ComwareV7 FW带VPN实例的AFT典型配置（V6访问V4）

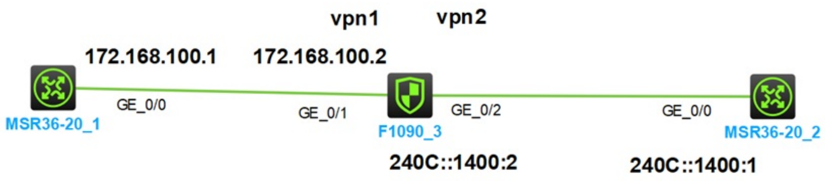
AFT 孔德飞 2024-01-19 发表

组网及说明

组网如下：

FW的g1/0/1属于vpn1，对接ipv6网络，FW的g1/0/2属于vpn2,对接ipv6网络

需求是：MSR通过访问2012:172.168.100.1，通过FW的AFT转换到V4侧，源地址转换为172.168.100.3，目的地址转换为172.168.100.1



配置步骤

MSR1的配置如下：

接口起IP地址

```
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 172.168.100.1 255.255.255.0
```

FW的配置如下：

```
ip vpn-instance vpn1
ip vpn-instance vpn2
```

配置IPV6到IPV4的目的地址转换

```
aft prefix-nat64 2012:: 96
```

配置IPV6到IPV4源地址转换地址池

```
aft address-group 1
 address 172.168.100.3 172.168.100.3
```

配置IPV6到IPV4源地址转换

```
 aft v6tov4 source prefix-nat64 2012:: 96 vpn-instance vpn2 address-group 1 vpn-instance vpn1
```

接口配置VPN实例，起IP地址，配置AFT

```
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 ip binding vpn-instance vpn1
 ip address 172.168.100.2 255.255.255.0
 aft enable

interface GigabitEthernet1/0/2
 port link-mode route
 combo enable copper
 ip binding vpn-instance vpn2
 aft enable
 ipv6 address 240C::1400:2/96
```

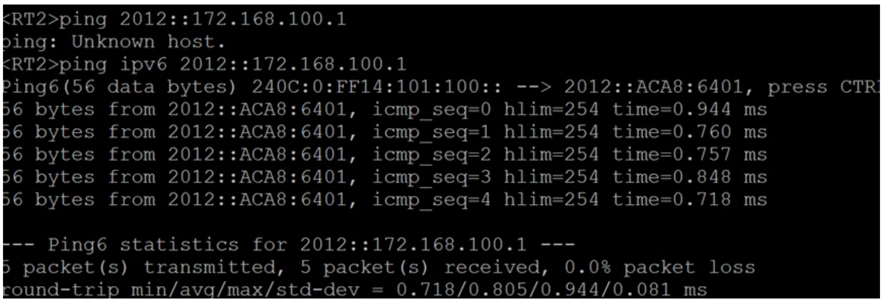
MSR2的配置

```
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ipv6 address 240C::1400:1/96
```

路由

```
ipv6 route-static 2012:: 96 240C::1400:2
```

配置完成之后，MSR2可以通过2012::172.178.100.1访问MSR1的172.168.100.1



```
<RT2>ping 2012::172.168.100.1
ping: Unknown host.
<RT2>ping ipv6 2012::172.168.100.1
Ping6(56 data bytes) 240C:0:FF14:101:100:: --> 2012::ACA8:6401, press CTRL
56 bytes from 2012::ACA8:6401, icmp_seq=0 hlim=254 time=0.944 ms
56 bytes from 2012::ACA8:6401, icmp_seq=1 hlim=254 time=0.760 ms
56 bytes from 2012::ACA8:6401, icmp_seq=2 hlim=254 time=0.757 ms
56 bytes from 2012::ACA8:6401, icmp_seq=3 hlim=254 time=0.848 ms
56 bytes from 2012::ACA8:6401, icmp_seq=4 hlim=254 time=0.718 ms

--- Ping6 statistics for 2012::172.168.100.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.718/0.805/0.944/0.081 ms
```

FW的AFT会话如下

```
[FW]display  aft  session  ipv4 verbose
Slot 1:
Total sessions found: 0
[FW]display  aft  session  ipv4 verbose
Slot 1:
Initiator:
  Source      IP/port: 172.168.100.3/2
  Destination IP/port: 172.168.100.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: vpn2/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Local
Responder:
  Source      IP/port: 172.168.100.1/2
  Destination IP/port: 172.168.100.3/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: vpn1/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
State: ICMP_REPLY
Application: ICMP
Rule ID: 1
Rule name: 1
Start time: 2024-01-19 12:49:23  TTL: 28s
Initiator->Responder:          5 packets       420 bytes
Responder->Initiator:          5 packets       420 bytes [FW]
[FW]
[FW]display  aft  session  ipv6 v
[FW]display  aft  session  ipv6 verbose
Slot 1:
Initiator:
  Source      IP/port: 240C::1400:1/10975
  Destination IP/port: 2012::ACA8:6401/32768
  VPN instance/VLAN ID/Inline ID: vpn2/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
Responder:
  Source      IP/port: 2012::ACA8:6401/10975
  Destination IP/port: 240C::1400:1/33024
  VPN instance/VLAN ID/Inline ID: vpn1/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Local
State: ICMPV6_REPLY
Application: ICMP
Rule ID: -/-/-
Rule name:
Start time: 2024-01-19 12:45:16  TTL: 14s
Initiator->Responder:            5 packets        520 bytes
Responder->Initiator:            5 packets        520 bytes

Total sessions found: 1
```

配置关键点

配置关键点:

配置IPV6到IPV4的目的地址转换

```
aft prefix-nat64 2012:: 96
```

配置IPV6到IPV4源地址转换地址池

```
aft address-group 1
 address 172.168.100.3 172.168.100.3
```

配置IPV6到IPV4源地址转换

```
 aft v6tov4 source prefix-nat64 2012:: 96 vpn-instance vpn2 address-group 1 vpn-instance vpn1
```