IP/Netmask:	Add
Delete			
<input type="checkbox"/>	IP/Netmask		
<input type="checkbox"/>	10.10.10.0/255.255.255.0		
<input type="checkbox"/>	172.16.1.0/255.255.255.0		

## Spoke1 配置 RIP:

```
config router rip
config network
edit 1
set prefix 10.10.10.0 255.255.255.0
next
edit 2
set prefix 172.16.2.0 255.255.255.0
next
end
```

RIP Version ☐ 1 ☒ 2

▶ **Advanced Options**(Defaults, Timers, Route Redistribution)

Apply

Networks		IP/Netmask:	Add
Delete			
<input type="checkbox"/>	IP/Netmask		
<input type="checkbox"/>	10.10.10.0/255.255.255.0		
<input type="checkbox"/>	172.16.2.0/255.255.255.0		

## Spoke2 配置 RIP:

```
config router rip
config network
edit 1
set prefix 10.10.10.0 255.255.255.0
next
edit 2
set prefix 172.16.3.0 255.255.255.0
next
end
```

RIP Version ☐ 1 ☒ 2

▶ **Advanced Options**(Defaults, Timers, Route Redistribution)

Apply

Networks		IP/Netmask:	Add
Delete			
<input type="checkbox"/>	IP/Netmask		
<input type="checkbox"/>	10.10.10.0/255.255.255.0		
<input type="checkbox"/>	172.16.3.0/255.255.255.0		

## Spoke 之间业务互访前设备状态观察（RIP v2）

SPOKE1 和 SPOKE2 之间无任何流量访问的时候，HUB/SPOKE1/SPOKE2 状态观察：

### HUB 状态

HUB IPsec VPN 建立情况：

Monitor--->IPsec Monitor

Refresh

Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2
ADVPN_0	Custom	202.3.3.1		Up	1.38 kB	1.14 kB	ADVPN
ADVPN_1	Custom	202.2.2.1		Up	1.09 kB	880 B	ADVPN

HUB 路由学习情况：

Monitor--->Routing Monitor

Refresh Route Lookup

Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	202.1.1.254	wan1	
Connected		10.10.10.1/32	0.0.0.0	ADVPN_0	
Connected		10.10.10.1/32	0.0.0.0	ADVPN_1	
Connected		10.10.10.2/32	0.0.0.0	ADVPN_1	
Connected		10.10.10.3/32	0.0.0.0	ADVPN_0	
Connected		172.16.1.0/24	0.0.0.0	lan	
RIP		172.16.2.0/24	10.10.10.2	ADVPN_1	0 00:04:18
RIP		172.16.3.0/24	10.10.10.3	ADVPN_0	0 00:04:24
Connected		202.1.1.0/24	0.0.0.0	wan1	

### SPOKE1 状态

SPOKE1 IPsec VPN 建立情况（只和 HUB 建立 IPsec）：

Monitor--->IPsec Monitor

Refresh

Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2
ADVPN	Custom	202.1.1.1		Up	11.35 kB	7.16 kB	ADVPN

SPOKE1 路由学习情况：

Monitor--->Routing Monitor

Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	202.2.2.254	wan1	
Connected		10.10.10.1/32	0.0.0.0	ADVPN	
Connected		10.10.10.2/32	0.0.0.0	ADVPN	
RIP		172.16.1.0/24	10.10.10.1	ADVPN	0 00:12:07
Connected		172.16.2.0/24	0.0.0.0	internal	
RIP		172.16.3.0/24	10.10.10.1	ADVPN	0 00:12:07
Connected		202.2.2.0/24	0.0.0.0	wan1	

业务路由全部指向 HUB。

## SPOKE2 状态

SPOKE2 IPsec VPN 建立情况（只和 HUB 建立 IPsec）：

Monitor--->IPsec Monitor

Refresh							
Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2
ADVPN	Custom	202.1.1.1		Up	975.01 kB	607.73 kB	ADVPN

SPOKE2 路由学习情况：

Monitor--->Routing Monitor

Refresh

Route Lookup

Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	202.3.3.254	wan1	
Connected		10.10.10.1/32	0.0.0.0	ADVPN	
Connected		10.10.10.3/32	0.0.0.0	ADVPN	
RIP		172.16.1.0/24	10.10.10.1	ADVPN	0 00:13:23
RIP		172.16.2.0/24	10.10.10.1	ADVPN	0 00:13:14
Connected		172.16.3.0/24	0.0.0.0	lan	
Connected		202.3.3.0/24	0.0.0.0	wan1	

业务路由全部指向 HUB。

## Spoke 之间业务互访后设备状态观察（RIP v2）

一旦发起 SPOKE1 与 SPOKE2 之间的互访将立马触发 ADVPN 机制，使得 SPOKE1 和 SPOKE2 之间动态协商出一条直连的 IPsec VPN 隧道。接下来我们观察一下，SPOKE1 和 SPOKE2 有流量访问并触发建立了动态 IPsec VPN 隧道时 HUB/SPOKE1/SPOKE2 的状态：

## HUB 状态

HUB IPsec VPN 建立情况：

Monitor--->IPsec Monitor

Refresh							
Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2
ADVPN_0	Custom	202.3.3.1		Up	6.90 kB	4.45 kB	ADVPN
ADVPN_1	Custom	202.2.2.1		Up	17.55 kB	9.71 kB	ADVPN

