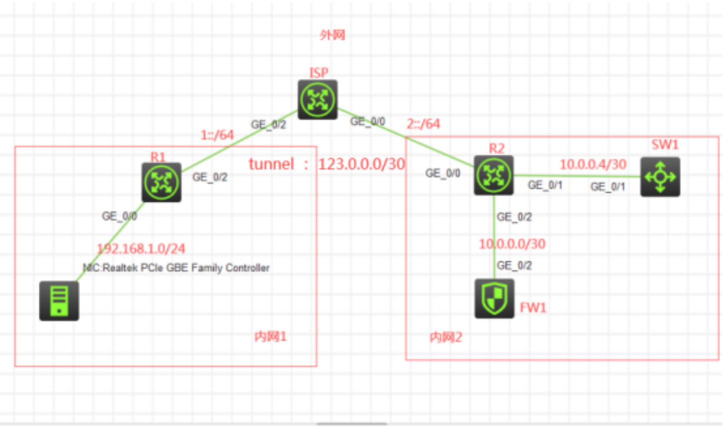
IPV6之IPV4 over IPV6隧道over SSL VPN TCP接入（缺省证书）双臂（旁路）典型组网配置案例

SSL VPN H3C模拟器 GRE VPN 韦家宁 2020-04-11 发表

组网及说明



组网说明：

本案例采用H3C HCL模拟器来模拟IPV4 over IPV6 over ssl vpn典型组网配置。内网和外网已经有了明确的标识。内网1和内网2都是采用IPV4作为基础网络的搭建。外网采用IPV6来实现内网1和内网2的互联。为了实现内网1和内网2的互通，要求在R1与R2之间建立隧道，采用IPV4 over IPV6的方式。内网2的FW1使用F1060防火墙做成SSL VPN网关，内网1的终端到达内网2之后，首先要进行SSL VPN的认证过后，方能访问SW1。因此需要在R2做策略路由，实现流量的引流。由于模拟器的局限性，因此使用SW1采用S5820交换机开启telnet功能来模拟telnet服务器。最后SSL VPN的接入的方式为TCP接入（缺省证书）双臂（旁路）的架构，提供TCP接入的服务并将内网2的telnet服务器进行发布。

配置步骤

1、按照网络拓扑图正确配置IP地址

2、R1与R2建立隧道

3、FW1开启SSL VPN功能

4、SW1开启telnet功能，并创建相关账号、赋予权限

配置关键点

SW1：

```
sys
System View: return to User View with Ctrl+Z.
[H3C]sysname SW1
[SW1]int gi 1/0/1
[SW1-GigabitEthernet1/0/1]port link-mode route
[SW1-GigabitEthernet1/0/1]des
[SW1-GigabitEthernet1/0/1]ip address 10.0.0.5 30
[SW1-GigabitEthernet1/0/1]quit
[SW1]ip route-static 0.0.0.0 0.0.0.0 10.0.0.6
[SW1]local-user admin
New local user added.
[SW1-luser-manage-admin]password simple admin
[SW1-luser-manage-admin]service-type telnet
[SW1-luser-manage-admin]authorization-attribute user-role network-admin
[SW1-luser-manage-admin]quit
[SW1]telnet server enable
[SW1]line vty 0 4
[SW1-line-vty0-4]authentication-mode scheme
[SW1-line-vty0-4]protocol inbound all
[SW1-line-vty0-4]quit
```

ISP：

```
sys
```

```
System View: return to User View with Ctrl+Z.
[H3C]sysname ISP
[ISP]int gi 0/2
[ISP-GigabitEthernet0/2]des
[ISP-GigabitEthernet0/2]ipv6 address 1::2 64
[ISP-GigabitEthernet0/2]quit
[ISP]int gi 0/0
[ISP-GigabitEthernet0/0]des
[ISP-GigabitEthernet0/0]ipv6 address 2::2 64
[ISP-GigabitEthernet0/0]quit
[ISP]
```

