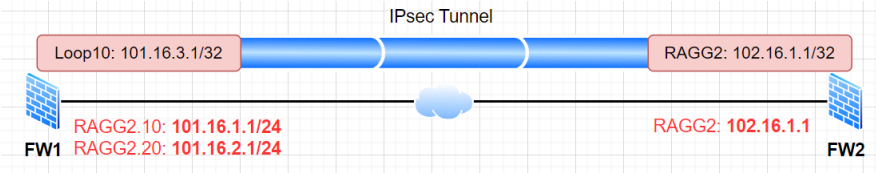
中低端防火墙单机等价双出口链路IPsec典型配置

IPSec VPN 孔凡安 2024-01-25 发表

组网及说明

理想组网如下：



FW1作为公网出口，存在等价双链路，和对端FW2设备建立IPsec隧道。

实际环境模拟公网用SW代替，通过OSPF动态路由协议打通设备间路由，FW上配置环回口Loop1模拟客户端流量。安全域及安全策略本案例不涉及，省略。

配置步骤

相关配置如下：

	FW1	FW2
IP、接口、路由基本配置	# interface LoopBack0 ip address 16.1.1.1 255.255.255.255 ---ospf router-id # interface LoopBack1 ip address 192.168.106.1 255.255.255.255 ---感兴趣流 # interface LoopBack10 ip address 101.16.3.1 255.255.255.255 ---隧道起点 # interface Route-Aggregation2.10 description ipsec_1 ip address 101.16.1.1 255.255.255.0 ospf network-type p2p vlan-type dot1q vid 10 ipsec apply policy ply # interface Route-Aggregation2.20 description ipsec_2 ip address 101.16.2.1 255.255.255.0 ospf network-type p2p vlan-type dot1q vid 20 ipsec apply policy ply # ospf 1 router-id 16.1.1.1 import-route direct route-policy ipsec ---将环回口地址引入到ospf中 area 0.0.0.0 network 101.16.1.0 0.0.0.255 network 101.16.2.0 0.0.0.255 # route-policy ipsec permit node 10 if-match ip address prefix-list ipsec # ip prefix-list ipsec index 10 permit 101.16.3.1 32 #	# interface LoopBack0 ip address 16.1.1.2 255.255.255.255 ---ospf router-id # interface LoopBack1 ip address 192.168.206.1 255.255.255.255 ---感兴趣流 # interface Route-Aggregation2 ip address 102.16.1.1 255.255.255.0 ---隧道终点 ospf network-type p2p ipsec apply policy ply # # ospf 1 router-id 16.1.1.2 area 0.0.0.0 network 102.16.1.0 0.0.0.255 #
Ike keychain配置	# ike keychain k1 pre-shared-key address 102.16.1.1 255.255.255.255 key cipher c3$WeDkyPg7q6q1PRMNDknQp4zQ0eWxZB0zdw== #	# ike keychain k1 pre-shared-key address 101.16.3.1 255.255.255.255 key cipher c3$/J6Q33LbK9vq57CUNIR/roA7qrZStXhR3w== #
Ike profile	# ike profile pf keychain k1 dpd interval 10 on-demand local-identity address 101.16.3.1 match remote identity address 102.16.1.1 255.255.255.255 #	# ike profile pf keychain k1 dpd interval 10 on-demand local-identity address 102.16.1.1 match remote identity address 101.16.3.1 255.255.255.255 #

IPsec policy	# acl advanced 3000 rule 0 permit ip source 192.168.106.1 0 destination 192.168.206.1 0 # ipsec policy ply 1 isakmp transform-set ts security acl 3000 local-address 101.16.3.1 ---一定要指定本端地址，不然缺省以 接口地址发送报文 remote-address 102.16.1.1 ike-profile pf # ipsec policy ply local-address LoopBack10 ---指定IPsec安全策略与Loop10进行绑定 #	# acl advanced 3000 rule 0 permit ip source 192.168.206.1 0 destination 192.168.106.1 0 # ipsec policy ply 1 isakmp transform-set ts security acl 3000 remote-address 101.16.3.1 ike-profile pf #

SW配置也罗列下，供参考：

```
#
interface LoopBack0
 ip address 68.1.1.1 255.255.255.255
#
interface Vlan-interface10
 ip address 101.16.1.2 255.255.255.0
 ospf network-type p2p
#
interface Vlan-interface20
 ip address 101.16.2.2 255.255.255.0
 ospf network-type p2p
#
interface Vlan-interface100
 ip address 102.16.1.2 255.255.255.0
 ospf network-type p2p
#
ospf 1 router-id 68.1.1.1
 default-route-advertise always
 area 0.0.0.0
  network 101.16.1.0 0.0.0.255
  network 101.16.2.0 0.0.0.255
  network 102.16.1.0 0.0.0.255
#
```

