MSR 基于ipsec隧道流量做流通qos时acl的调用方式

QoS IPSec VPN 罗梦恺 2022-09-23 发表

组网及说明

MSR======ipsec=======MSR

问题描述

MSR设备 做ipsec vpn时，基于ipsec的流量做qos 流通时的acl调用情况实验室测试如下：

版本：Release 0707P16 其余版本测试接口基本一致

MSR1：内网地址10.1.1.1 ， wan口地址100.1.1.1

MSR2：内网地址10.1.2.1 ， wan口地址100.1.1.2

配置：

MSR1	MSR2
# traffic classifier 1 operator and if-match acl 3001 # traffic behavior 1 filter permit # qos policy 1 classifier 1 behavior 1 # interface LoopBack0 ip address 10.1.1.1 255.255.255.0 # interface GigabitEthernet0/0 port link-mode route description Single_Line1 ip address 100.1.1.1 255.255.255.0 qos apply policy 1 inbound qos apply policy 1 outbound ipsec apply policy map1 # ip route-static 0.0.0.0 0 100.1.1.2 # acl advanced 3000 rule 0 permit ip source 10.1.1.0 0.0.0.2 55 destination 10.1.2.0 0.0.0.255 # acl advanced 3001 rule 0 permit ip source 10.1.1.1 0 desti nation 10.1.2.1 0 rule 10 permit ip source 10.1.2.1 0 des tination 10.1.1.1 0 # ipsec transform-set tran1 esp encryption-algorithm aes-cbc- 128 esp authentication-algorithm sha1 # ipsec policy map1 10 isakmp transform-set tran1 security acl 3000 local-address 100.1.1.1 remote-address 100.1.1.2 ike-profile profile1 # ike profile profile1 keychain keychain1 match remote identity address 100.1. 1.2 255.255.255.0 # ike keychain keychain1 pre-shared-key address 100.1.1.2 255. 255.255.0 key cipher c3$hGd/G70U 2sNc62XvPnFTJ+FaK+vre8zqsA==	# interface LoopBack0 ip address 10.1.2.1 255.255.255.0 # interface GigabitEthernet0/0 port link-mode route ip address 100.1.1.2 255.255.255.0 ipsec apply policy use1 # ip route-static 0.0.0.0 0 100.1.1.1 # acl advanced 3000 rule 0 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 # ipsec transform-set tran1 esp encryption-algorithm aes-cbc-128 esp authentication-algorithm sha1 # ipsec policy use1 10 isakmp transform-set tran1 security acl 3000 local-address 100.1.1.2 remote-address 100.1.1.1 ike-profile profile1 # ike profile profile1 keychain keychain1 match remote identity address 100.1.1.1 255.255.255.0 # ike keychain keychain1 pre-shared-key address 100.1.1.1 255.2 55.255.0 key cipher c3$UwmBOA4QA vEHrnXloqrbHyRYL0j1Zmez4g==

测试1:基于内网地址做qos

```
<830>dis ike sa
   Connection-ID  Remote            Flag       DOI
-------------------------------------------------------------------------
9              100.1.1.2         RD         IPsec
<830>dis ipsec sa brief
-------------------------------------------------------------------------------
Interface/Global        Dst Address      SPI        Protocol   Status
-------------------------------------------------------------------------------
GE0/0                   100.1.1.2        3613014362 ESP        Active
GE0/0                   100.1.1.1        4167624094 ESP        Active
GE0/0                   100.1.1.2        1670495072 ESP        Active
GE0/0                   100.1.1.1        1609372173 ESP        Active
<830>ping -a 10.1.1.1 10.1.2.1   //内网地址ping测试
```

Ping 10.1.2.1 (10.1.2.1) from 10.1.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 10.1.2.1: icmp_seq=0 ttl=255 time=1.085 ms
56 bytes from 10.1.2.1: icmp_seq=1 ttl=255 time=0.617 ms
56 bytes from 10.1.2.1: icmp_seq=2 ttl=255 time=0.582 ms
56 bytes from 10.1.2.1: icmp_seq=3 ttl=255 time=0.568 ms
56 bytes from 10.1.2.1: icmp_seq=4 ttl=255 time=0.517 ms

过程分析

针对ipsec流量的qos，MSR设备入方向可直接统计到基于内网地址的流量，出方向需要配置pre-classify后才能统计到内网地址流量。

<830>dis qos policy int g0/0　//入方向不配置pre-classify也能统计到，出方向无法统计到
Interface: GigabitEthernet0/0
Direction: Inbound
 Policy: 1
  Classifier: default-class
    Matched : 5 (Packets) 830 (Bytes)
    5-minute statistics:
     Forwarded: 0/22 (pps/bps)
     Dropped : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     If-match any
    Behavior: be
     -none-
  Classifier: 1
    Matched : 5 (Packets) 490 (Bytes)
    5-minute statistics:
     Forwarded: 0/13 (pps/bps)
     Dropped : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     If-match acl 3001
    Behavior: 1
     Filter enable: Permit

Interface: GigabitEthernet0/0
 Direction: Outbound
 Policy: 1
  Classifier: default-class
    Matched : 5 (Packets) 830 (Bytes)
    5-minute statistics:
     Forwarded: 0/22 (pps/bps)
     Dropped : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     If-match any
    Behavior: be
     -none-
  Classifier: 1
    Matched : 0 (Packets) 0 (Bytes)
    5-minute statistics:
     Forwarded: 0/0 (pps/bps)
     Dropped : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     If-match acl 3001
    Behavior: 1
     Filter enable: Permit

测试2：添加qos pre-classify
添加配置：
#
ipsec policy map1 10 isakmp
transform-set tran1
 security acl 3000
 local-address 100.1.1.1
remote-address 100.1.1.2

```
qos pre-classify
ike-profile profile1
```

解决方法

最佳的配置方式，基于内网地址acl做qos，同时配置pre-classify，出入方向都能匹配上。

```
<830>reset counters interface 清空qos统计


<830>ping -a 10.1.1.1 10.1.2.1
Ping 10.1.2.1 (10.1.2.1) from 10.1.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 10.1.2.1: icmp_seq=0 ttl=255 time=1.096 ms
56 bytes from 10.1.2.1: icmp_seq=1 ttl=255 time=0.593 ms
56 bytes from 10.1.2.1: icmp_seq=2 ttl=255 time=0.601 ms
56 bytes from 10.1.2.1: icmp_seq=3 ttl=255 time=0.601 ms
56 bytes from 10.1.2.1: icmp_seq=4 ttl=255 time=0.598 ms



<830>dis qos policy int g0/0
Interface: GigabitEthernet0/0
Direction: Inbound
  Policy: 1
   Classifier: default-class
     Matched : 5 (Packets) 830 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: 1
     Matched : 5 (Packets) 490 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match acl 3001
     Behavior: 1
      Filter enable: Permit

Interface: GigabitEthernet0/0
Direction: Outbound
  Policy: 1
   Classifier: default-class
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: 1
     Matched : 5 (Packets) 830 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match acl 3001
     Behavior: 1
```

Filter enable: Permit