R1：

```
sys
System View: return to User View with Ctrl+Z.
[H3C]sysname R1
[R1]int gi 0/0
[R1-GigabitEthernet0/0]ip address 192.168.1.1 24
[R1-GigabitEthernet0/0]quit
[R1]int gi 0/2
[R1-GigabitEthernet0/2]des
[R1-GigabitEthernet0/2]ipv6 address 1::1 64
[R1-GigabitEthernet0/2]quit
[R1]ipv6 route-static :: 0 1::2
```

R1 IPV4 over IPV6隧道关键配置点:

```
[R1]int tunnel 0 mode ipv6
[R1-Tunnel0]ip address 123.0.0.1 30
[R1-Tunnel0]source 1::1
[R1-Tunnel0]destination 2::1
[R1-Tunnel0]undo shutdown
[R1-Tunnel0]quit
[R1]ip route-static 10.0.0.0 255.255.255.0 123.0.0.2
[R1]
```

R2：

```
sys
System View: return to User View with Ctrl+Z.
[H3C]sysname R2
[R2]int gi 0/1
[R2-GigabitEthernet0/1]des
[R2-GigabitEthernet0/1]ip address 10.0.0.6 30
[R2-GigabitEthernet0/1]quit
[R2]int gi 0/2
[R2-GigabitEthernet0/2]des
[R2-GigabitEthernet0/2]ip address 10.0.0.2 30
[R2-GigabitEthernet0/2]quit
[R2]int gi 0/0
[R2-GigabitEthernet0/0]des
[R2-GigabitEthernet0/0]ipv6 address 2::1 64
[R2-GigabitEthernet0/0]quit
[R2]ipv6 route-static :: 0 2::2
```

R2 策略路由及IPV4 over IPV6隧道配置关键点:

```
[R2]acl basic 2000
[R2-acl-ipv4-basic-2000]rule 0 permit source 192.168.1.0 0.0.0.255
[R2-acl-ipv4-basic-2000]quit
[R2]policy-based-route james permit node 1
[R2-pbr-james-1]if-match acl 2000
[R2-pbr-james-1]apply next-hop 10.0.0.1
[R2-pbr-james-1]quit
[R2]int Tunnel 0 mode ipv6
[R2-Tunnel0]ip address 123.0.0.2 30
[R2-Tunnel0]source 2::1
[R2-Tunnel0]destination 1::1
```

```
[R2-Tunnel0]ip policy-based-route james
[R2-Tunnel0]undo shutdown
[R2-Tunnel0]quit
[R2]ip route-static 192.168.1.0 255.255.255.0 123.0.0.1
```

FW1：

```
sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW1
[FW1]int gi 1/0/2
[FW1-GigabitEthernet1/0/2]des
[FW1-GigabitEthernet1/0/2]ip address 10.0.0.1 30
[FW1-GigabitEthernet1/0/2]quit
[FW1]ip route-static 0.0.0.0 0.0.0.0 10.0.0.2
[FW1]security-zone name trust
[FW1-security-zone-Trust]import interface GigabitEthernet 1/0/2
[FW1-security-zone-Trust]quit
[FW1]acl basic 2001
[FW1-acl-ipv4-basic-2001]rule 0 permit source any
[FW1-acl-ipv4-basic-2001]quit
[FW1]
[FW1]zone-pair security source trust destination untrust
[FW1-zone-pair-security-Trust-Untrust]packet-filter 2001
[FW1-zone-pair-security-Trust-Untrust]quit
[FW1]
[FW1]zone-pair security source untrust destination trust
[FW1-zone-pair-security-Untrust-Trust]packet-filter 2001
[FW1-zone-pair-security-Untrust-Trust]quit
[FW1]
[FW1]zone-pair security source trust destination local
[FW1-zone-pair-security-Trust-Local]packet-filter 2001
[FW1-zone-pair-security-Trust-Local]quit
[FW1]
[FW1]zone-pair security source local destination trust
[FW1-zone-pair-security-Local-Trust]packet-filter 2001
[FW1-zone-pair-security-Local-Trust]quit
[FW1]
[FW1]zone-pair security source untrust destination local
[FW1-zone-pair-security-Untrust-Local]packet-filter 2001
[FW1-zone-pair-security-Untrust-Local]quit
[FW1]
[FW1]zone-pair security source local destination untrust
[FW1-zone-pair-security-Local-Untrust]packet-filter 2001
[FW1-zone-pair-security-Local-Untrust]quit
```

