

实验四十五、VPN (IKE) 的配置

一、 实验目的

1. 掌握 VPN (IKE) 的配置
2. 理解 IKE 在隧道建立过程中的作用

二、 应用环境

IKE (Internet 密钥交换) 技术提供额外的特性, 使配置 IPSec 时更加灵活和容易

三、 实验设备

1. DCR-1751 两台
2. PC 机 两台

四、 实验拓扑



五、 实验要求

配置表

Router-A

F0/0 192.168.0.1/24
S1/1 (DCE) 192.168.1.1/24

PC

IP 192.168.0.10/24
网关 192.168.0.1

Router-B

F0/0 192.168.2.1/24
S1/0 192.168.1.2/24

SERVER

192.168.2.2/24
192.168.2.1

结果:

在路由器 A 与 B 之间建立 VPN, 保护从 PC 到 SERVER 的数据

六、 实验步骤

第一步: 路由器 A 的配置

```
Router-A#conf
Router-A_config#ip access-list extended 101          ! 确定要经过 VPN 保护的数据流
Router-A_config_ext_nacl#permi ip 192.168.0.0 255.255.255.0 192.168.2.0 255.255.255.0
Router-A_config_ext_nacl#exit
Router-A_config#ip route 0.0.0.0 0.0.0.0 192.168.1.2    ! 配置静态路由
Router-A_config#crypt isakmp policy 10                ! 配置 IKE 策略
Router-A_config_isakmp#authentication pre-share         ! 设置认证方式
Router-A_config_isakmp#encryption des                  ! 设置加密方式
Router-A_config_isakmp#hash md5                        ! 设置数字签名算法
Router-A_config_isakmp#group 1                         ! 设置 DH 方式
Router-A_config_isakmp#lifetime 86400                  ! 设置生存期
Router-A_config_isakmp#exit
Router-A_config#crypto isakmp key digital 192.168.1.2    ! 设置共用密钥
Router-A_config#crypto ipsec transform-set one          ! 设置变换集
Router-A_config_crypto_trans#transform-type esp-des esp-md5-hmac ! ESP 加密和验证
Router-A_config_crypto_trans#mode tunnel                ! 设置为隧道模式
Router-A_config_crypto_trans#exit
Router-A_config#crypto map my 10 ipsec-isakmp           ! 配置 IPSec 加密映射
Router-A_config_crypto_map#set transform-set one        ! 关联变换集
Router-A_config_crypto_map#set peer 192.168.1.2         ! 设置对等体地址
Router-A_config_crypto_map#match address 101            ! 关联需要加密的数据流
Router-A_config_crypto_map#exit
Router-A_config#int s1/1                                ! 进入 VPN 的接口
Router-A_config_s1/1#crypto map my                      ! 绑定 IPSec 加密映射
Router-A_config_s1/1#^Z
```

第二步: 查看配置

```
Router-A#sh crypto isakmp policy          ! 查看 IKE 策略
Protection suite of priority 10
  encryption algorithm:  DES   - Data Encryption Standard (56 bit keys).
  hash algorithm:       Message Digest 5
  authentication method: Pre-Shared Key
  Diffie-Hellman group: #1 (768 bit)
  lifetime:             86400 seconds

Default protection suite
  encryption algorithm:  DES   - Data Encryption Standard (56 bit keys).
  hash algorithm:       Secure Hash Standard
  authentication method: Pre-Shared Key
  Diffie-Hellman group: #1 (768 bit)
  lifetime:             86400 seconds
```

Router-A#**sh crypto isakmp sa** ! 查看 IKE 安全关联 (没有建立, 为空)

Router-A#**sh crypto map** ! 查看 IPSec 映射

```
Crypto Map my 10 ipsec-isakmp
  Extended IP access list 101
    permit ip 192.168.0.0 255.255.255.0 192.168.2.0 255.255.255.0
  peer = 192.168.1.2
  PFS (Y/N): N
  Security association lifetime: 4608000 kilobytes/3600 seconds
  Transform sets={ one, }
```

Router-A#**sh crypto ipsec sa** ! 查看 IPSec 关联

```
Interface: Serial1/1
Crypto map name:my , local addr. 192.168.1.1

local ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
local crypto endpt.: 192.168.1.1, remote crypto endpt.: 192.168.1.2
```

