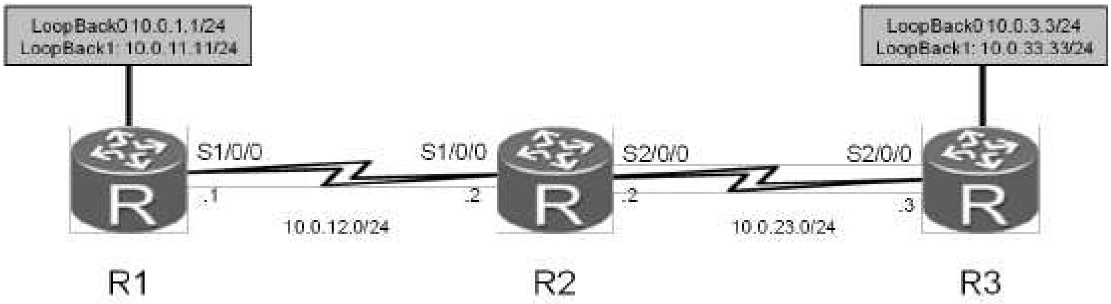
网络实训 实验

IPSec VPN 配置

学习目标

掌握 IPSec 提议的配置方法
掌握使用 ACL 定义感兴趣流的方法
掌握 IPSec 策略的配置方法
掌握在接口绑定 IPSec 策略的方法

拓扑图



IPSec VPN 实验拓扑图

场景

企业的某些私有数据在公网传输时要确保完整性和机密性。作为企业的网络管理员，您需要在企业总部的边缘路由器（R1）和分支机构路由器（R3）之间部署 IPSec VPN 解决方案，建立 IPSec 隧道，用于安全传输来自指定部门的数据流。

操作步骤

步骤一 实验环境准备

```
<Jxust>system-view
[Jxust]sysname R1
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ip address 10.0.12.1 24
[R1-Serial1/0/0]quit
[R1]interface loopback 0
[R1-LoopBack0]ip address 10.0.1.1 24

<Jxust>system-view
[Jxust]sysname R2
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]ip address 10.0.12.2 24
```

```
[R2-Serial1/0/0]quit
[R2]interface serial 2/0/0
[R2-Serial2/0/0]ip address 10.0.23.2 24
[R2-Serial2/0/0]quit
[R2]interface loopback 0
[R2-LoopBack0]ip address 10.0.2.2 24
```

```
<Jxust>system-view
[Jxust]sysname R3
[R3]interface Serial 2/0/0
[R3-Serial2/0/0]ip address 10.0.23.3 24
[R3-Serial2/0/0]quit
[R3]interface loopback 0
[R3-LoopBack0]ip address 10.0.3.3 24
```

步骤二

创建逻辑接口

```
[R1-LoopBack0]interface loopback 1
[R1-LoopBack1]ip address 10.0.11.11 24
```

```
[R3-LoopBack0]interface loopback 1
[R3-LoopBack1]ip address 10.0.33.33 24
```

步骤三

配置 OSPF

在 R1、R2 和 R3 上配置 OSPF，将 Loopback 0 的 IP 地址作为路由器的 Router ID，使用 OSPF 的默认进程 1，并将公网网段 10.0.12.0/24 和 10.0.23.0/24 以及环回接口地址通告在 OSPF 区域 0。

```
[R1]ospf router-id 10.0.1.1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.11.0 0.0.0.255
```

```
[R2]ospf router-id 10.0.2.2
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.0.2.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.23.0 0.0.0.255
```

```
[R3]ospf router-id 10.0.3.3
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.0.23.0 0.0.0.255
```

```
[R3-ospf-1-area-0.0.0.0]network 10.0.3.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network 10.0.33.0 0.0.0.255
```

待 OSPF 收敛完成后，查看 OSPF 邻居以及路由表。

```
<R2>display ospf peer brief
OSPF Process 1 with Router ID 10.0.2.2
Peer Statistic Information
----------------------------------------------------------------------------
```