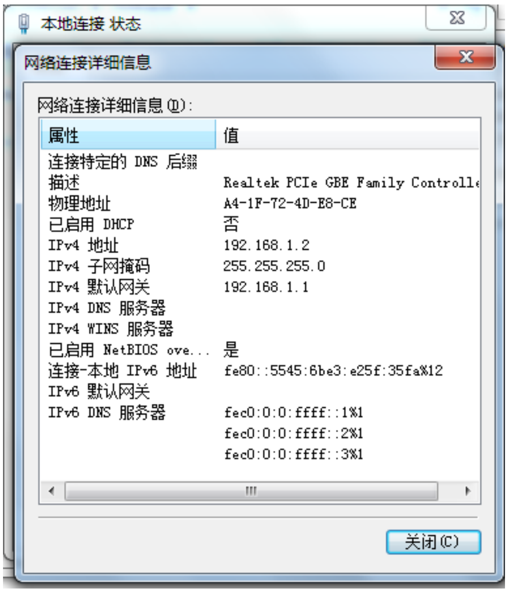
FW1 SSL VPN关键配置点：

```
[FW1]acl advanced 3000
[FW1-acl-ipv4-adv-3000]rule 0 permit tcp source any destination any
[FW1-acl-ipv4-adv-3000]quit
[FW1]sslvpn context james
[FW1-sslvpn-context-james]gateway james domain james
[FW1-sslvpn-context-james]port-forward-item james
[FW1-sslvpn-context-james-port-forward-item-james]local-port 2323 local-name 127.0.0.23 remote-server 10.0.0.5 remote-port 23
[FW1-sslvpn-context-james-port-forward-item-james]port-forward list
[FW1-sslvpn-context-james-port-forward-list]resources port-forward-item james
[FW1-sslvpn-context-james-port-forward-list]quit
[FW1-sslvpn-context-james]policy-group james
[FW1-sslvpn-context-james-policy-group-james]resources port-forward list
[FW1-sslvpn-context-james-policy-group-james]filter tcp-access acl 3000
[FW1-sslvpn-context-james-policy-group-james]quit
[FW1-sslvpn-context-james]service enable
[FW1-sslvpn-context-james]quit
```

```
[FW1]local-user james class network
New local user added.
[FW1-luser-network-james]password simple james
[FW1-luser-network-james]service-type sslvpn
[FW1-luser-network-james]authorization-attribute user-role network-operator
[FW1-luser-network-james]authorization-attribute sslvpn-policy-group james
[FW1-luser-network-james]quit
```

测试：

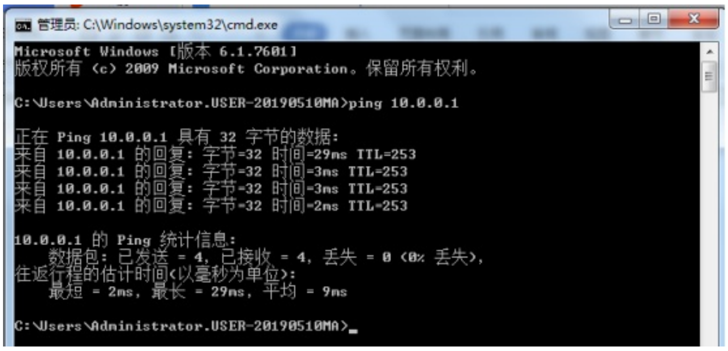
物理机填写IP地址：



网络连接详细信息(D)：

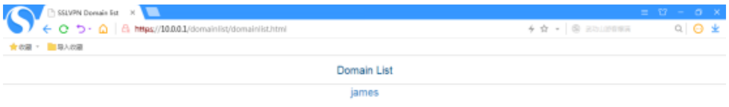
```
属性                    值
连接特定的 DNS 后缀
描述                    Realtek PCIe GBE Family Controlle
物理地址                A4-1F-72-4D-E8-CE
已启用 DHCP             否
IPv4 地址               192.168.1.2
IPv4 子网掩码           255.255.255.0
IPv4 默认网关           192.168.1.1
IPv4 DNS 服务器
IPv4 WINS 服务器
已启用 NetBIOS ove...   是
连接-本地 IPv6 地址     fe80::5545:6be3:e25f:35fa%12
IPv6 默认网关
IPv6 DNS 服务器         fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
```

