第5章

IPSec VPN

CHAPTER 5


视频讲解

5.1　IPSec 概述

IPSec 是一种开放标准的框架结构,特定的通信方之间在 IP 层通过加密和数据摘要(hash)等手段,来保证数据包在 Internet 网上传输时的私密性(confidentiality)、完整性(data integrity)和真实性(origin authentication),它工作在 IP 层,载荷协议和承载协议都是 IP。

5.1.1　保证数据的私密性

IPSec 通过数据加密来保证数据的私密性,数据加密过程就是对原来为明文的文件和数据按某种算法进行处理,使其成一段不可读的代码,而解密过程是利用密钥将密文转换成明文的过程。

1. 对称加密算法保证私密性

数据的私密性由加密算法提供,在明文与密文间相互转换的过程中,除了加密算法外,还需要一个加解密的参数,称为密钥。密码学中常用的加密技术有对称加密算法和非对称加密算法。如图 5-1 所示,是一个利用对称加密算法对文件加密和解密的过程,明文首先通过对称加密算法和密钥进行加密,得到密文,然后接收端收到加密密文之后使用对称加密算法和加密密钥解密,得到明文。对称加密算法加解密文件的速度非常快,但由于加密和解密密钥是同一个,存在密钥传输安全性问题,如果密钥在传输的过程中被截获,攻击者可以使用该密钥解密被加密的文件。

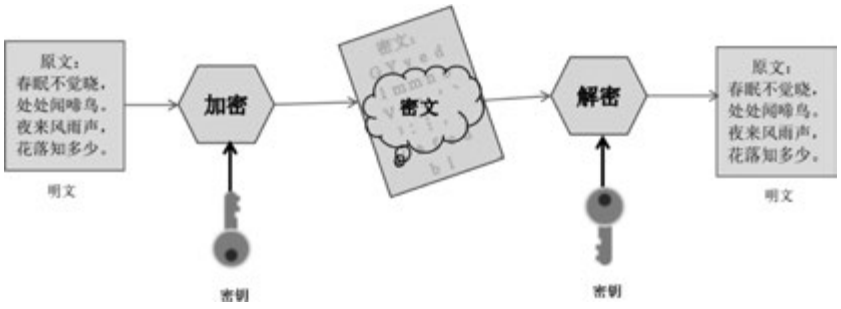

图 5-1　对称算法加解密文件

如图 5-2 所示,左边用户想发送一个文件给右边用户,使用加密算法 E 和密钥 K,将明文 M 加密生成密文 C,然后将密文 C 和密钥 K 通过网络传输,密文 C 和密钥 K 被互联网中的黑客截获,黑客直接将截获的密文 C 通过密钥 K 解密,从而获得文件原文信息。

2. 非对称加密算法保证数据私密性

非对称密钥算法也称公开密钥算法,此算法为加密用户分配一个密钥对,一个称为公钥(完全对外公开的密钥)、另一个称为私钥(私人拥有的密钥),这两个密钥不能互逆推算。用其中一个密钥加密的数据,只有另外一个密钥才能解密。发送方发送数据时,用接收方的公钥对数据进行加密,接收方收到加密数据后,只有拥有私钥的用户使用私

