MSR路由器IPSec VPN总部使用节点方式建立隧道出现只能与第一个节点通信问题的解决方法

魏添 2012-07-30 发表

MSR路由器IPSec VPN总部使用节点方式建立隧道出现只能与第一个节点通信问题的解决方法

一、 组网：

MSR路由器和三个分支节点建立IPSec VPN，总部的公网地址是1.1.1.1/24，分支的三台路由器的公网地址分别是2.2.2.2/24，3.3.3.3/24，4.4.4.4/24。

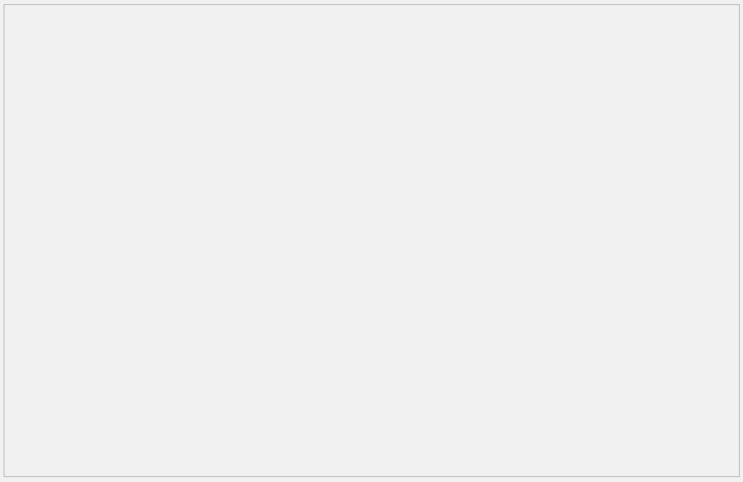

图1

二、 问题描述：

MSR路由器和三个分支节点建立IPSec VPN，发现只能和第一个节点通信，并且后两个节点均正常建立IPSec VPN隧道，但是无法通信。

三、 过程分析：

总部MSR路由器主要配置：

```
version 5.20, Release 2209P21, Standard
sysname IPSec
acl number 3001
 rule 0 permit ip source 10.10.10.10 0 destination 20.20.20.20 0
 rule 5 deny ip
acl number 3002
 rule 0 permit ip source 10.10.10.10 0 destination 30.30.30.30 0
 rule 5 deny ip
acl number 3003
 rule 0 permit ip source 10.10.10.10 0 destination 40.40.40.40 0
 rule 5 deny ip
ike proposal 1
 encryption-algorithm aes-cbc 128
 sa duration 28800
ike peer 1
 proposal 1
 pre-shared-key cipher $c$3$1+SFRrfPojx/CBya4Jm68VVsxLY=
 remote-address 2.2.2.2
 local-address 1.1.1.1
ike peer 2
 proposal 1
 pre-shared-key cipher $c$3$nH3DI7gxrRRbVjEB+IUxm5ha24M=
 remote-address 3.3.3.3
 local-address 1.1.1.1
ike peer 3
 proposal 1
 pre-shared-key cipher $c$3$nMF7zBCyKiJ9/Ix/szEDM46mLRg=
 remote-address 4.4.4.4
 local-address 1.1.1.1
ipsec proposal cd
```

```
 esp authentication-algorithm sha1
 esp encryption-algorithm aes 128
#
ipsec policy cd 1 isakmp
 security acl 3001
 ike-peer 1
 proposal cd
#
ipsec policy cd 2 isakmp
 security acl 3002
 ike-peer 2
 proposal cd
#
ipsec policy cd 3 isakmp
 security acl 3003
 ike-peer 3
 proposal cd

interface LoopBack0
 ip address 10.10.10.10 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
 ipsec policy cd
ospf 1
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
分支1：
version 5.20, Release 2209P15
sysname branch 1
acl number 3000
 rule 0 permit ip source 20.20.20.20 0 destination 10.10.10.10 0
ike proposal 1
 encryption-algorithm aes-cbc 128
 sa duration 28800
#
ike peer 1
 proposal 1
 pre-shared-key cipher $c$3$G/puASrWbfhoRyZl8AYKOMkiBFo=
 remote-address 1.1.1.1
 local-address 2.2.2.2
ipsec proposal 1
 esp authentication-algorithm sha1
 esp encryption-algorithm aes 128
#
ipsec policy 1 1 isakmp
 security acl 3000
 ike-peer 1
 proposal 1
interface Ethernet0/0
 port link-mode route
 ip address 2.2.2.2 255.255.255.0
 ipsec policy 1
interface LoopBack0
 ip address 20.20.20.0 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 2.2.2.0 0.0.0.255
#
 ip route-static 0.0.0.0 0.0.0.0 2.2.2.1
```