Router-A#**sh crypto ipsec transform-set** ! 查看变换集

```
Transform set one: { esp-des esp-md5-hmac }
will negotiate = { Tunnel }
```

第三步: 路由器 B 的配置

Router-B>**ena**

Router-B#**conf**

Router-B_config#**ip access-list extended 101**

Router-B_config_ext_nacl#**permit ip 192.168.2.0 255.255.255.0 192.168.0.0 255.255.255.0**

Router-B_config_ext_nacl#**exit**

Router-B_config#**ip route 192.168.0.0 255.255.255.0 192.168.1.1**

Router-B_config#**crypto isakmp policy 10** ! 注意与 A 要一致

Router-B_config_isakmp#**authentication pre-share**

Router-B_config_isakmp#**hash md5**

Router-B_config_isakmp#**encryption des**

Router-B_config_isakmp#**group 1**

Router-B_config_isakmp#**lifetime 86400**

Router-B_config_isakmp#**exit**

Router-B_config#**crypto isakmp key digital 192.168.1.1** ! 注意与 A 要一致

Router-B_config#**crypto ipsec transform-set one**

Router-B_config_crypto_trans#**transform-type esp-des esp-md5-hmac** ! 注意与 A 要一致

Router-B_config_crypto_trans#**mode tunnel**

```
Router-B_config_crypto_trans#exit
Router-B_config#crypto map my 10 ipsec-isakmp
Router-B_config_crypto_map#set transform-set one
Router-B_config_crypto_map#set peer 192.168.1.1
Router-B_config_crypto_map#match address 101
Router-B_config_crypto_map#exit
Router-B_config#int s1/0
Router-B_config_s1/0#crypto map my
Router-B_config_s1/0#^Z
```

! 注意与 A 要一致

第四步：查看配置

Router-B#**sh crypto isakmp policy**

Protection suite of priority 10

encryption algorithm:	DES - Data Encryption Standard (56 bit keys).
hash algorithm:	Message Digest 5
authentication method:	Pre-Shared Key
Diffie-Hellman group:	#1 (768 bit)
lifetime:	86400 seconds

Default protection suite

encryption algorithm:	DES - Data Encryption Standard (56 bit keys).
hash algorithm:	Secure Hash Standard
authentication method:	Pre-Shared Key
Diffie-Hellman group:	#1 (768 bit)
lifetime:	86400 seconds

Router-B#**sh crypto isakmp sa**

Router-B#**sh crypto ipsec sa**

Interface: Serial1/0

Crypto map name:my , local addr. 192.168.1.2

local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)