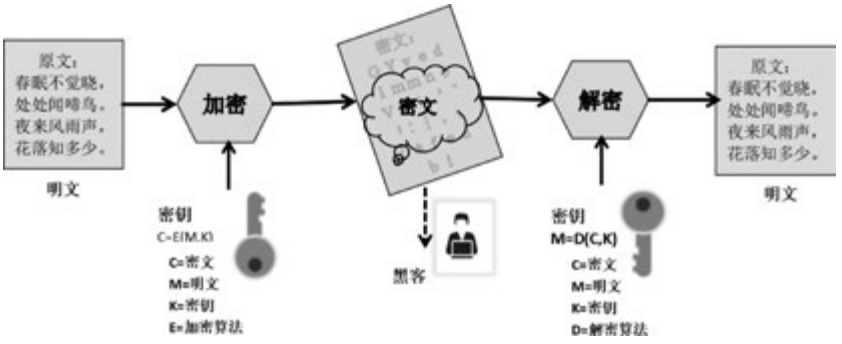

图 5-2　对称加密算法密钥安全问题

钥才能进行解密。

如图 5-3 所示，用户 B 拥有一个密钥对，用户 B 将其中一个密钥私下保存（私钥），另一个密钥公开发布（公钥），此时 A 想单独发送信息给 B，A 使用 B 的公钥加密要发送的信息，然后发给 B，B 收到加密的信息，用自己的私钥解密信息，得到原文，注意没有 B 私钥的用户是无法解开用 B 用户的公钥加密后的信息的。很多时候，对称加密算法和非对称加密算法结合使用，由于对称加密算法加密速度快，通常使用对称加密算法加密待传输的文件，然后使用非对称加密算法传输对称加密算法需要私密传输的密钥，从而保证了密钥数据传输的私密性。

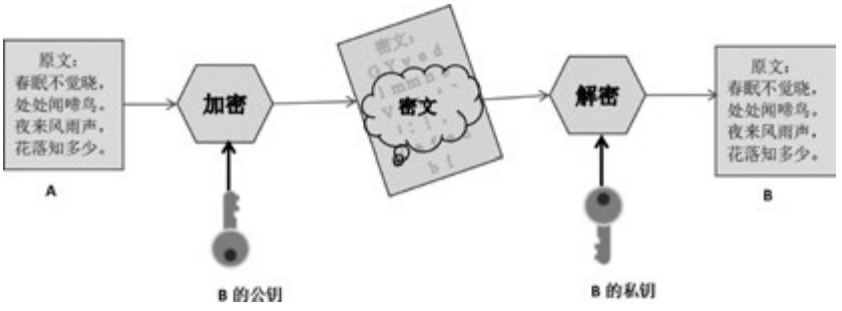

图 5-3　非对称加密算法

5.1.2　保证数据的完整性

数据的完整性是指数据没有被非法篡改，在互联网上传输的数据时常会有被截获修改的可能性，为了保证数据的安全性需要校验数据的完整性。常用的数据完整性校验方法有 HASH 算法，也称为摘要算法，采用 HASH 函数对不同长度的数据进行 HASH 运算会得到固定长度的结果，这个数据称为原数据的摘要，也称为消息验证码（Message Authentication Code，MAC），摘要结果具有单向性、不可逆性，不同的内容其摘要结果是不同的。

如图 5-4 所示，发送方将公司财务报告销售额和利润值进行了 HASH，生成摘要 52952769691，然后发送方将公司财务报告在网上发送，如果黑客截获了报文，修改了报文内容，将报文原来的利润值减少了 10 000，接收方收到报文后，采用同样的摘要算法 HASH 计算出的摘要变成了 43162898451 与传送的摘要（原摘要为 52952769691）不一致，这时就知道原文被修改了。

