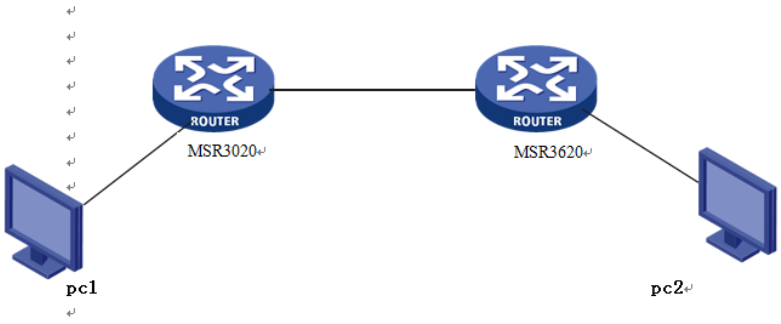
MSR IPsec V5-V7 野蛮模式对接

刘文峰 2015-03-25 发表

MSR3020 采用拨号上网方式，MSR3620 采用固定ip上网，两端私网通过ipsec 隧道通信



实验说明：pc1和pc2采用设备上的loopback地址代替，pc1 IP地址是2.2.2.2/32，pc2的IP地址是1.1.1.1/32，测试过程中MSR3020 虽然是固定IP地址10.153.42.73，但是在测试当中对端是指的名字而不是IP地址，MSR3620 ip地址10.153.42.93。

1：MSR3620 主要配置（采用模版方式）

```
acl number 3010
 rule 0 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
ipsec transform-set 3620
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
ipsec policy-template 1 1          //此处必须使用模版方式，不然ipsec野蛮模式是无法成功建立的
transform-set 3620
 security acl 3010
 ike-profile 3620
#
ipsec policy 1 1 isakmp template 1
 ike identity fqdn 3620                //标明本段名字标识
ike profile 3620
 keychain 3620
 exchange-mode aggressive
 local-identity fqdn 3620
 match remote identity fqdn 3020        //指对端的标识
 proposal 3620
ike proposal 3620
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
#
ike keychain 1
#
ike keychain 3620
 pre-shared-key hostname 3020 key simple 123
#
interface GigabitEthernet0/0
 ipsec apply policy 1
```

版本：

```
<MSR3620>display version
H3C Comware Software, Version 7.1.042, Release 0007P03
Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C MSR36-20 uptime is 0 weeks, 1 day, 10 hours, 22 minutes
Last reboot reason : User reboot
Boot image: cfa0:/msr36-cmw710-boot-r0007p03.bin
Boot image version: 7.1.042P06, Release 0007P03
  Compiled Sep 17 2013 11:45:32
System image: cfa0:/msr36-cmw710-system-r0007p03.bin
System image version: 7.1.042, Release 0007P03
  Compiled Sep 17 2013 11:46:05
Feature image(s) list:
```

```
  cfa0:/msr36-cmw710-security-r0007p03.bin, version: 7.1.042
    Compiled Sep 17 2013 11:46:57
  cfa0:/msr36-cmw710-voice-r0007p03.bin, version: 7.1.042
    Compiled Sep 17 2013 11:46:57
  cfa0:/msr36-cmw710-data-r0007p03.bin, version: 7.1.042
    Compiled Sep 17 2013 11:47:00
```

2：MSR3020 主要配置：（用ICG2000C模拟）

```
acl number 3010
  rule 0 permit ip source 2.2.2.2 0 destination 1.1.1.1 0
ipsec transform-set 3020
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
 esp encryption-algorithm 3des
#
ipsec policy 3020 10 isakmp
 security acl 3010
 ike-peer 3020
     transform-set 3020

ike peer 3020
 exchange-mode aggressive
 pre-shared-key simple 123
 id-type name
 remote-name 3620
 remote-address 10.153.42.93
 local-name 3020
     nat traversal
interface Ethernet0/0
 ipsec policy 3020

<H3C>dis ver
H3C Comware Platform Software
Comware Software, Version 5.20, ESS 2318
Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C ICG2000C uptime is 0 week, 1 day, 9 hours, 27 minutes
Last reboot 2007/01/01 08:00:38
System returned to ROM By <Reboot> Command.
```

