实验四十四、VPN（IPSec）的配置

一、 实验目的

1. 掌握手工配置密钥建立 VPN 的配置
2. 理解密钥在隧道建立过程中的作用

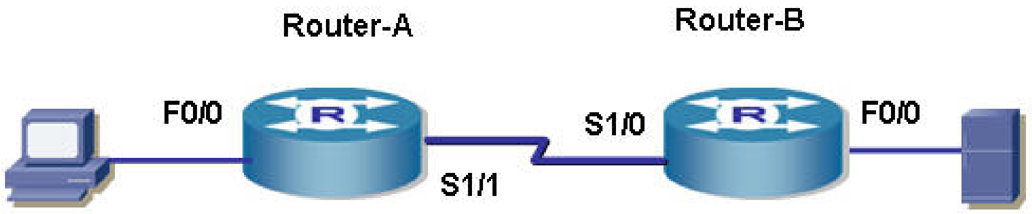
二、 应用环境

IPSec 实现了在网络上的数据机密性、完整性和源认证的功能，有效的保护了数据。手工配置密钥减少了密钥交换的开销，提高了效率

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		**Router-B**	
F0/0	192.168.0.1/24	F0/0	192.168.2.1/24
S1/1 (DCE)	192.168.1.1/24	S1/0	192.168.1.2/24
PC		**SERVER**	
IP	192.168.0.10/24		192.168.2.2/24
网关	192.168.0.1		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#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#exit
Router-A_config#crypto map my 10 ipsec-manu                  ！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#set security-association inbound esp 2001 cipher ffeeddccbbaa00112233445566778899998877665544332
 Router-A_config_crypto_map#set security-association inbound ah 2000 ffeeddccbbaa00112233445566778899
 Router-A_config_crypto_map#set security-association outbound esp 1001 cipher aabbccddeeff00112233445566778899998877665544332
 Router-A_config_crypto_map#set security-association outbound ah 1000 aabbccddeeff00112233445566778899
                                                           ！手工配置密钥
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（两端 VPN 建议成功以后的显示）

```
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
 inbound esp sas:
   spi:0x7d1(2001)
     transform:   esp-3des
     in use settings ={ Tunnel }
     no sa timing

 inbound ah sas:
   spi:0x7d0(2000)
     transform:    ah-md5-hmac
     in use settings ={ Tunnel }
     no sa timing

 outbound esp sas:
   spi:0x3e9(1001)
     transform:    esp-3des
     in use settings ={ Tunnel }
     no sa timing

 outbound ah sas:
   spi:0x3e8(1000)
     transform:    ah-md5-hmac
     in use settings ={ Tunnel }
     no sa timing
```

```
Router-A#sh crypto map                              ！查看 IPSec 映射
Crypto Map my 10 ipsec-manual
          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
          Inbound esp spi: 2001 ,
            cipher key: ffeeddccbbaa001122334455667788999988776655443322 ,
            auth key     ,
          Inbound ah spi: 2000 ,
            key: ffeeddccbbaa00112233445566778899 ,
          Outbound esp spi: 1001 ,
            cipher key: aabbccddeeff001122334455667788999988776655443322 ,
            auth key     ,
          Outbound ah spi: 1000 ,
            key: aabbccddeeff00112233445566778899
          Transform sets={ one}

Router-A#sh crypto ipsec transform-set                    ！查看转换集
Transform set one: { ah-md5-hmac esp-3des }
          will negotiate ={ Tunnel }
```

第三步：路由器 B 的配置

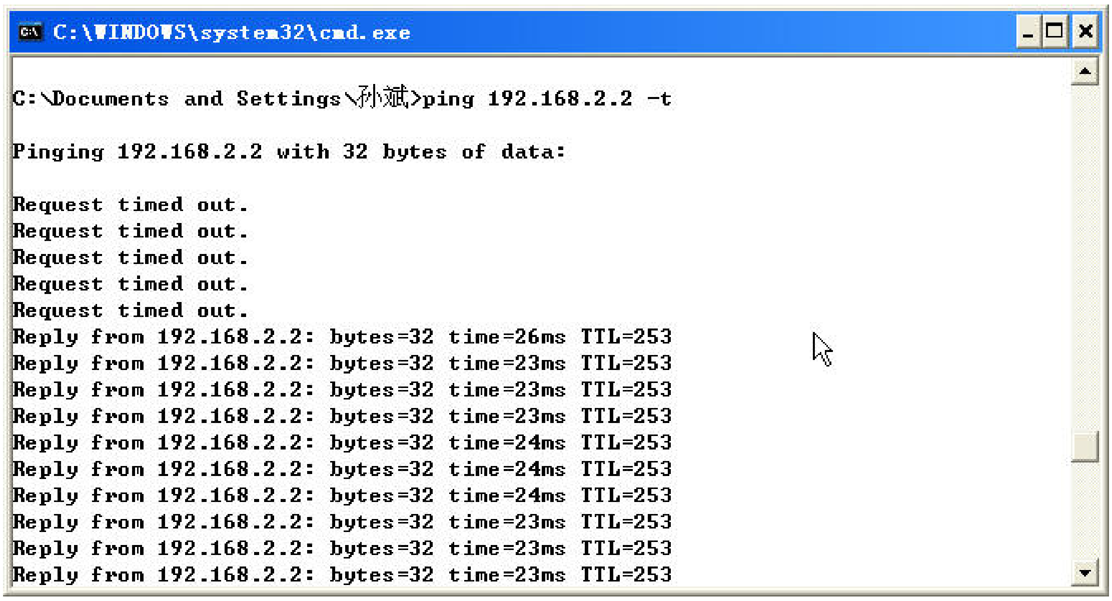
```
Router-B>ena
Router-B#conf
```

```
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 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#exit
Router-B_config#crypto map my 10 ipsec-manu                      ！注意密钥与 A 要对应
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# set security-association inbound esp 1001 cipher aabbccddeeff001122334455667788999988776655443322
 Router-B_config_crypto_map# set security-association inbound ah 1000 aabbccddeeff00112233445566778899
 Router-B_config_crypto_map# set security-association outbound esp 2001 cipher ffeeddccbbaa001122334455667788999988776655443322
 Router-B_config_crypto_map# set security-association outbound ah 2000 ffeeddccbbaa00112233445566778899
                                   ！注意与 A 的对应，inbound 与 outbound 交叉一致
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
```