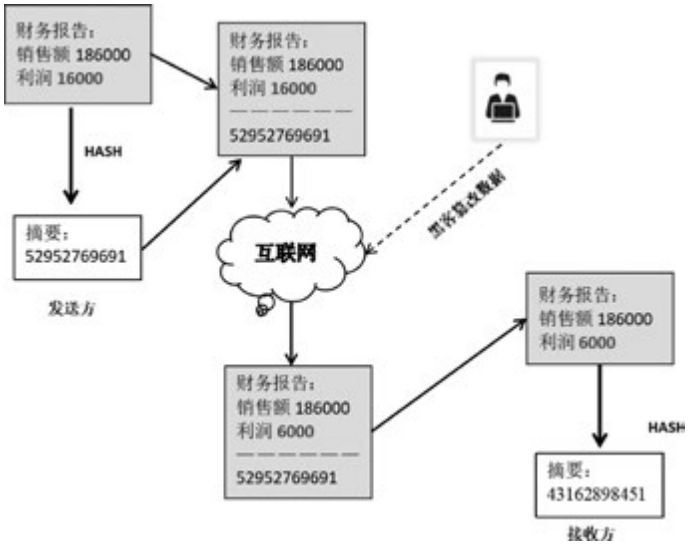

图 5-4 HASH 摘要保证数据完整性

如果黑客篡改原始数据的同时,将截获的摘要信息修改为篡改后的数据产生的摘要,这样接收方就不能发现数据被篡改了。因此,对原始单输入的 HASH 算法改进为 HMAC 算法。

HMAC(Hash Message Authentication Code)需要收发双方共享一个 MAC 密钥,计算摘要时,除了数据摘要外,还需要提供 MAC 密钥,即 MAC 密钥与原数据一起进行 HASH,但是传送的内容不包括 MAC 密钥。如果黑客截获了报文,修改了报文内容,伪造了摘要,由于不知道 MAC 密钥,黑客无法造出正确的摘要,接收方重新计算摘要时,一定会发现报文的 HMAC 与传送的 HMAC 码不一致。

如图 5-5 所示,发送方在发送公司财务报告之前,将 MAC 密钥与公司财务报告一起 HASH,生成 HMAC 摘要值 52952769691,此时在网上只发送公司财务报告和 HMAC 摘要值,MAC 密钥不发送,只私密地告诉接收方,当公司财务报告和 HMAC 摘要值被黑客截

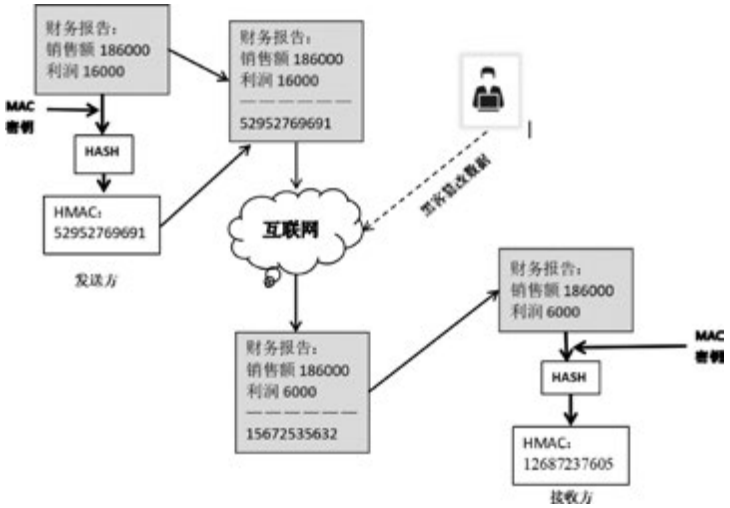

图 5-5 MAC 密钥 HASH

获并修改了利润(减少了 10 000),生成新的 HASH 摘要值为 15672535632,当接收方收到被修改的信息后,接收方将公司财务报告和发送方约定的 MAC 密钥进行 HASH,发现生成的 HMAC 值为 12687237605 与黑客篡改后传输过来的 HASH 值(15672535632)不一致,接收方就知道公司财务报告被劫持并修改了。