一、 测试结果：

1. MSR3020 侧：

```
   <H3C>reset ike sa
<H3C>reset ipsec sa
<H3C>ping -a 2.2.2.2 1.1.1.1
  PING 1.1.1.1: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 1.1.1.1: bytes=56 Sequence=1 ttl=255 time=3 ms
    Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=255 time=3 ms
    Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=255 time=3 ms

  --- 1.1.1.1 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 2/2/3 ms

<H3C>dis ike sa
    total phase-1 SAs:  1
    connection-id  peer                 flag       phase   doi
  --------------------------------------------------------------------------
      140          10.153.42.93          RD|ST      1       IPSEC
      141          10.153.42.93          RD|ST      2       IPSEC
```

```
  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT RK--REKEY
<H3C>dis ipsec sa
===============================
Interface: Ethernet0/0
    path MTU: 1500
===============================

  -----------------------------
  IPsec policy name: "3020"
  sequence number: 10
  acl version: ACL4
  mode: isakmp
  -----------------------------
    PFS: N, DH group: none
    tunnel:
        local  address: 10.153.42.73
        remote address: 10.153.42.93
    flow:
        sour addr: 2.2.2.2/255.255.255.255  port: 0  protocol: IP
        dest addr: 1.1.1.1/255.255.255.255  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 0x72A987D8(1923712984)
      transform: ESP-ENCRYPT-3DES ESP-AUTH-MD5
      in use setting: Tunnel
      connection id: 11
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843199/3589
      anti-replay detection: Enabled
        anti-replay window size(counter based): 32
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 0x5E5BA19(98941465)
      transform: ESP-ENCRYPT-3DES ESP-AUTH-MD5
      in use setting: Tunnel
      connection id: 12
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843199/3589
      anti-replay detection: Enabled
        anti-replay window size(counter based): 32
      udp encapsulation used for nat traversal: N
<H3C>
2.MSR3620 侧
<MSR3620>dis ike sa
    Connection-ID   Remote              Flag        DOI
-------------------------------------------------------------------
    21              10.153.42.73        RD          IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
<MSR3620>ping -a 1.1.1.1 2.2.2.2
Ping 2.2.2.2 (2.2.2.2) from 1.1.1.1: 56 data bytes, press escape sequence to break
56 bytes from 2.2.2.2: icmp_seq=0 ttl=255 time=1.856 ms
56 bytes from 2.2.2.2: icmp_seq=1 ttl=255 time=1.803 ms
56 bytes from 2.2.2.2: icmp_seq=2 ttl=255 time=2.241 ms
56 bytes from 2.2.2.2: icmp_seq=3 ttl=255 time=1.665 ms
56 bytes from 2.2.2.2: icmp_seq=4 ttl=255 time=1.707 ms

--- Ping statistics for 2.2.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.665/1.854/2.241/0.205 ms
<MSR3620>dis ipse sa
```

```
--------------------------------
Interface: GigabitEthernet0/0
--------------------------------

  ------------------------------
  IPsec policy: 1
  Sequence number: 1
  Mode: template
  ------------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Path MTU: 1443
    Tunnel:
        local  address: 10.153.42.93
        remote address: 10.153.42.73
    Flow:
    sour addr: 1.1.1.1/255.255.255.255  port: 0  protocol: ip
    dest addr: 2.2.2.2/255.255.255.255  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 98941465 (0x05e5ba19)
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3517
      Max received sequence-number: 9
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for nat traversal: N
      Status: active

    [Outbound ESP SAs]
      SPI: 1923712984 (0x72a987d8)
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3517
      Max sent sequence-number: 9
      UDP encapsulation used for nat traversal: N
      Status: active
```

测试结果2：当模版侧安全acl去掉，也是能正常建立起来的，该参数在未配置的情况下，相当于支持最大范围的保护，即完全接受协商发起端的ACL设置

```
[MSR3620]ipsec policy-template 1 1
[MSR3620-ipsec-policy-template-1-1]undo security acl
[MSR3620-ipsec-policy-template-1-1]dis this
#
ipsec policy-template 1 1
 transform-set 3620
 ike-profile 3620
#
return
[MSR3620-ipsec-policy-template-1-1]qu
[MSR3620]qu
<MSR3620>reset ike sa
<MSR3620>reset ipsec sa
```

MSR3020侧：

```
<H3C> reset ike sa
<H3C>reset ipsec sa
<H3C>ping -a 2.2.2.2 1.1.1.1
  PING 1.1.1.1: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 1.1.1.1: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=255 time=3 ms
    Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=255 time=3 ms
```

--- 1.1.1.1 ping statistics ---
5 packet(s) transmitted
4 packet(s) received
20.00% packet loss

1. 当V5 设备侧采用野蛮模式的自动获取地址情况下，V7 设备侧必须使用模版方式，不然IPsec无法成功建立。如果是主模式的话，就没有这个局限性。

2. 在V5 设备和V5设备做野蛮模式的，可以不用模版方式能建立，但是V7的设备由于在ipsec policy中无法指IP地址，指对端名字不起作用。

```
ipsec policy 3620 10 isakmp
 transform-set 3620
 security acl 3010
 local-address 10.153.42.93
 remote-address 3020
 ike-profile 3620
```

3. 当模版侧安全acl去掉，也是能正常建立起来的，该参数在未配置的情况下，相当于支持最大范围的保护，即完全接受协商发起端的ACL设置。