第四步：查看配置

```
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:0x3e9(1001)
       transform:   esp-3des
       in use settings ={ Tunnel }
       no sa timing

 inbound ah sas:
    spi:0x3e8(1000)
       transform:   ah-md5-hmac
       in use settings ={ Tunnel }
       no sa timing
 outbound esp sas:
    spi:0x7d1(2001)
        transform:    esp-3des
        in use settings ={ Tunnel }
        no sa timing

 outbound ah sas:
    spi:0x7d0(2000)
        transform:    ah-md5-hmac
        in use settings ={ Tunnel }
        no sa timing

Router-B#sh crypto ipsec transform-set
Transform set one: { ah-md5-hmac esp-3des }
        will negotiate ={ Tunnel }

Router-B#sh crypto map
Crypto Map my 10 ipsec-manual
        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
        Inbound esp spi: 1001 ,
          cipher key: aabbccddeeff001122334455667788999988776655443322 ,
          auth key    ,
        Inbound ah spi: 1000 ,
          key: aabbccddeeff00112233445566778899 ,
        Outbound esp spi: 2001 ,
          cipher key: ffeeddccbbaa001122334455667788999988776655443322 ,
          auth key    ,
        Outbound ah spi: 2000 ,
          key: ffeeddccbbaa00112233445566778899
        Transform sets={ one}
```

第五步：测试



```
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
```

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
3. 密钥要交叉对应

八、 配置序列

```
Router-A#sh run
Building configuration...

Current configuration:
!
!version 1.3.2E
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname Router-A
!
!
!
!
!
crypto ipsec transform-set one
 transform-type ah-md5-hmac esp-3des
!
crypto map my 10 ipsec-manual
```

```
 set peer 192.168.1.2
 set security-association inbound esp 2001 cipher ffeeddccbbaa0011223344556677889
999988776655443322
 set security-association inbound ah 2000 ffeeddccbbaa00112233445566778899
 set security-association outbound esp 1001 cipher aabbccddeeff001122334455667788
8999988776655443322
 set security-association outbound ah 1000 aabbccddeeff00112233445566778899
 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
!
!
!




Router-B#sh run
Building configuration...

Current configuration:
!
!version 1.3.2E
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname Router-B
!
ip host a 192.168.1.1
ip host c 192.168.2.2
!
!
!
!
crypto ipsec transform-set one
  transform-type ah-md5-hmac esp-3des
!
crypto map my 10 ipsec-manual
  set peer 192.168.1.1
  set security-association inbound esp 1001 cipher aabbccddeeff0011223344556677889999988776655443322
  set security-association inbound ah 1000 aabbccddeeff00112233445566778899
  set security-association outbound esp 2001 cipher ffeeddccbbaa0011223344556677889999988776655443322
  set security-association outbound ah 2000 ffeeddccbbaa00112233445566778899
  set transform-set one
  match address 101
!
!
!
!
interface FastEthernet0/0
  ip address 192.168.2.1 255.255.255.0
  no ip directed-broadcast
!
interface Serial1/0
  ip address 192.168.1.2 255.255.255.0
  no ip directed-broadcast
  crypto map my
!
interface Async0/0
  no ip address
  no ip directed-broadcast
!
!
!
!
ip route 192.168.0.0 255.255.255.0 192.168.1.1
!
!
!
!
!
!
!
ip access-list extended 101
  permit ip 192.168.2.0 255.255.255.0 192.168.0.0 255.255.255.0
!
!
!
!
```

九、 共同思考

1. 为什么要手工配置密钥？
2. MAP 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

crypto ipsec transform-set

要定义一个 ipsec 变换集合——安全协议和算法的一个可行组合，使用 crypto ipsec transform-set 全局配置命令。要删除一个变换集合，可以使用这条命令的 no 格式。

```
crypto ipsec transform-set transform-set-name
no crypto ipsec transform-set transform-set-name
```

参数

参数	参数说明
transform-set-name	指定要创建（或修改）的变换集合的名称。

缺省

无

命令模式

全局配置态。执行此命令将进入加密变换配置态。

使用说明

变换集合是安全协议、算法以及将用于受 IPSec 保护的通信的其它设置的组合。

可以配置多个变换集合，然后在加密映射表中指定这些变换集合中的一个或多个。在加密映射表中定义的变换集合用于协商 IPSec 安全联盟，以保护匹配加密映射表设定的访问列表的那些报文。在协商过程中，双方寻找一个在双方都有的相同变换集合。当找到了一个这样的变换集合时，此集合将被选中，并作为双方 IPSec 安全联盟的一部分被运用到受保护的通信上。

如果不是使用 IKE 来建立安全联盟，那么必须指定唯一一个变换集合。此集合无须进行协商。

只有使用此命令对变换集合进行了定义后，此变换集合才能被设置在加密映射表中。

可使用 transform-type 命令来具体配置变换类型。

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
```