local crypto endpt.: 192.168.1.2, remote crypto endpt.: 192.168.1.1

Router-B#**sh crypto ipsec transform-set**

Transform set one: { esp-des esp-md5-hmac }

will negotiate ={ Tunnel }

Router-B#**sh crypto map**

Crypto Map my 10 ipsec-isakmp

Extended IP access list 101

permit ip 192.168.2.0 255.255.255.0 192.168.0.0 255.255.255.0

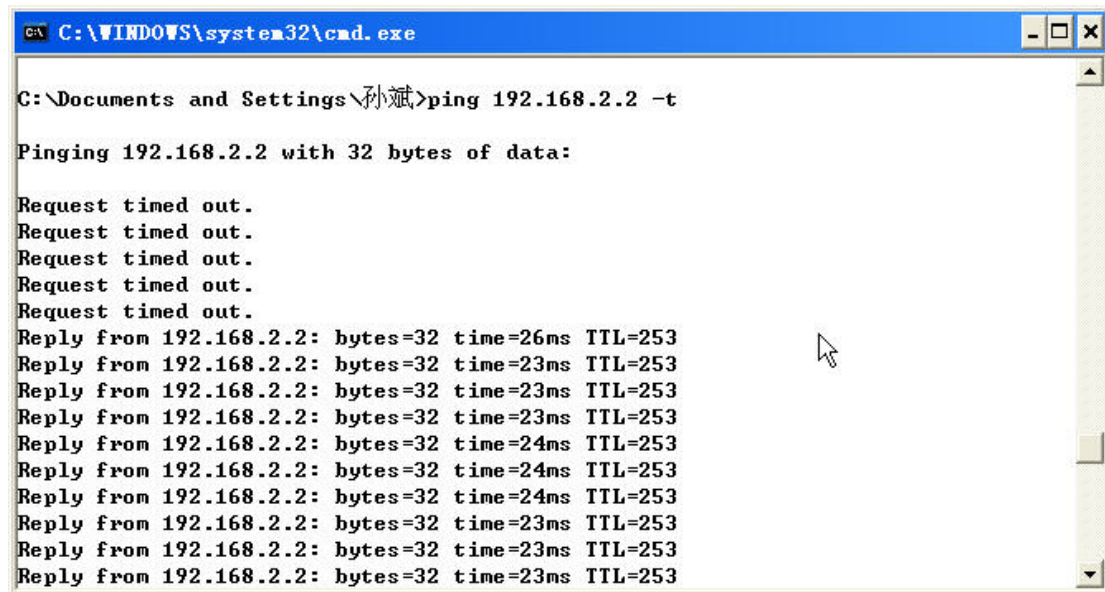
peer = 192.168.1.1

PFS (Y/N): N

Security association lifetime: 4608000 kilobytes/3600 seconds

Transform sets={ one, }

第五步: 测试



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\孙斌>ping 192.168.2.2 -t

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.2.2: bytes=32 time=26ms TTL=253
Reply from 192.168.2.2: bytes=32 time=23ms TTL=253
Reply from 192.168.2.2: bytes=32 time=23ms TTL=253
Reply from 192.168.2.2: bytes=32 time=23ms TTL=253
Reply from 192.168.2.2: bytes=32 time=24ms TTL=253
Reply from 192.168.2.2: bytes=32 time=24ms TTL=253
Reply from 192.168.2.2: bytes=32 time=24ms TTL=253
Reply from 192.168.2.2: bytes=32 time=23ms TTL=253
Reply from 192.168.2.2: bytes=32 time=23ms TTL=253
Reply from 192.168.2.2: bytes=32 time=23ms TTL=253
```

再次查看安全关联:

Router-B#sh crypto isakmp sa

dst	src	state	state-id	conn
192.168.1.1	192.168.1.2	<R>Q_SA_SETUP	2	3 my 10
192.168.1.1	192.168.1.2	<R>M_SA_SETUP	1	3 my 10

Router-B#sh crypto ipsec sa

Interface: Serial1/0

Crypto map name:my , local addr. 192.168.1.2

local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)

local crypto endpt.: 192.168.1.2, remote crypto endpt.: 192.168.1.1

inbound esp sas:

spi:0x6a83b104(1787015428)

transform: esp-des esp-md5-hmac

in use settings={ Tunnel }

sa timing: remaining key lifetime (k/sec): (4607996/3073)

outbound esp sas:

spi:0xfe0d0282(4262265474)

transform: esp-des esp-md5-hmac

in use settings={ Tunnel }

sa timing: remaining key lifetime (k/sec): (4607998/3072)

七、 注意事项和排错

1. 注意两端参数要一致
2. ACL 的作用是确定哪些数据需要经过 VPN

八、 配置序列

Router-A#show running-config
Building configuration...

Current configuration:

```
!  
!version 1.3.2E  
service timestamps log date  
service timestamps debug date  
no service password-encryption  
!  
hostname Router-A  
!  
!  
!  
!  
!  
crypto isakmp key digital 192.168.1.2 255.255.255.255  
!  
crypto isakmp policy 10  
  hash md5  
!  
crypto ipsec transform-set one  
  transform-type esp-des esp-md5-hmac  
!  
crypto map my 10 ipsec-isakmp  
  set peer 192.168.1.2  
  set transform-set one  
  match address 101  
!  
!  
!  
!  
interface FastEthernet0/0  
  ip address 192.168.0.1 255.255.255.0  
  no ip directed-broadcast
```