物理机能PING通FW1：

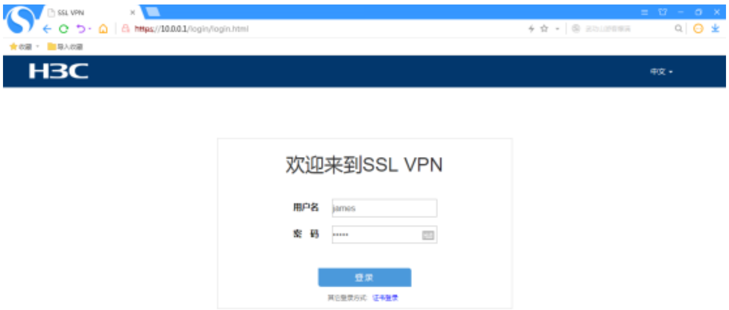


```
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator.USER-20190510MA>ping 10.0.0.1

正在 Ping 10.0.0.1 具有 32 字节的数据:
来自 10.0.0.1 的回复: 字节=32 时间=29ms TTL=253
来自 10.0.0.1 的回复: 字节=32 时间=3ms TTL=253
来自 10.0.0.1 的回复: 字节=32 时间=3ms TTL=253
来自 10.0.0.1 的回复: 字节=32 时间=2ms TTL=253

10.0.0.1 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms，最长 = 29ms，平均 = 9ms

C:\Users\Administrator.USER-20190510MA>_
```

打开浏览器，输入网址：https://10.0.0.1， 回车,点击“james”



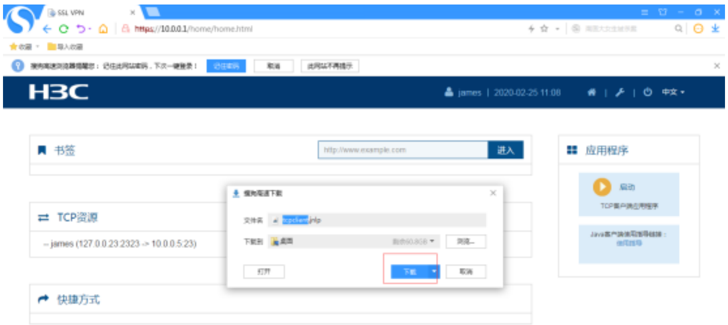
输入用户名、密码，点击“登陆”：



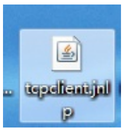
用户名 james

密　码 •••••

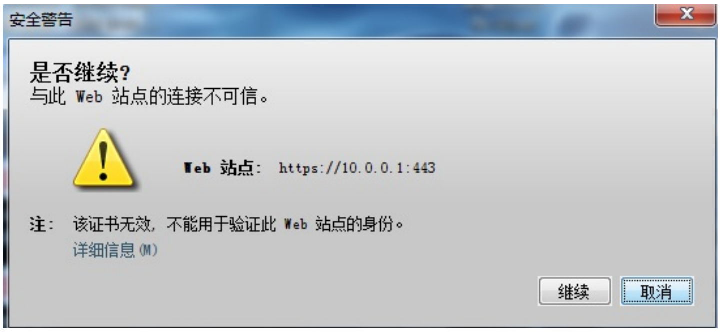
登陆SSL VPN网关成功，点击右边的“启动 TCP客户端应用程序”，下载客户端：