5.1.3　保证数据的真实性

真实性是指数据确实由特定的对端发出,通过身份认证可以保证数据的真实性,常用的身份认证方式有数字签名和数字证书。

1. 数字签名

数字签名是指使密码算法对要发送的数据进行加密,生成一段信息,附着在原文上一起发送,这段信息类似于现实中的签名或印章,接收方对其进行验证,判断原文的真伪。

如图 5-6 所示,发送方 A 要向接收方 B 发送报文,为了确认发送方 A 的身份,采用了数字签名的方式,其数字签名过程如下。

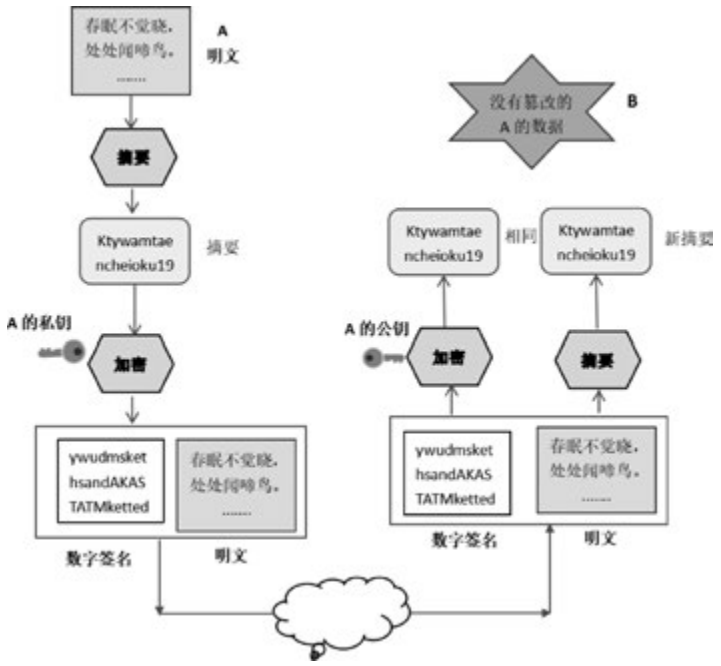

图 5-6　数字签名身份认证

(1) 发送方 A 首先将待发送的原始数据进行 HASH,得到该原始数据的 MAC 值。

(2) 发送方 A 将自己的私钥对 MAC 值进行加密,得到一个密文串 K。

(3) 将该密文串附在原始报文后面一起送给 B。

(4) 接收方 B 收到该报文后,也对原始报文内容进行 HASH,得到一个 MAC 值。

(5) B 用 A 的公钥对密文串 K 进行解密,比较解密后的值与运算后的 MAC 值是否相等,相等则说明报文是合法的发送方 A 发送的,且报文在传递过程中未被篡改。

2. 数字证书

数字证书相当于电子化的身份证明,它和身份证类似,证书中是一些帮助确定身份的信息资料。数字证书就是将公钥与身份绑定在一起,由一个可信的第三方对绑定后的数据进行签名,以证明数据的可靠性。

数字证书包含:发信人的公钥、发信人的姓名、证书颁发者的名称、证书的序列号、证书颁发者的数字签名和证书的有效期限等。

5.2 实践应用:配置 USG6000V 上的 IPSec VPN


视频讲解

5.2.1 Web 页面配置 IPSec VPN


视频讲解

已知公司总部局域网的主机要通过互联网实现与分公司局域网的主机通信,分公司与总部之间进行通信要保证数据的安全性,在总部和分部之间建立一个虚拟的专用网络通道,即 VPN 通道,其组网图如图 5-7 所示。根据组网图在 eNSP 模拟器中画出网络拓扑图,并通过云连接到物理机上,通过物理机的浏览器访问防火墙,并配置防火墙 A、防火墙 B 的 IPSec VPN 功能,如图 5-8 所示。

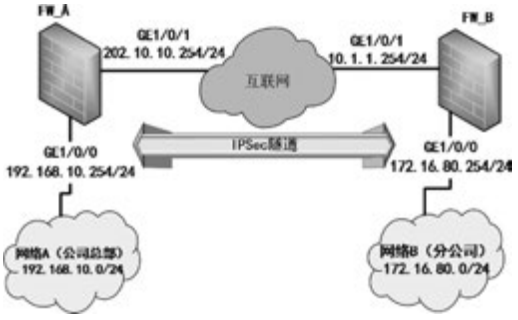

图 5-7 基于 IKE 的 IPSec 组网图

要通过 Web 页面访问防火墙 A 和防火墙 B,完成总公司和分公司 IPSec VPN 的配置,在命令模式下,登录防火墙 A 和防火墙 B,在两个防火墙的 GE0/0/0 口上开启 HTTPS 服务,并将防火墙 B 的 GE0/0/0 口的 IP 地址修改为 192.168.0.2/24,然后将两个防火墙的 GE0/0/0 口通过交换机连接到云上,如何配置云、修改接口 IP 地址和开启接口上的服务,请参考前面章节的配置过程,此处不再介绍。