配置关键点

关键点表格已列出，实验室测试单机收发加密ESP报文不在同一接口业务正常，但案例仅供参考。

	Time	Source	Destination	Protoc	Time to	Identification	Tota	ID	Info
1	2024-01-25 02:40:43.496218	101.16.3.1	102.16.1.1	ESP	255	0x7495 (29845)	156	10	ESP (SPI=0x2d0a04ad)
2	2024-01-25 02:40:43.496578	102.16.1.1	101.16.3.1	ESP	254	0x11e6 (4582)	156	20	ESP (SPI=0x8a733cd7)
3	2024-01-25 02:40:43.697498	101.16.3.1	102.16.1.1	ESP	255	0x7499 (29849)	156	10	ESP (SPI=0x2d0a04ad)
4	2024-01-25 02:40:43.697652	102.16.1.1	101.16.3.1	ESP	254	0x11e9 (4585)	156	20	ESP (SPI=0x8a733cd7)
5	2024-01-25 02:40:43.898125	101.16.3.1	102.16.1.1	ESP	255	0x749c (29852)	156	10	ESP (SPI=0x2d0a04ad)
6	2024-01-25 02:40:43.898252	102.16.1.1	101.16.3.1	ESP	254	0x11eb (4587)	156	20	ESP (SPI=0x8a733cd7)
7	2024-01-25 02:40:44.098684	101.16.3.1	102.16.1.1	ESP	255	0x74a0 (29856)	156	10	ESP (SPI=0x2d0a04ad)
8	2024-01-25 02:40:44.098806	102.16.1.1	101.16.3.1	ESP	254	0x11ed (4589)	156	20	ESP (SPI=0x8a733cd7)
9	2024-01-25 02:40:44.299275	101.16.3.1	102.16.1.1	ESP	255	0x74a5 (29861)	156	10	ESP (SPI=0x2d0a04ad)
10	2024-01-25 02:40:44.299405	102.16.1.1	101.16.3.1	ESP	254	0x11ef (4591)	156	20	ESP (SPI=0x8a733cd7)

vlan:id

对应 IPsec SA：

Interface: LoopBack10 ---下发接口为Loop接口

IPsec policy: ply

Sequence number: 1

Mode: ISAKMP

Tunnel id: 1

Encapsulation mode: tunnel

Perfect Forward Secrecy:

Inside VPN:

Extended Sequence Numbers enable: N

Traffic Flow Confidentiality enable: N

```
  Transmitting entity: Responder
  Path MTU: 1460
  Tunnel:
    local  address: 101.16.3.1
    remote address: 102.16.1.1
  Flow:
    sour addr: 192.168.106.1/255.255.255.255  port: 0  protocol: ip
    dest addr: 192.168.206.1/255.255.255.255  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 1552869680 (0x5c8ee930)
    Connection ID: 1138166333442
    Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843200/2627
    Max received sequence-number: 0
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

  [Outbound ESP SAs]
    SPI: 2575420673 (0x9981cd01)
    Connection ID: 1138166333443
    Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843200/2627
    Max sent sequence-number: 0
    UDP encapsulation used for NAT traversal: N

    Status: Active
```

对应IKE SA信息：

```
  -----------------------------------------------
  Connection ID: 12
  Outside VPN:
  Inside VPN:
  Profile: pf
  Transmitting entity: Responder
  Initiator COOKIE: 6658e2b12d9faafb
  Responder COOKIE: f08a4ec966e88d24
  -----------------------------------------------
  Local IP/port: 101.16.3.1/500
  Local ID type: IPV4_ADDR
  Local ID: 101.16.3.1

  Remote IP/port: 102.16.1.1/500
  Remote ID type: IPV4_ADDR
  Remote ID: 102.16.1.1

  Authentication-method: PRE-SHARED-KEY
  Authentication-algorithm: SHA1
  Encryption-algorithm: DES-CBC

  Life duration(sec): 86400
  Remaining key duration(sec): 71948
  Exchange-mode: Main
  Diffie-Hellman group: Group 1
  NAT traversal: Not detected

  Extend authentication: Disabled
  Assigned IP address:
  Vendor ID index:0xffffffff

  Vendor ID sequence number:0x0
```