打开客户端：



点击“继续”：



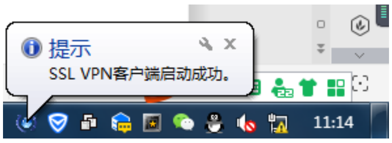
安全警告

是否继续?
与此 Web 站点的连接不可信。

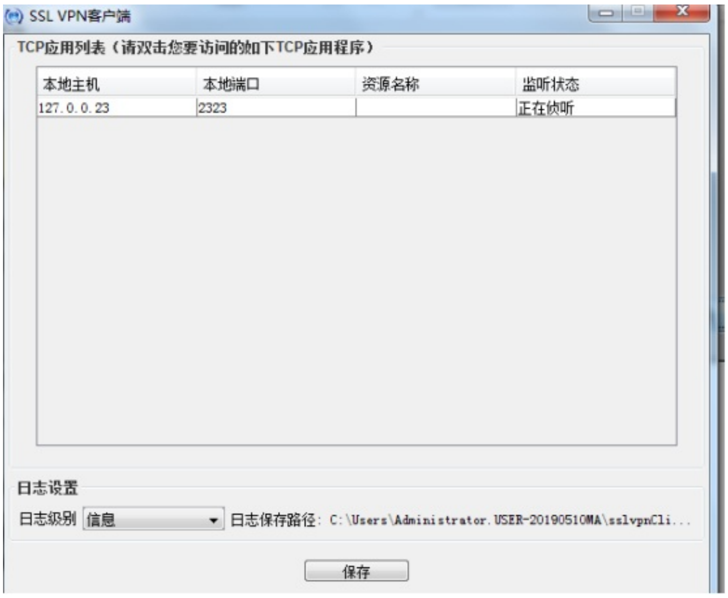
Web 站点: https://10.0.0.1:443

注: 该证书无效，不能用于验证此 Web 站点的身份。
详细信息(M)

SSL VPN启动成功：



提示
SSL VPN客户端启动成功。



SSL VPN客户端

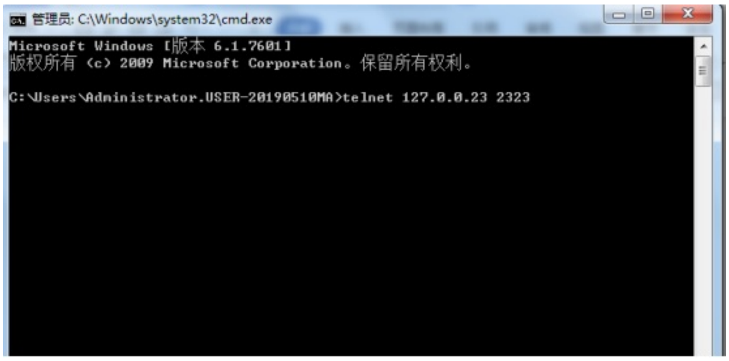
TCP应用列表（请双击您要访问的如下TCP应用程序）

本地主机	本地端口	资源名称	监听状态
127.0.0.23	2323		正在侦听

日志设置

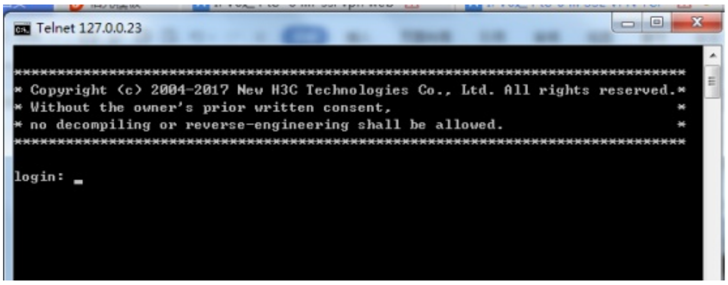
日志级别 信息　日志保存路径：C:\Users\Administrator.USER-20190510MA\sslvpnCli...

打开CMD，输入命令telnet 127.0.0.23 2323，回车：



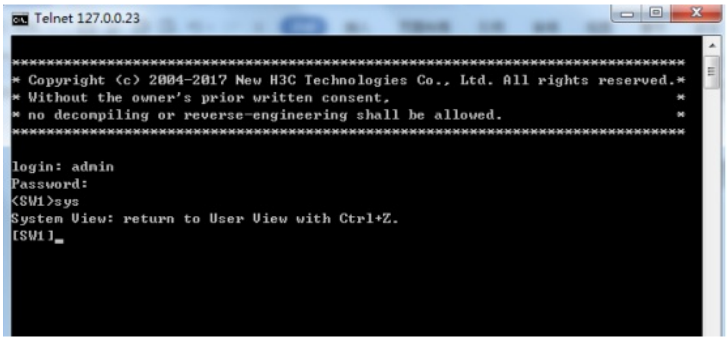
```
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator.USER-20190510MA>telnet 127.0.0.23 2323
```