其他两个分支路由器的配置跟分支一路由器大致相同。
此时，在总部路由器上查看ike sa：

```
<IPSec>display ike sa
  total phase-1 SAs: 3
  connection-id  peer          flag       phase   doi
 ------------------------------------------------------------------------
    1          2.2.2.2       RD|ST       1     IPSEC
    3          3.3.3.3       RD          1     IPSEC
    5          4.4.4.4       RD          1     IPSEC
    2          2.2.2.2       RD|ST       2     IPSEC
    4          3.3.3.3       RD          2     IPSEC
    6          4.4.4.4       RD          2     IPSEC
```

可以看到每个分直接点都已经建立起来了两个阶段的sa，尝试ping测试,结果如下：

```
<IPSec>ping -a 10.10.10.10 20.20.20.20
 PING 20.20.20.20: 56  data bytes, press CTRL_C to break
   Reply from 20.20.20.20: bytes=56 Sequence=1 ttl=255 time=6 ms
   Reply from 20.20.20.20: bytes=56 Sequence=2 ttl=255 time=6 ms
   Reply from 20.20.20.20: bytes=56 Sequence=3 ttl=255 time=5 ms
   Reply from 20.20.20.20: bytes=56 Sequence=4 ttl=255 time=5 ms
Reply from 20.20.20.20: bytes=56 Sequence=5 ttl=255 time=5 ms
```

第一个节点没有问题。
第二个节点测试结果如下：

```
<IPSec>ping -a 10.10.10.10 30.30.30.30
 PING 30.30.30.30: 56  data bytes, press CTRL_C to break
   Request time out
   Request time out
   Request time out
```

第二个节点ping测试失败。
第三个节点测试如下：

```
<IPSec>ping -a 10.10.10.10 40.40.40.40
 PING 40.40.40.40: 56  data bytes, press CTRL_C to break
   Request time out
   Request time out
   Request time out
   Request time out
```

实验结果只有第一个节点可以正常通信，我们检查配置，发现有一点可疑现象，在每个安全ACL的最后一个规则中，都是deny any。这样配置可能会出现的问题是所有的流量全部都匹配到了第一个节点，导致其他节点没有流量匹配，而除了第一个节点匹配上了，后面的流量会被deny掉。

四、 解决方法：

分析的时候，我们已经知道后面没有为什么不能ping通的原因，我们尝试将ACL中的deny any规则去掉。
第二个节点测试：

```
<IPSec>ping -a 10.10.10.10 30.30.30.30
 PING 30.30.30.30: 56  data bytes, press CTRL_C to break
   Reply from 30.30.30.30: bytes=56 Sequence=1 ttl=255 time=2 ms
   Reply from 30.30.30.30: bytes=56 Sequence=2 ttl=255 time=2 ms
Reply from 30.30.30.30: bytes=56 Sequence=3 ttl=255 time=2 ms
```

第二个节点果然通过了。
第三个节点测试：

```
<IPSec>ping -a 10.10.10.10 40.40.40.40
 PING 40.40.40.40: 56  data bytes, press CTRL_C to break
   Reply from 40.40.40.40: bytes=56 Sequence=1 ttl=255 time=2 ms
   Reply from 40.40.40.40: bytes=56 Sequence=2 ttl=255 time=2 ms
   Reply from 40.40.40.40: bytes=56 Sequence=3 ttl=255 time=2 ms
```

也没有任何问题。
从上面的案例我们可以总结一下，如果IPSec VPN在节点方式建立的情况下ACL的最后一条如果匹配到了所有流量，那么后面的节点将不会再被匹配。所以，在使用节点方式建立IPSec VPN的时候，我们不能让前面的节点匹配上后面节点的流量。