

# 前言

基于国家安全和经济发展的客观需求,在安全产品中采用国密算法,确保网络通信自主安全十分必要。通过将 IPSec 协议中的默认非对称协商算法、哈希算法和对称加密算法分别采用国密设计,采用国密算法来满足需求, Panabit 采用的国密认证算法 SM3, 加密算法 SM4 为验证 Panabit 设备, 国密后的互联效果进行本次实验测试。

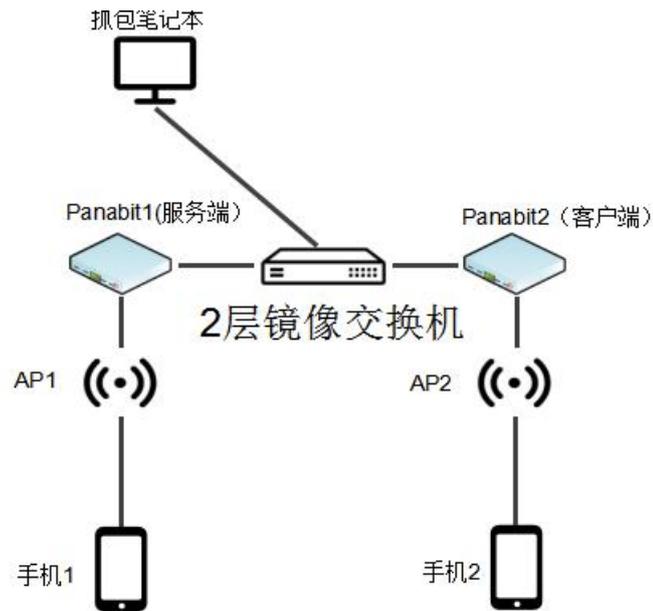
## IPSec 国密使用实测试验

### 1. 准备实验材料设备清单

设备名称	数量	作用
Panabit 设备	2	起 IPSec 隧道并采用国密算法
手机设备	2	业务 ping 测互通
AP 设备	2	发送无线数据让手机入网
笔记本电脑	1	SD-WAN 封装数据包并留存
2 层镜像交换机	1	流量镜像

### 2. 测试拓扑

本次测试拓扑如下图:



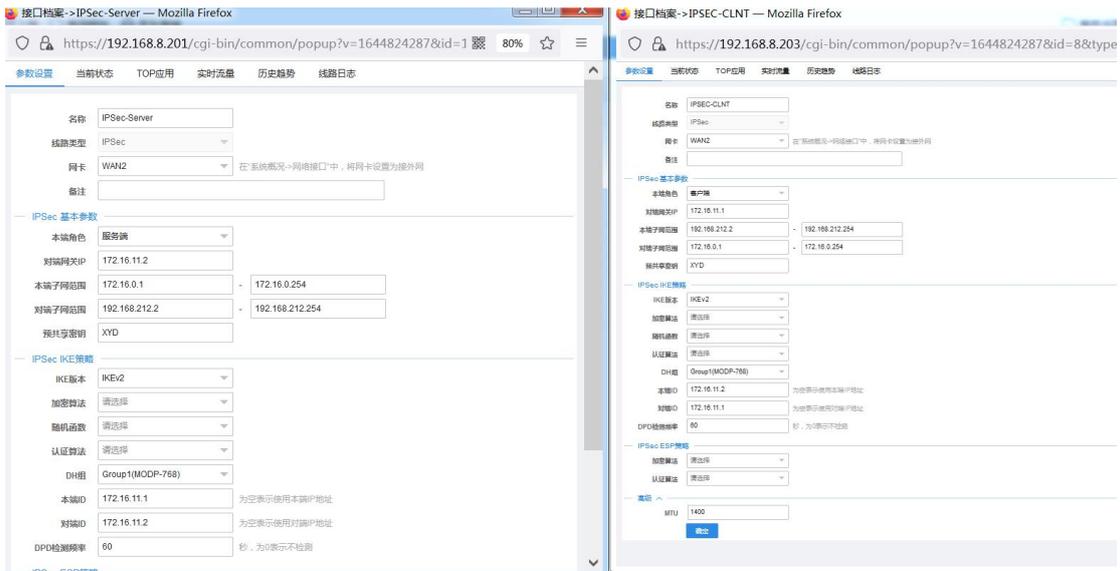
### 组网说明:

- 1) Panabit 设备 1 作为 IPSCE 服务端加密算法为国密 4 与 SD-WAN 盒子 2 进行互联;
- 2) Panabit 设备 2 作为 IPSCE 客户端加密算法为国密 4 与 SD-WAN 盒子 1 进行互联;
- 3) 每台 Panabit 设备下, 下挂 AP 及手机互为 ping 测对象;
- 4) 二层交换机镜像流量发送给抓包笔记本
- 5) 抓包笔记本对封装加密数据进行抓包保存。

## 3. 基础配置

- 1) Panabit 设备 1 创建承载 IPsec 线路, IP 地址为: 172.16.11.1
- 2) Panabit 设备 2 创建承载 IPsec 线路, IP 地址为: 172.16.11.2
- 3) Panabit 设备 1 创建 IPsec 服务端
- 4) Panabit 设备 2 创建 IPsec 客户端