连接上了发布出来的SW1的telnet功能，输入用户名和密码，回车：



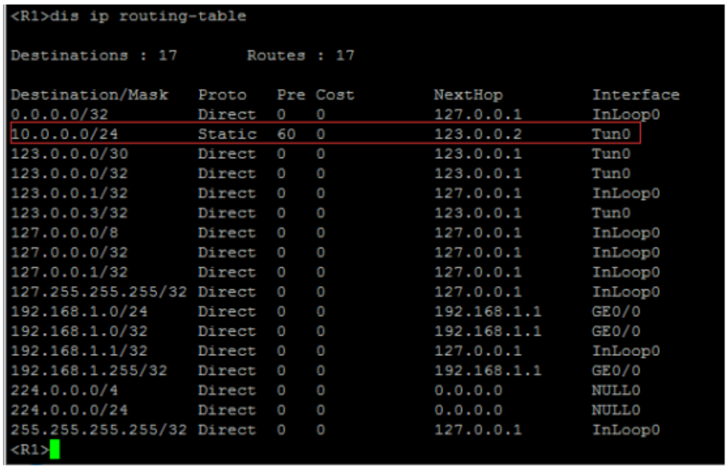
```
******************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: _
```

成功登陆SW1：



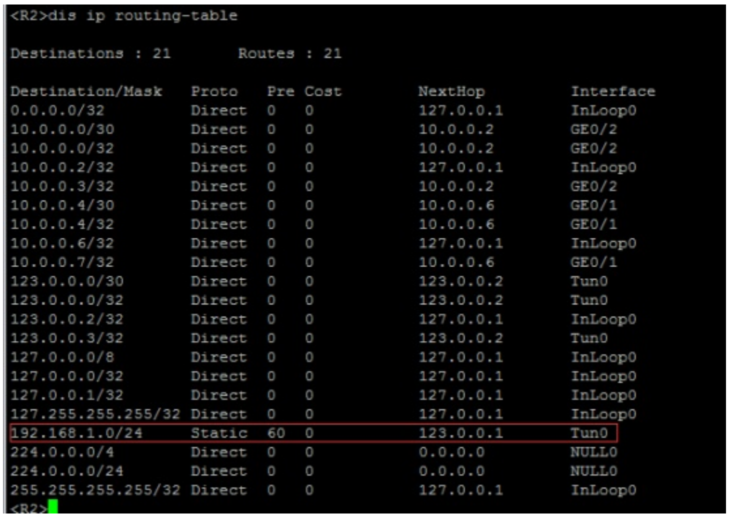
```
******************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: admin
Password:
<SW1>sys
System View: return to User View with Ctrl+Z.
[SW1]_
```

查看R1的路由表，可看到隧道的路由：



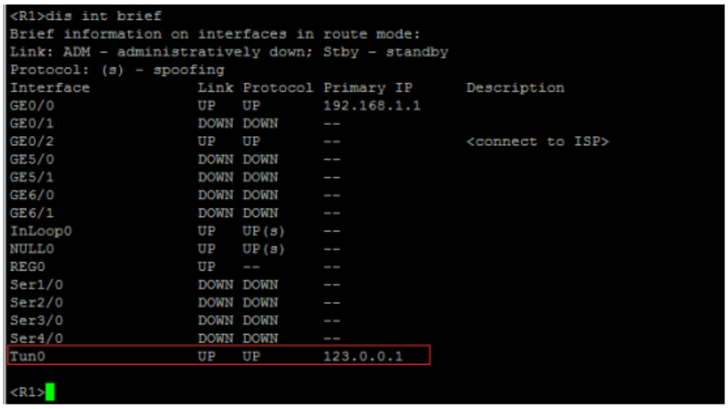
```
<R1>dis ip routing-table

Destinations : 17       Routes : 17

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
10.0.0.0/24        Static  60  0           123.0.0.2       Tun0
123.0.0.0/30       Direct  0   0           123.0.0.1       Tun0
123.0.0.0/32       Direct  0   0           123.0.0.1       Tun0
123.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
123.0.0.3/32       Direct  0   0           123.0.0.1       Tun0
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
192.168.1.0/24     Direct  0   0           192.168.1.1     GE0/0
192.168.1.0/32     Direct  0   0           192.168.1.1     GE0/0
192.168.1.1/32     Direct  0   0           127.0.0.1       InLoop0
192.168.1.255/32   Direct  0   0           192.168.1.1     GE0/0
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
<R1>
```