Area Id	Interface	Neighbor id	State
0.0.0.0	Serial1/0/0	10.0.1.1	Full
0.0.0.0	Serial2/0/0	10.0.3.3	Full

```
----------------------------------------------------------------------------
<R1>display ip routing-table
Route Flags: R - relay, D - download to fib
----------------------------------------------------------------------------
Routing Tables: Public
Destinations : 17 Routes : 17
Destination/Mask Proto Pre Cost Flags NextHop Interface
10.0.1.0/24 Direct 0 0 D 10.0.1.1 LoopBack0
10.0.1.1/32 Direct 0 0 D 127.0.0.1 LoopBack0
10.0.1.255/32 Direct 0 0 D 127.0.0.1 LoopBack0
10.0.2.2/32 OSPF 10 781 D 10.0.12.2 Serial1/0/0
10.0.3.3/32 OSPF 10 2343 D 10.0.12.2 Serial1/0/0
10.0.11.0/24 Direct 0 0 D 10.0.11.11 LoopBack1
10.0.11.11/32 Direct 0 0 D 127.0.0.1 LoopBack1
10.0.11.255/32 Direct 0 0 D 127.0.0.1 LoopBack1
10.0.12.0/24 Direct 0 0 D 10.0.12.1 Serial1/0/0
10.0.12.1/32 Direct 0 0 D 127.0.0.1 Serial1/0/0
10.0.12.2/32 Direct 0 0 D 10.0.12.2 Serial1/0/0
10.0.12.255/32 Direct 0 0 D 127.0.0.1 Serial1/0/0
10.0.23.0/24 OSPF 10 2343 D 10.0.12.2 Serial1/0/0
10.0.33.33/32 OSPF 10 2343 D 10.0.12.2 Serial1/0/0
127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0
127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
127.255.255.255/32 Direct 0 0 D 127.0.0.1 InLoopBack0
255.255.255.255/32 Direct 0 0 D 127.0.0.1 InLoopBack0
```

步骤四 配置 ACL 定义感兴趣流

配置高级 ACL 来定义 IPSec VPN 的感兴趣流。高级 ACL 能够基于特定的参数来匹配流量。

```
[R1]acl 3001
[R1-acl-adv-3001]rule 5 permit ip source 10.0.1.0 0.0.0.255 destination 10.0.3.0 0.0.0.255

[R3]acl 3001
[R3-acl-adv-3001]rule 5 permit ip source 10.0.3.0 0.0.0.255 destination 10.0.1.0 0.0.0.255
```

步骤五 配置 IPSec VPN 提议

创建 IPSec 提议，并进入 IPSec 提议视图来指定安全协议。注意确保隧道两端的设备使用相同的安全协议。

```
[R1]ipsec proposal tran1
[R1-ipsec-proposal-tran1]esp authentication-algorithm sha1
[R1-ipsec-proposal-tran1]esp encryption-algorithm 3des

[R3]ipsec proposal tran1
[R3-ipsec-proposal-tran1]esp authentication-algorithm sha1
[R3-ipsec-proposal-tran1]esp encryption-algorithm 3des
```

执行 display ipsec proposal 命令，验证配置结果。

```
[R1]display ipsec proposal
Number of proposals: 1
IPSec proposal name : tran1
Encapsulation mode : Tunnel
Transform : esp-new
ESP protocol : Authentication SHA1-HMAC-96
Encryption 3DES
[R3]display ipsec proposal
Number of proposals: 1
IPSec proposal name : tran1
Encapsulation mode : Tunnel
Transform : esp-new
ESP protocol : Authentication SHA1-HMAC-96
Encryption 3DES
```

步骤六 创建 IPSec 策略

手工创建 IPSec 策略，每一个 IPSec 安全策略都使用唯一的名称和序号来标识，IPSec 策略中会应用 IPSec 提议中定义的安全协议、认证算法、加密算法和封装模式，手工创建的 IPSec 策略还需配置安全联盟（SA）中的参数。

```
[R1]ipsec policy P1 10 manual
[R1-ipsec-policy-manual-P1-10]security acl 3001
[R1-ipsec-policy-manual-P1-10]proposal tran1
[R1-ipsec-policy-manual-P1-10]tunnel remote 10.0.23.3

[R1-ipsec-policy-manual-P1-10]tunnel local 10.0.12.1
[R1-ipsec-policy-manual-P1-10]sa spi outbound esp 54321
[R1-ipsec-policy-manual-P1-10]sa spi inbound esp 12345
[R1-ipsec-policy-manual-P1-10]sa string-key outbound esp simple jxust
[R1-ipsec-policy-manual-P1-10]sa string-key inbound esp simple jxust

[R3]ipsec policy P1 10 manual
```

```
[R3-ipsec-policy-manual-P1-10]security acl 3001
[R3-ipsec-policy-manual-P1-10]proposal tran1
[R3-ipsec-policy-manual-P1-10]tunnel remote 10.0.12.1
[R3-ipsec-policy-manual-P1-10]tunnel local 10.0.23.3
[R3-ipsec-policy-manual-P1-10]sa spi outbound esp 12345
[R3-ipsec-policy-manual-P1-10]sa spi inbound esp 54321
[R3-ipsec-policy-manual-P1-10]sa string-key outbound esp simple jxust
[R3-ipsec-policy-manual-P1-10]sa string-key inbound esp simple jxust
```