1. 配置总公司 IPSec VPN

现在配置公司总部局域网防火墙 A 的 VPN 功能的过程如下。

(1) 配置接口信息。

按照网络拓扑图,配置接口 g0/0/0 为默认 IP 地址,g1/0/0 口 IP 地址为 192.168.10.254/24,g1/0/1 接口 IP 地址为 202.10.10.254/24;将接口 g0/0/0 和 g1/0/0 加入 trust 区域,g1/0/1 加入 untrust 区域;并在接口 g0/0/0 上开启 HTTPs 服务,g1/0/0 和 g1/0/1 接

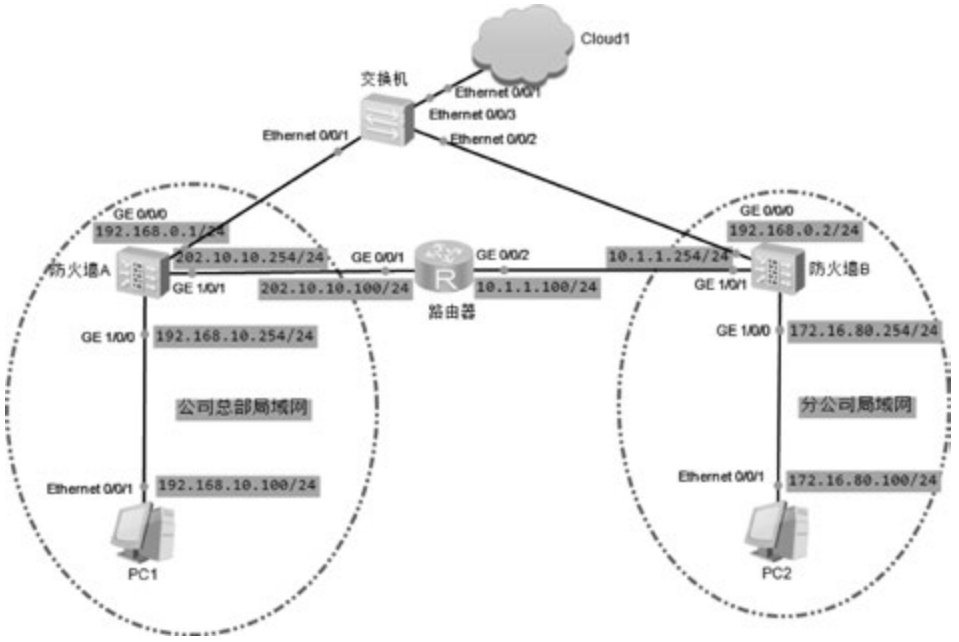

图 5-8　IPSec VPN 网络拓扑图

口上开启 ping 服务，如图 5-9 所示。

接口名称	安全区域	IP地址	连接类型	VL
GE0/0/0(GE0/MGMT)	trust(default)	192.168.0.1 ---	静态IP(IPv4 静态IP(IPv6	
GE1/0/0	trust(public)	192.168.10.254 ---	静态IP(IPv4 静态IP(IPv6	
GE1/0/1	untrust(public)	202.10.10.254 ---	静态IP(IPv4 静态IP(IPv6	

图 5-9　配置接口信息

（2）配置静态路由。

数据包通过防火墙 A(IPSec VPN)能够转发出去，需要创建一条缺省路由，为了保障从总公司内网出去的数据包能够到达分公司内网，还需要添加一条到分公司内网的路由信息，如图 5-10 所示。