查看R2的路由表，可看到隧道的路由：



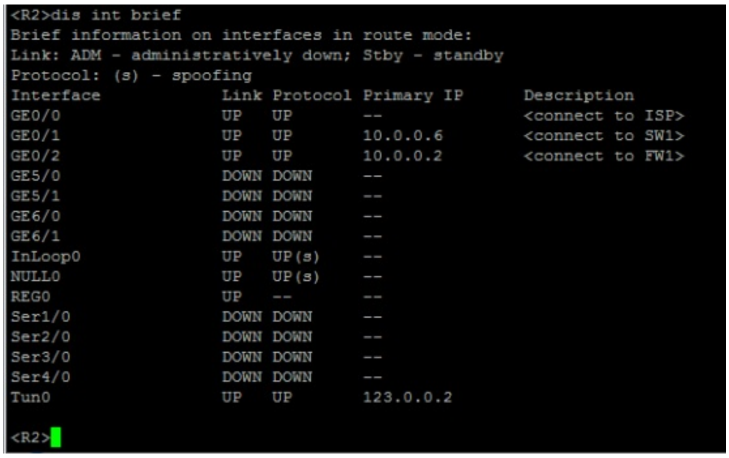
```
<R2>dis ip routing-table

Destinations : 21       Routes : 21

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct  0    0            127.0.0.1       InLoop0
10.0.0.0/30         Direct  0    0            10.0.0.2        GE0/2
10.0.0.0/32         Direct  0    0            10.0.0.2        GE0/2
10.0.0.2/32         Direct  0    0            127.0.0.1       InLoop0
10.0.0.3/32         Direct  0    0            10.0.0.2        GE0/2
10.0.0.4/30         Direct  0    0            10.0.0.6        GE0/1
10.0.0.4/32         Direct  0    0            10.0.0.6        GE0/1
10.0.0.6/32         Direct  0    0            127.0.0.1       InLoop0
10.0.0.7/32         Direct  0    0            10.0.0.6        GE0/1
123.0.0.0/30        Direct  0    0            123.0.0.2       Tun0
123.0.0.0/32        Direct  0    0            123.0.0.2       Tun0
123.0.0.2/32        Direct  0    0            127.0.0.1       InLoop0
123.0.0.3/32        Direct  0    0            123.0.0.2       Tun0
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0            127.0.0.1       InLoop0
192.168.1.0/24      Static  60   0            123.0.0.1       Tun0
224.0.0.0/4         Direct  0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct  0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct  0    0            127.0.0.1       InLoop0
<R2>
```

查看R1的隧道状态：



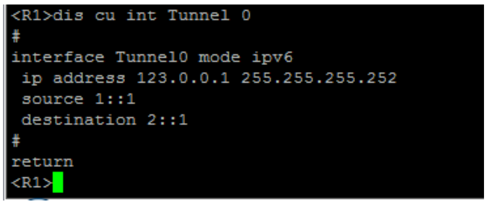
```
<R1>dis int brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
GE0/0                UP   UP       192.168.1.1
GE0/1                DOWN DOWN     --
GE0/2                UP   UP       --              <connect to ISP>
GE5/0                DOWN DOWN     --
GE5/1                DOWN DOWN     --
GE6/0                DOWN DOWN     --
GE6/1                DOWN DOWN     --
InLoop0              UP   UP(s)    --
NULL0                UP   UP(s)    --
REG0                 UP   --       --
Ser1/0               DOWN DOWN     --
Ser2/0               DOWN DOWN     --
Ser3/0               DOWN DOWN     --
Ser4/0               DOWN DOWN     --
Tun0                 UP   UP       123.0.0.1

<R1>
```

