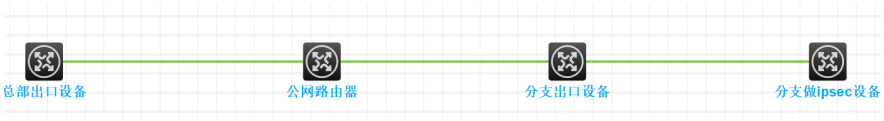
ipsec vpn 两端采用主模式穿越nat

IPSec VPN IPSec VPN zhiliao_Pyc3dM 2023-08-06 发表

组网及说明

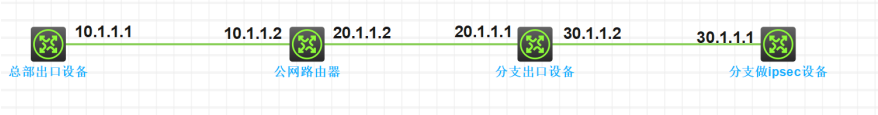
客户2台做ipsec vpn的设备，一台设备在公网，已经有ipsec 配置，现今在某分支内部有需求加入一台ipsec vpn设备与总部的ipsec主模式建立连接，但总部设备无法申请到配置变更时间窗口。拓扑图如下。



问题描述

主模式能否通过nat的网络环境建立ipsec连接?

过程分析



总部ipsec 相关配置：

```
 #
 ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec policy-template zhou 1 transform-set 1 ike-profile 1
 #
 ipsec policy h3c 1 isakmp template zhou
 #
ike profile 1 keychain 1 match remote identity address 0.0.0.0 0.0.0.0 proposal 1
 #
ike proposal 1 encryption-algorithm 3des-cbc authentication-algorithm md5
#
 ike keychain 1 pre-shared-key address 0.0.0.0 0.0.0.0 key cipher
$c$3$T1l9qJ8+TCAB1xIrhB9H0G7tm1vReA== # return
```

解决方法

分支ipsec 配置：

#

ipsec transform-set 1 esp encryption-algorithm 3des-cbc esp authentication-algorithm sha1

#

ipsec policy h3c 1 isakmp transform-set 1 security acl 3000 remote-address 10.1.1.1 ike-profile 1

#

ike profile 1 keychain 1 match remote identity address 10.1.1.1 0.0.0.0 proposal 1

#

ike proposal 1 encryption-algorithm 3des-cbc authentication-algorithm md5

#

ike keychain 1 pre-shared-key address 10.1.1.1 0.0.0.0 key cipher c3$1W4lciAT88WpcGZZRrvznv
cvPgFKFQ==

#

return

ping测试：

[H3C]PING -a 4.4.4.4 1.1.1.1 Ping 1.1.1.1 (1.1.1.1)

from 4.4.4.4: 56 data bytes, press CTRL+C to break Request time out 56 bytes

from 1.1.1.1: icmp_seq=1 ttl=255 time=5.787 ms 56 bytes

from 1.1.1.1: icmp_seq=2 ttl=255 time=5.744 ms 56 bytes

from 1.1.1.1: icmp_seq=3 ttl=255 time=4.478 ms 56 bytes

from 1.1.1.1: icmp_seq=4 ttl=255 time=4.510 ms ---

Ping statistics for 1.1.1.1 --- 5 packet(s) transmitted, 4 packet(s) received, 20.0% packet loss

附件下载：ipsec 主模式穿越nat.rar