执行 display ipsec policy 命令，验证配置结果。

```
<R1>display ipsec policy
===========================================
IPSec policy group: "P1"
Using interface:
===========================================
Sequence number: 10
Security data flow: 3001
Tunnel local address: 10.0.12.1
Tunnel remote address: 10.0.23.3
Qos pre-classify: Disable
Proposal name:tran1
Inbound AH setting:
AH SPI:
AH string-key:
AH authentication hex key:
Inbound ESP setting:
ESP SPI: 12345 (0x3039)
ESP string-key: jxust
ESP encryption hex key:
ESP authentication hex key:
Outbound AH setting:

AH SPI:
AH string-key:
AH authentication hex key:
Outbound ESP setting:
ESP SPI: 54321 (0xd431)
ESP string-key: jxust
ESP encryption hex key:
ESP authentication hex key:
```

```
<R3>display ipsec policy
===========================================
IPSec policy group: "P1"
```

```
Using interface:
============================================
Sequence number: 10
Security data flow: 3001
Tunnel local address: 10.0.23.3
Tunnel remote address: 10.0.12.1
Qos pre-classify: Disable
Proposal name:tran1
Inbound AH setting:
AH SPI:
AH string-key:
AH authentication hex key:
Inbound ESP setting:
ESP SPI: 54321 (0xd431)
ESP string-key: jxust
ESP encryption hex key:
ESP authentication hex key:
Outbound AH setting:
AH SPI:
AH string-key:
AH authentication hex key:
Outbound ESP setting:
ESP SPI: 12345 (0x3039)
ESP string-key: jxust
ESP encryption hex key:
ESP authentication hex key:
```

步骤七 在接口下应用 IPSec 策略

在物理接口应用 IPSec 策略，接口将对感兴趣流量进行 IPSec 加密处理。

```
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ipsec policy P1

[R3]interface Serial 2/0/0
[R3-Serial2/0/0]ipsec policy P1
```

步骤八 检测网络的连通性

验证设备对不感兴趣流量不进行 IPSec 加密处理。

```
<R1>ping -a 10.0.11.11 10.0.33.33
PING 10.0.33.33: 56
data bytes, press CTRL_C to break
Reply from 10.0.33.33: bytes=56 Sequence=1 ttl=254 time=60 ms
Reply from 10.0.33.33: bytes=56 Sequence=2 ttl=254 time=50 ms
Reply from 10.0.33.33: bytes=56 Sequence=3 ttl=254 time=50 ms
Reply from 10.0.33.33: bytes=56 Sequence=4 ttl=254 time=60 ms
Reply from 10.0.33.33: bytes=56 Sequence=5 ttl=254 time=50 ms
--- 10.0.33.33 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 50/54/60 ms
```

```
<R1>display ipsec statistics esp
Inpacket count : 0
Inpacket auth count : 0
Inpacket decap count : 0
Outpacket count : 0
Outpacket auth count : 0
Outpacket encap count : 0
Inpacket drop count : 0
Outpacket drop count : 0
BadAuthLen count : 0
AuthFail count : 0
InSAAclCheckFail count : 0
PktDuplicateDrop count : 0
PktSeqNoTooSmallDrop count : 0
PktInSAMissDrop count : 0
```

验证设备将对感兴趣流量进行 IPSec 加密处理。

```
<R1>ping -a 10.0.1.1 10.0.3.3
PING 10.0.3.3: 56 data bytes, press CTRL_C to break
Reply from 10.0.3.3: bytes=56 Sequence=1 ttl=255 time=80 ms
Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=255 time=77 ms
Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=255 time=77 ms
Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=255 time=80 ms
Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=255 time=77 ms
--- 10.0.3.3 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 77/78/80 ms
```

```
<R1>display ipsec statistics esp
Inpacket count : 5
Inpacket auth count : 0
Inpacket decap count : 0
Outpacket count : 5
Outpacket auth count : 0
Outpacket encap count : 0
```

```
Inpacket drop count : 0
Outpacket drop count : 0
BadAuthLen count : 0
AuthFail count : 0
InSAAclCheckFail count : 0
PktDuplicateDrop count : 0
PktSeqNoTooSmallDrop count : 0
PktInSAMissDrop count : 0
```