HUB 路由学习情况：

Monitor--->Routing Monitor

Refresh Route Lookup

Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	202.1.1.254	wan1	
Connected		10.10.10.1/32	0.0.0.0	ADVPN_0	
Connected		10.10.10.1/32	0.0.0.0	ADVPN_1	
Connected		10.10.10.2/32	0.0.0.0	ADVPN_1	
Connected		10.10.10.3/32	0.0.0.0	ADVPN_0	
Connected		172.16.1.0/24	0.0.0.0	lan	
RIP		172.16.2.0/24	10.10.10.2	ADVPN_1	0 00:16:13
RIP		172.16.3.0/24	10.10.10.3	ADVPN_0	0 00:16:19
Connected		202.1.1.0/24	0.0.0.0	wan1	

可以看出 HUB 端没有任何变化。变化主要在 SPOKE 端。

## SPOKE1 状态

SPOKE1 IPsec VPN 建立情况:

Monitor--->IPsec Monitor

Refresh Spoke1与Spoke2之间建立的动态IPsec VPN隧道

Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2
ADVPN_0	Custom	202.3.3.1		Up	14.40 kB	7.23 kB	ADVPN
ADVPN	Custom	202.1.1.1		Up	33.78 kB	18.99 kB	ADVPN

SPOKE1 路由学习情况:

Monitor--->Routing Monitor

Refresh Route Lookup

Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	202.2.2.254	wan1	
Connected		10.10.10.1/32	0.0.0.0	ADVPN	
Connected		10.10.10.2/32	0.0.0.0	ADVPN	
Connected		10.10.10.2/32	0.0.0.0	ADVPN_0	
Connected		10.10.10.3/32	0.0.0.0	ADVPN_0	
RIP		172.16.1.0/24	10.10.10.1	ADVPN	0 00:18:05
Connected		172.16.2.0/24	0.0.0.0	internal	
RIP		172.16.3.0/24	10.10.10.3	ADVPN_0	0 00:03:13
Connected		202.2.2.0/24	0.0.0.0	wan1	

重新收敛了 RIP 路由, 去往 172.16.3.0 的业务路由指向了 Spoke2 (10.10.10.3 ADVPN\_0)。

## SPOKE2 状态

SPOKE2 IPsec VPN 建立情况:

Monitor--->IPsec Monitor

Refresh Spoke2和Spoke1之间建立的动态IPsec VPN隧道

Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2
ADVPN_0	Custom	202.2.2.1		Up	35.22 kB	17.81 kB	ADVPN
ADVPN	Custom	202.1.1.1		Up	977.70 kB	609.37 kB	ADVPN

SPOKE2 路由学习情况:

Monitor--->Routing Monitor

Refresh		Route Lookup			
Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	202.3.3.254	wan1	
Connected		10.10.10.1/32	0.0.0.0	ADVPN	
Connected		10.10.10.2/32	0.0.0.0	ADVPN_0	
Connected		10.10.10.3/32	0.0.0.0	ADVPN	
Connected		10.10.10.3/32	0.0.0.0	ADVPN_0	
RIP		172.16.1.0/24	10.10.10.1	ADVPN	0 00:20:26
RIP		172.16.2.0/24	10.10.10.2	ADVPN_0	0 00:05:23
Connected		172.16.3.0/24	0.0.0.0	lan	
Connected		202.3.3.0/24	0.0.0.0	wan1	

重新收敛了 RIP 路由，去往 172.16.2.0 的业务路由指向了 Spoke1（10.10.10.2 ADVPN\_0）。

**RIP 方式的 ADVPN 业务测试与 BGP 方式的 ADVPN 一致，不再进一步描述。**

## FAQ

### 1. 问：为何文档中没有提到最常用的 OSPF 路由协议，ADVPN 中是否不支持 OSPF？

答：是，Forti5.4 暂不支持 OSPF。

因为 IPsec Tunnel 是点对点的隧道，OSPF 的接口类型也固定为 P2P，不能修改为广播或点对多点，因此 HUB 侧无法使用 OSPF 进行多点间的路由连接，这也是不使用 OSPF 的原因。

### 2. 问：HUB 和 SPOKE 是否支持置于 NAT 设备后，是否支持 NAT-T？

答：支持，从 FortiOS5.4（Build 1001）开始就支持 HUB/SPOKE 置于 NAT 后面，建议外网的 NAT 设备最好使用“一对一 NAT”尽量不要使用“目的 NAT”，防止外网 NAT 设备有会话保持有些情况下可能引起 IPsec 协商异常。有 NAT 穿越的 SPOKE 会多进行一次 NAT-T 的协商，业务转发报文都将使用 UDP4500 进行封装。ADVPN 触发的时候，如果是非 NAT 的 Spoke 向 NAT 后的 Spoke 触发流量，HUB 会发送 IKE 信息告诉非 NAT 的 Spoke 对方做了 NAT，而向 NAT 后的 Spoke 发起 IKE 信息，让 NAT 后的 Spoke 发起向非 NAT 后的 Spoke IPsec VPN 连接，做了这样一个反转的操作，这样做的原因是 ADVPN 设计之初本不能支持 Spoke 做 NAT。

**注意：**关于 ADVPN 的 Spoke 处于 NAT 后的使用，还是有一些限制，目前只支持其中一个 SPOKE 处于 NAT 后。如果两个 SPOKE 同时都处于 NAT 后，这样 ADVPN 是不支持的，没办法触发两个 Spoke 之间发起 IPsec 连接，这样的情况下会通过 HUB 中转这两个 Spoke 之间的业务流量。HUB 端是否处于 NAT 设备后面，则没有限制。FortiOS 软件也在持续更新中，至于后续功能的可能变化还请大家关注 OS 版本的更新情况。

### 参考文档资料：

The Fortinet CookBook --- Configuring ADVPN in FortiOS 5.4 (Expert)

<http://cookbook.fortinet.com/configuring-advpn-in-fortios-5-4-dynamic-hub-and-spoke-vpns/>

<https://fuse.fortinet.com/p/fo/st/topic=370&post=7176#p7176>