```
!  
interface Serial1/0  
  no ip address  
  no ip directed-broadcast  
  physical-layer speed 64000  
!  
interface Serial1/1  
  ip address 192.168.1.1 255.255.255.0  
  no ip directed-broadcast  
  crypto map my  
  physical-layer speed 64000  
!  
interface Async0/0  
  no ip address  
  no ip directed-broadcast  
!  
!  
!  
!  
ip route default 192.168.1.2  
!  
!  
!  
!  
!  
!  
!  
ip access-list extended 101  
  permit ip 192.168.0.0 255.255.255.0 192.168.2.0 255.255.255.0  
!  
!  
!
```

九、 共同思考

1. IKE 的作用是什么?
2. ACL 的作用是什么?

十、 课后练习

请重复以上实验



十一、 相关命令详解

transform-type

加密变换配置态下，要设置变换类型，使用 transform-type 命令。
transform-type transform1 [transform2[transform3]]

参数

参数	参数说明
transform1/ transform2/ transform3	可以指定3个以下的变换。这些变换定义了IPSec安全协议和算法。可接受的变换值在“使用说明”中详细阐述。

缺省

缺省的变换类型为 ESP-DES（ESP 采用 DES 加密算法）

命令模式

加密变换配置态

使用说明

变换集合可以指定一个或两个 IPSec 安全协议（或 ESP，或 AH，或两者都有），并且指定和选定的安全协议一起使用哪种算法。ESP 和 AH IPSec 安全协议在“IPSec 协议：封装安全协议和校验头”一节中做了详细阐述。

变换集合的定义可以指定一到三个变换——每个变换代表一个 IPSec 安全协议(ESP 或 AH)和想要使用的算法的组合。当 IPSec 安全联盟协商时使用了某一变换集合，整个变换集合(协议、算法和其它设置的组合)必须和对端的一个变换集合相匹配。

在一个变换集合中，可以指定 AH 协议、ESP 或两者都指定。如果在变换集合中指定了一个 ESP，那么可以只定义 ESP 加密变换，也可以 ESP 加密变换和 ESP 验证变换两者都定义。下表中显示了可行的变换组合。

为变换集合选择变换：可行的变换组合					
AH 变换中选择一种		ESP 加密变换中选择一种		ESP 验证变换中选择一种，	
变换	描述	变换	描述	变换	描述
ah-md5-hmac	带 MD5（HMAC 变量）的AH验证算法	esp-des	采用 DES 的 ESP 加密算法	esp-md5-hmac	带 MD5（HMAC 变量）的ESP验证算法

ah-sha-hmac	带 SHA (HMAC 变 量) 的 AH 验 证算法	esp-3des	采用3DES的 ESP 加 密 算 法	esp-sha-hmac	带 SHA (HMAC 变 量) 的 ESP 验 证算法
-------------	--	----------	---------------------------	--------------	---

IPSec 协议：ESP 和 AH

ESP 和 AH 协议都为 IPSec 提供了安全服务。

ESP 提供了分组加密，以及可选的数据验证和抗重播服务。

AH 提供了数据验证和抗重播服务。

ESP 使用一个 ESP 头和一个 ESP 尾对受保护数据——或是一个完整的 IP 自寻址数据包（或仅是有效负载）——进行封装。AH 是嵌入在受保护数据中的；它将一个 AH 头直接插入在外部 IP 头后、内部 IP 数据包或有效负载前。隧道模式中要对整个 IP 数据报文进行封装和保护，而传送模式中只对 IP 数据报文中的有效负载进行封装/保护。要进一步了解这两种模式，请参阅 mode 命令的描述。

选择适当的变换

IPSec 变换比较复杂。下面的提示能够帮助你选择适合自己情况的变换：

- 1 如果想要提供数据机密性，那么可以使用 ESP 加密变换。
- 1 如果想要提供对外部 IP 报头以及数据的数据验证，那么可以使用 AH 变换。
- 1 如果使用一个 ESP 加密变换，那么可以考虑使用 ESP 验证变换或 AH 变换来提供变换集合的验证服务。
- 1 如果想要数据验证功能（或使用 ESP 或使用 AH），可以选择 MD5 或 SHA 验证算法。

SHA 算法比 MD5 要健壮，但速度更慢。

加密变换配置态

在执行了 crypto ipsec transform-set 命令以后，就将进入加密变换配置态。在这种状态下，可以将模式改变到隧道模式或传输模式（这是可选的改变）。在做完这些改变以后，键入 exit 来返回到全局配置态下。要深入了解这些可选改变的信息，请参看 mode 命令的详细阐述。

改变现存的变换

如果在 transform-type 命令中为一个变换集合指定一个或多个变换，那么指定的这些变换将会替换掉变换集合中现存的变换。如果改变了 transform-type，改变将只被运用到引用了此变换集合的加密映射表上。但改变将不会被运用到现存的安全联盟上，会被用于新建立的安全联盟。如果想让新的设置立即生效，可以使用 clear crypto sa 命令来清除安全联盟数据库的部分或全部。

示例

以下例子定义了一个变换集合。

```
crypto ipsec transform-set one
transform-type esp-des esp-sha-hmac
```