静态路由列表

新建　删除

源虚拟路由器	目的地址/掩码	目的虚拟路由器	下一跳	优先级	出接口	绑定IP-Link...
public	0.0.0.0/0.0.0.0	public	202.10.10.100	60	GE1/0/1	
public	172.16.80.0/255.255.2...	public	202.10.10.100	60	GE1/0/1	

图 5-10　配置静态路由

（3）配置安全策略。

为了使得数据包能够在防火墙上转发，需要配置 4 条安全策略，如图 5-11 所示，配置允许数据包在防火墙 A 与防火墙 B 间互访的安全策略，即防火墙 A 的 local 区域与防火墙 B 的 untrust 区域互访；允许公司总部内网与分公司内网用户互访，此处需要说明的是，对于公司总部内网，防火墙 A 是信任的，被定义为 trust 区域，但是对于分公司过来的数据包，防

火墙 A 认为是不安全的,故不信任,将其定义为 untrust 区域,此处 untrust 区域有相同的,所以需要特指源 IP 地址和目的 IP 地址。

名称	源安全...	目的安...	源地址/地区	目的地址/地区	服务	应用	时间段	动作
local_untrust	local	untrust	202.10.10.0/24	10.1.1.0/24	any	any	any	允许
untrust_local	untrust	local	10.1.1.0/24	202.10.10.0/24	any	any	any	允许
trust_untrust	trust	untrust	192.168.10.0/24	172.16.80.0/24	any	any	any	允许
untrust_trust	untrust	trust	172.16.80.0/24	192.168.10.0/24	any	any	any	允许

图 5-11 配置安全策略

(4) 配置 IPSec。

在 IPSec 策略配置窗口中,场景选择"点到点",策略名为 new_0,本端接口使用 GE1/0/1,认证方式选择"预共享密钥",输入与对端一致的认证方式和密钥,本端和对端 ID 都选择 IP 地址。新建待加密的数据流,源地址为 192.168.10.0/24,目的地址为 172.16.80.0/24,源端口、目的端口、源协议任意,动作选择"加密",如图 5-12 所示。

图 5-12 配置 IPSec

2. 配置分公司 IPSec VPN

现在配置分公司局域网防火墙 B 的 VPN 功能的过程如下。

(1) 配置接口信息。

按照网络拓扑图,配置接口 GE0/0/0 的 IP 地址为 192.168.0.2/24,GE1/0/0 接口的 IP 地址为 172.16.80.254/24,GE1/0/1 接口的 IP 地址为 10.1.1.254/24;将接口 GE0/0/0 和 GE1/0/0 加入 trust 区域,GE1/0/1 加入 untrust 区域;并在接口 GE0/0/0 上开启 HTTPs

服务，GE1/0/0 和 GE1/0/1 接口上开启 ping 服务，如图 5-13 所示。

图 5-13　配置接口信息

（2）配置静态路由。

数据包通过防火墙 B（IPSec VPN）能够转发出去，同防火墙 A 一样，需要创建一条缺省路由，为了保障从分公司内网出去的数据包能够到达总公司内网，还需要添加一条到总公司内网的路由信息，如图 5-14 所示。

图 5-14　配置静态路由

（3）配置安全策略。

此处防火墙 B 安全策略的配置与防火墙 A 安全策略的配置相似，只是在 IP 地址上有区别，如图 5-15 所示。

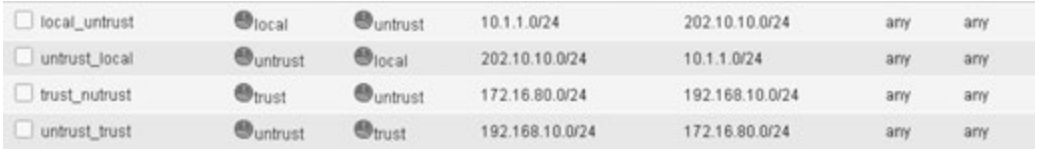

图 5-15　配置安全策略

（4）配置 IPSec。

在 IPSec 策略窗口中，场景选择“点到点”，策略命名为 new_1，本端接口选择 GE1/0/1，认证方式选择“预共享密钥”，密钥同防火墙 A 预共享密钥，本端和对端 ID 都选择 IP 地址，新建一条待加密的数据流，源地址为 172.16.80.0/24，目的地址为 192.168.10.0/24，协议、源端口、目的端口为任意，动作为“加密”，如图 5-16 所示。