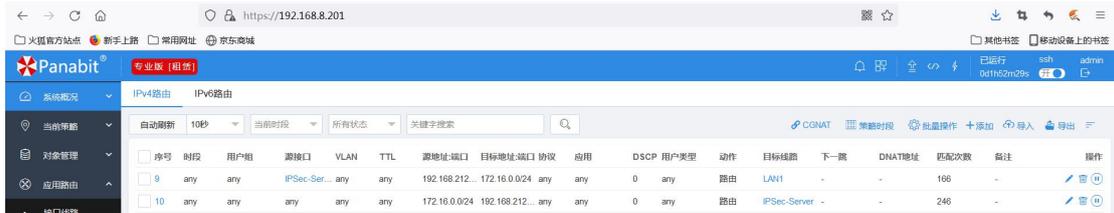
IPsec 配置截图:



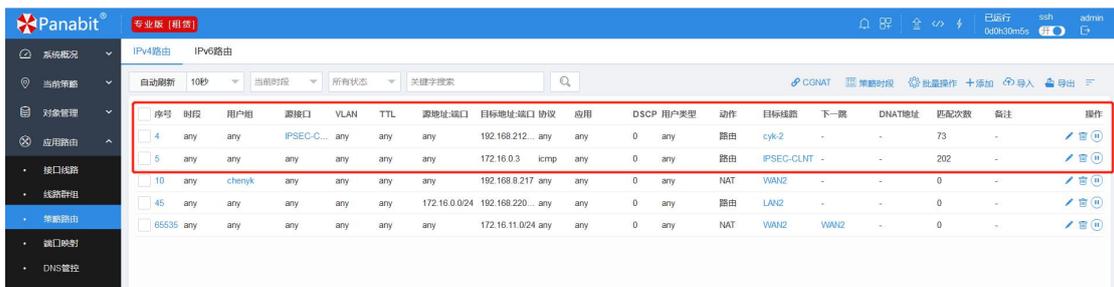
Panabit 设备 1 和 Panabit 设备 2 配置策略路由互通设置

策略路由互通设置截图：

服务端策略路由配置



客户端策略路由配置



加密算法国密 4 截图：

服务端国密配置

WEB终端 — Mozilla Firefox

https://192.168.8.201/cgi-bin/common/popup?v=1644824287&pop\_title=WEB终端&pop\_route=system/termi

```
ifname=WAN2
interface_name=em4
ifstatus=up
role=responder
addr=172.16.11.1
peer_addr=172.16.11.2
vlan=0
vlan1=0
my_net=172.16.0.1-172.16.0.254
peer_net=192.168.212.2-192.168.212.254
psk=XYD
ike_version=2
ike_mode=main
ike_encr=SM4-CBC
ike_prf=SM3
ike_auth=SM3
ike_dh=Group1(MODP-768)
ike_live=28800
my_id=172.16.11.1
peer_id=172.16.11.2
dpd_freq=60
esp_encr=SM4-CBC
esp_auth=SM3
esp_dh=none
esp_live=3600
my_port=0
peer_nat_port=4500
peer_nat_addr=172.16.11.2
linkup=1
gatewayup=1
gateway=172.16.11.2
gwmac=b0-1c-6d-b3-00-00
flowcnt=1
dnsaddr=0.0.0.0
dnsreqs=0
dnstimeouts=0
dnsokper=0
snatdrop=0
pingip=0.0.0.0
pingip2=0.0.0.0
minping=0
maxping=0
curping=0
gottime=0
hismtts=0
floweye
```

## 客户端国密配置

```
ifname=WAN2
interface_name=pa4
ifstatus=up
role=initiator
addr=172.16.11.2
peer_addr=172.16.11.1
vlan=0
vlan1=0
my_net=192.168.212.2-192.168.212.254
peer_net=172.16.0.1-172.16.0.254
psk=XYD
ike_version=2
ike_mode=main
ike_encr=SM4-CBC
ike_prf=SM3
ike_auth=SM3
ike_dh=Group1(MODP-768)
ike_live=28800
my_id=172.16.11.2
peer_id=172.16.11.1
dpd_freq=60
esp_encr=SM4-CBC
esp_auth=SM3
esp_dh=none
esp_live=3600
my_port=0
peer_nat_port=4500
peer_nat_addr=172.16.11.1
linkup=1
gatewayup=1
gateway=172.16.11.1
gwmac=b0-fd-48-5e-00-40
flowcnt=0
dnsaddr=0.0.0.0
dnsreqs=0
dnstimeouts=0
dnsokper=0
snatdrop=0
pingip=0.0.0.0
pingip2=0.0.0.0
minping=0
maxping=0
curping=0
gottime=0
bigpkts=0
```

