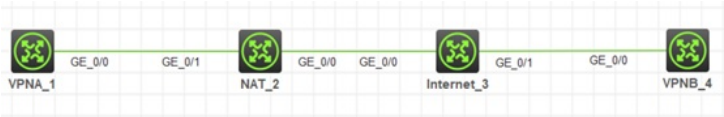
IPSec NAT穿越典型配置案例

IPSec VPN 孙轶宁 2020-12-14 发表

组网及说明



在内网的VPNA与在公网的VPNB建立IPSec隧道

配置步骤

1. VPNA配置

```
interface LoopBack0 # 配置内网接口
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet0/0 # 配置物理接口
 ip address 192.168.1.2 255.255.255.0
 ipsec apply policy ipsec # 绑定IPSec策略
#
ip route-static 0.0.0.0 0 192.168.1.1 # 配置静态路由
#
acl advanced 3000 # 配置IPSec感兴趣流
 rule 10 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
#
ipsec transform-set ipsec # 配置IPSec转换集
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha1
#
ipsec policy ipsec 10 isakmp # 配置IPSec策略
 transform-set ipsec
 security acl 3000
 remote-address 200.200.200.2 # 非模板模式必须指定对端地址
 ike-profile ike
#
 ike identity fqdn vpna # 配置IKE name
#
ike profile ike # 配置IKE对等体
 keychain ike
 exchange-mode aggressive
 match remote identity address 200.200.200.2 255.255.255.255
#
ike keychain ike # 配置IKE预共享密钥
 pre-shared-key address 200.200.200.2 255.255.255.255 key simple ipsec
```

2. VPNB配置

```
interface LoopBack0 # 配置内网接口
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet0/0 # 配置外网接口
 ip address 200.200.200.2 255.255.255.252
 ipsec apply policy ipsec # 绑定IPSec策略
#
ip route-static 0.0.0.0 0 200.200.200.1 # 配置静态路由
#
ipsec transform-set ipsec # 配置IPSec转换集
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha1
#
ipsec policy-template ipsec 10 # 配置IPSec策略模板
 transform-set ipsec
 ike-profile ike
```

#
ipsec policy ipsec 10 isakmp template ipsec # 将IPSec策略模板应用到策略中
#
ike profile ike # 配置IKE对等体
 keychain ike
 exchange-mode aggressive
 match remote identity fqdn vpna # 匹配对端name
#
ike keychain ike # 配置IKE预共享密钥
 pre-shared-key hostname vpna key simple ipsec

3、测试

```
<VPNA>ping -a 192.168.2.1 192.168.3.1
Ping 192.168.3.1 (192.168.3.1) from 192.168.2.1: 56 data bytes, press CTRL_C to break
Request time out
56 bytes from 192.168.3.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 192.168.3.1: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 192.168.3.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 192.168.3.1: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 192.168.3.1 ---
5 packet(s) transmitted, 4 packet(s) received, 20.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.250/2.000/0.433 ms
<VPNA>%Feb  6 09:50:24:431 2018 VPNA PING/6/PING_STATISTICS: Ping statistics for 192.16
packet loss, round-trip min/avg/max/std-dev = 1.000/1.250/2.000/0.433 ms.
```

```
<VPNA>dis ike sa v
  ---------------------------------------------
  Connection ID: 2
  Outside VPN:
  Inside VPN:
  Profile: ike
  Transmitting entity: Initiator
  ---------------------------------------------
  Local IP: 192.168.1.2
  Local ID type: FQDN
  Local ID: vpna

  Remote IP: 200.200.200.2
  Remote ID type: IPV4_ADDR
  Remote ID: 200.200.200.2

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

  Life duration(sec): 86400
  Remaining key duration(sec): 86358
  Exchange-mode: Aggressive
  Diffie-Hellman group: Group 1
  NAT traversal: Detected

  Extend authentication: Disabled
  Assigned IP address:
```

```
<VPNB>dis ike sa v
  ---------------------------------------------
  Connection ID: 2
  Outside VPN:
  Inside VPN:
  Profile: ike
  Transmitting entity: Responder
  ---------------------------------------------
  Local IP: 200.200.200.2
  Local ID type: IPV4_ADDR
  Local ID: 200.200.200.2

  Remote IP: 100.100.100.2
  Remote ID type: FQDN
  Remote ID: vpna

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

  Life duration(sec): 86400
  Remaining key duration(sec): 86288
  Exchange-mode: Aggressive
  Diffie-Hellman group: Group 1
  NAT traversal: Detected

  Extend authentication: Disabled
  Assigned IP address:
```

```
<VPNA>dis ipsec sa br
-------------------------------------------------------------------------------
Interface/Global       Dst Address       SPI         Protocol   Status
-------------------------------------------------------------------------------
GE0/0                  200.200.200.2     3288054643  ESP        Active
GE0/0                  192.168.1.2       2352338375  ESP        Active
```

```
<VPNB>dis ipsec sa br
-------------------------------------------------------------------------------
Interface/Global       Dst Address       SPI         Protocol   Status
-------------------------------------------------------------------------------
GE0/0                  100.100.100.2     2352338375  ESP        Active
GE0/0                  200.200.200.2     3288054643  ESP        Active
```

配置关键点

注意模板方式配置的IPSec不能主动触发IPSec SA协商，必须在另一端非模板方式配置的IPSec触发协商。