配置文件

```
<R1>display current-configuration
[V200R007C00SPC600]
#
sysname R1
#
acl number 3001
rule 5 permit ip source 10.0.1.0 0.0.0.255 destination 10.0.3.0 0.0.0.255
#
ipsec proposal tran1
esp authentication-algorithm sha1
esp encryption-algorithm 3des
#
ipsec policy P1 10 manual
security acl 3001
proposal tran1
tunnel local 10.0.12.1
tunnel remote 10.0.23.3
sa spi inbound esp 12345
sa string-key inbound esp simple jxust
sa spi outbound esp 54321
sa string-key outbound esp simple jxust
#
interface Serial1/0/0
link-protocol ppp
ppp authentication-mode pap
ip address 10.0.12.1 255.255.255.0
ipsec policy P1
baudrate 128000
#
interface LoopBack0
ip address 10.0.1.1 255.255.255.0
#
interface LoopBack1
ip address 10.0.11.11 255.255.255.0
```

```
#
ospf 1 router-id 10.0.1.1
area 0.0.0.0
network 10.0.1.0 0.0.0.255
network 10.0.11.0 0.0.0.255
network 10.0.12.0 0.0.0.255
#
user-interface con 0
authentication-mode password
set authentication password cipher %$%$dD#}P<HzJ;Xs%X>hOkm!,.+Iq61QK`K6tI}cc
-;k_o`C.+L,%$%$
user-interface vty 0 4
authentication-mode aaa
#
return
<R2>display current-configuration
[V200R007C00SPC600]
#
sysname R2
#
interface Serial1/0/0
link-protocol ppp
ppp pap local-user jxust password cipher %$%$u[hr6d<JVHR@->T7xr1<$.iv%$%$
ip address 10.0.12.2 255.255.255.0
#
interface Serial2/0/0
link-protocol ppp
ppp chap user jxust
ppp chap password cipher %$%$e{5h)gh"/Uz0mUC%vEx3$4<m%$%$
ip address 10.0.23.2 255.255.255.0
#
interface LoopBack0
ip address 10.0.2.2 255.255.255.0
#
ospf 1 router-id 10.0.2.2
area 0.0.0.0
network 10.0.12.0 0.0.0.255
network 10.0.23.0 0.0.0.255
#
user-interface con 0
authentication-mode password
set authentication password cipher %$%$|nRPL^hr2IXi7LHDID!/,.*%.8%h;3:,hXO2d
k#ikaWI.*(,%$%$
user-interface vty 0 4
```

```
#
return
<R3>display current-configuration
[V200R007C00SPC600]
#
sysname R3
#
acl number 3001
rule 5 permit ip source 10.0.3.0 0.0.0.255 destination 10.0.1.0 0.0.0.255
#
ipsec proposal tran1
esp authentication-algorithm sha1
esp encryption-algorithm 3des
#
ipsec policy P1 10 manual
security acl 3001
proposal tran1
tunnel local 10.0.23.3
tunnel remote 10.0.12.1
sa spi inbound esp 54321
sa string-key inbound esp simple jxust
sa spi outbound esp 12345
sa string-key outbound esp simple jxust
#
interface Serial2/0/0
link-protocol ppp
ppp authentication-mode chap
ip address 10.0.23.3 255.255.255.0
ipsec policy P1
#
interface LoopBack0
ip address 10.0.3.3 255.255.255.0
#
interface LoopBack1
ip address 10.0.33.33 255.255.255.0
#
ospf 1 router-id 10.0.3.3
area 0.0.0.0
network 10.0.3.0 0.0.0.255
network 10.0.23.0 0.0.0.255
network 10.0.33.0 0.0.0.255
#
user-interface con 0
authentication-mode password
```

```
set authentication password cipher %$%$W|$)M5D}v@bY^gK\;>QR,.*d;8Mp>|+EU,:~D
~8b59~..*g,%$%$
user-interface vty 0 4
authentication-mode aaa
#
return
```