## 4. 测试结果

手机经过 IPSCE 隧道连通测试，互通正常。

**互通 ping 测手机截图：**



图示：客户端截图



图示：服务端截图

Panabit 设备观察连通性正常

Panabit 设备观察结果截图：

服务端

应用	协议	状态	首包接口	连接	地理位置	策略路由	接口线路	时长	客户时延	服务时延	应用时延	上行报文	下行报文	最大包长	MSS	流量
ICMP	icmp	NIL	LAN1/em1	源:172.16.0.3:10335 目:192.168.212.3:1	10	IPSec-Ser...	0	0.00	0.00	39.33	0/1	0/1	98/98	0	98/98	
ICMP	icmp	NIL	IPSec-Ser...	源:192.168.212.3:11779 目:172.16.0.3:1	9	LAN1	1	0.00	0.00	311.44	0/1	0/1	126/98	0	126/98	
ICMP	icmp	NIL	LAN1/em1	源:172.16.0.3:10334 目:192.168.212.3:1	10	IPSec-Ser...	2	0.00	0.00	3.01	0/1	0/1	98/98	0	98/98	
ICMP	icmp	NIL	IPSec-Ser...	源:192.168.212.3:11778 目:172.16.0.3:1	9	LAN1	2	0.00	0.00	421.31	0/1	0/1	126/98	0	126/98	
ICMP	icmp	NIL	LAN1/em1	源:172.16.0.3:10333 目:192.168.212.3:1	10	IPSec-Ser...	3	0.00	0.00	41.71	0/1	0/1	98/98	0	98/98	
ICMP	icmp	NIL	IPSec-Ser...	源:192.168.212.3:11777 目:172.16.0.3:1	9	LAN1	4	0.00	0.00	168.41	0/1	0/1	126/98	0	126/98	

客户端

应用	协议	状态	首包接口	连接	地理位置	策略路由	接口线路	时长	客户时延	服务时延	应用时延	上行报文	下行报文	最大包长	MSS	流量	HOST
ICMP	icmp	NIL	cyk-2/pa3	源:192.168.212.3:11552 目:172.16.0.3:1	5	IPSEC-CLINT	1	0.00	0.00	68.50	0/1	0/1	98/98	0	98/98		
ICMP	icmp	NIL	cyk-2/pa3	源:192.168.212.3:11551 目:172.16.0.3:1	5	IPSEC-CLINT	2	0.00	0.00	61.82	0/1	0/1	98/98	0	98/98		
ICMP	icmp	NIL	cyk-2/pa3	源:192.168.212.3:11550 目:172.16.0.3:1	5	IPSEC-CLINT	3	0.00	0.00	30.93	0/1	0/1	98/98	0	98/98		

笔记本电脑抓包观察数据包国密加密正常

抓包截图：

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	b0:fd:48:5e:00:a0	Broadcast	ARP	60	Who has 1.1.1.2? Tell 1.1.1.1
2	0.000241	b0:fd:48:5e:00:d0	Broadcast	ARP	60	Who has 200.1.1.254? Tell 200.1.1.1
3	0.462296	172.16.11.1	172.16.11.2	UDP	126	60158 → 8001 Len=84
4	0.462369	172.16.11.1	172.16.11.2	UDP	102	60158 → 8001 Len=60
5	0.462573	172.16.11.1	172.16.11.2	ESP	146	ESP (SPI=0xab3a2e3)
6	0.483432	172.16.11.1	172.16.11.2	UDP	120	60158 → 8001 Len=78
7	0.483824	172.16.11.1	172.16.11.2	UDP	120	60158 → 8001 Len=78
8	0.556909	172.16.11.1	172.16.11.2	ESP	146	ESP (SPI=0xab3a2e3)
9	0.556927	172.16.11.2	172.16.11.1	ESP	146	ESP (SPI=0x93f4eab8)
10	0.563107	172.16.11.2	172.16.11.1	ESP	146	ESP (SPI=0x93f4eab8)
11	0.847696	172.16.11.1	172.16.11.2	UDP	117	60158 → 8001 Len=75
12	1.000017	b0:fd:48:5e:00:a0	Broadcast	ARP	60	Who has 1.1.1.2? Tell 1.1.1.1
13	1.000267	b0:fd:48:5e:00:d0	Broadcast	ARP	60	Who has 200.1.1.254? Tell 200.1.1.1
14	1.077615	172.16.11.1	172.16.11.2	UDP	118	60158 → 8001 Len=76
15	1.206395	172.16.11.1	172.16.11.2	UDP	108	60158 → 8001 Len=66
16	1.221233	10.18.18.250	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
17	1.221420	10.18.18.250	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1

```

Header Checksum: 0x79d5 [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.16.11.1
Destination Address: 172.16.11.2
User Datagram Protocol, Src Port: 4500, Dst Port: 4500
Source Port: 4500
Destination Port: 4500
Length: 112
[checksum: [missing]]
[checksum status: Not present]
[Stream index: 1]
[Timestamps]
UDP payload (104 bytes)
UDP Encapsulation of IPsec Packets
Encapsulating Security Payload
ESP SPI: 0xab3a2e3 (2879620003)
ESP Sequence: 1243

```

## 附带抓包文件



IPSC.E.pcapng

## 测试总结

本实验通过实践，证明 Panabit 提供的国密算法，进行方案组网，连通性无任何问题，实践证明,通过 Panabit 设备能够有效满足国密组网需求。