查看R2的隧道状态：



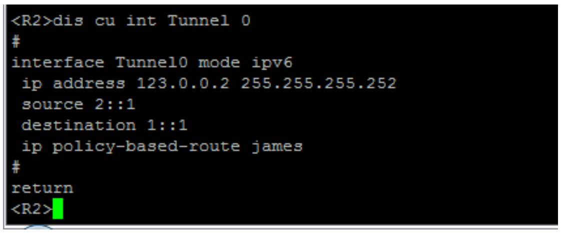
```
<R2>dis int brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
GE0/0                UP   UP       --              <connect to ISP>
GE0/1                UP   UP       10.0.0.6        <connect to SW1>
GE0/2                UP   UP       10.0.0.2        <connect to FW1>
GE5/0                DOWN DOWN     --
GE5/1                DOWN DOWN     --
GE6/0                DOWN DOWN     --
GE6/1                DOWN DOWN     --
InLoop0              UP   UP(s)    --
NULL0                UP   UP(s)    --
REG0                 UP   --       --
Ser1/0               DOWN DOWN     --
Ser2/0               DOWN DOWN     --
Ser3/0               DOWN DOWN     --
Ser4/0               DOWN DOWN     --
Tun0                 UP   UP       123.0.0.2

<R2>
```

查看R1的隧道配置信息：



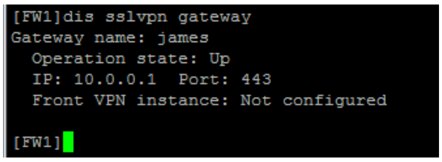
```
<R1>dis cu int Tunnel 0
#
interface Tunnel0 mode ipv6
 ip address 123.0.0.1 255.255.255.252
 source 1::1
 destination 2::1
#
return
<R1>
```

查看R2的隧道配置信息：

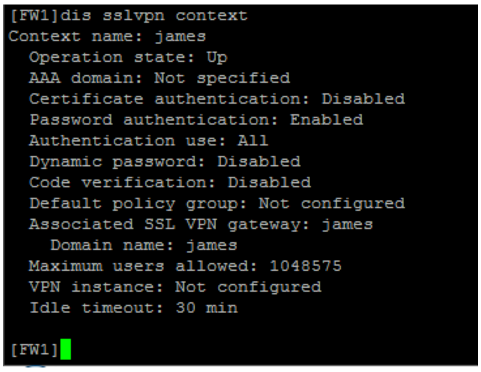


```
<R2>dis cu int Tunnel 0
#
interface Tunnel0 mode ipv6
 ip address 123.0.0.2 255.255.255.252
 source 2::1
 destination 1::1
 ip policy-based-route james
#
return
<R2>
```

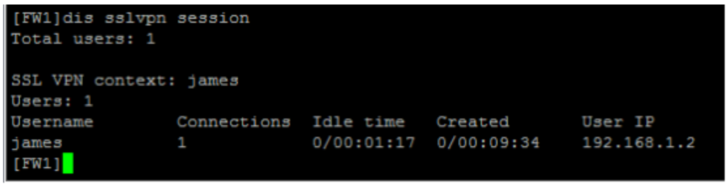
查看FW1的SSL VPN显示信息：



```
[FW1]dis sslvpn gateway
Gateway name: james
  Operation state: Up
  IP: 10.0.0.1  Port: 443
  Front VPN instance: Not configured

[FW1]
```



```
[FW1]dis sslvpn context
Context name: james
  Operation state: Up
  AAA domain: Not specified
  Certificate authentication: Disabled
  Password authentication: Enabled
  Authentication use: All
  Dynamic password: Disabled
  Code verification: Disabled
  Default policy group: Not configured
  Associated SSL VPN gateway: james
    Domain name: james
  Maximum users allowed: 1048575
  VPN instance: Not configured
  Idle timeout: 30 min

[FW1]
```



```
[FW1]dis sslvpn session
Total users: 1

SSL VPN context: james
Users: 1
Username         Connections  Idle time    Created       User IP
james            1            0/00:01:17   0/00:09:34    192.168.1.2
[FW1]
```

至此，IPV6之IPV4 over IPV6 over ssl vpn（双臂旁路TCP接入）典型组网配置案例已完成！