3. 配置路由器 IP 地址

配置路由器 GE0/0/0 接口的 IP 地址为 202.10.10.100/24，GE0/0/1 接口的 IP 地址为 10.1.1.100/24，命令如图 5-17 所示。

4. 配置 PC1、PC2 主机的 IP 地址

配置 PC1、PC2 主机的 IP 地址如图 5-18 所示。

5. 测试

通过 PC1 ping PC2 和 PC2 ping PC1 来检查网络连通性，同时查看 IPSec 监控列表，观

图 5-16　配置 IPSec

图 5-17　配置路由器 IP 地址

图 5-18　配置 PC1、PC2 主机的 IP 地址

察 IPSec VPN 上的数据包流向，如图 5-19 所示。

5.2.2　命令模式配置 IPSec VPN

按照图 5-8 的 IPSec VPN 网络拓扑图，使用命令完成 IPSec VPN 的配置，在防火墙 A、防火墙 B 上的配置过程如下。

图 5-19　IPSec 监控列表

1. 配置防火墙 A

(1) 配置防火墙(GE1/0/0、GE1/0/1)接口 IP 地址，并开启 ping 服务：

```
[USG6000V1]interface GigabitEthernet1/0/0
[USG6000V1-GigabitEthernet1/0/0]ip address 192.168.10.254 255.255.255.0
[USG6000V1-GigabitEthernet1/0/0]service-manage ping permit
[USG6000V1-GigabitEthernet1/0/0]quit
[USG6000V1]interface GigabitEthernet1/0/1
[USG6000V1-GigabitEthernet1/0/1]ip address 202.10.10.254 255.255.255.0
[USG6000V1-GigabitEthernet1/0/1]service-manage ping permit
[USG6000V1-GigabitEthernet1/0/1]quit
```

(2) 将接口 g1/0/0 加入 trust 区，将 g1/0/1 加入 untrust 区：

```
[USG6000V1]firewall zone trust
[USG6000V1-zone-trust]add interface GigabitEthernet1/0/0
[USG6000V1-zone-trust]quit
[USG6000V1]firewall zone untrust
[USG6000V1-zone-untrust]add interface GigabitEthernet1/0/1
[USG6000V1-zone-untrust]quit
```

(3) 添加两条静态路由：

```
[USG6000V1]ip route-static 0.0.0.0 0 g1/0/1 202.10.10.100
[USG6000V1]ip route-static 172.16.80.0 24 g1/0/1 202.10.10.100
```

(4) 创建 local-untrust 区和 trust-untrust 区允许互访的安全策略：

```
[USG6000V1]security-policy
[USG6000V1-policy-security]rule name local-untrust
[USG6000V1-policy-security-rule-local-untrust]source-zone local
[USG6000V1-policy-security-rule-local-untrust]destination-zone untrust
[USG6000V1-policy-security-rule-local-untrust]source-address 202.10.10.0 24
```

```
[USG6000V1-policy-security-rule-local-untrust]destination-address 10.1.1.0 24
[USG6000V1-policy-security-rule-local-untrust]action permit
[USG6000V1-policy-security-rule-local-untrust]quit
[USG6000V1-policy-security]rule name untrust-local
[USG6000V1-policy-security-rule-untrust-local]source-zone untrust
[USG6000V1-policy-security-rule-untrust-local]destination-zone local
[USG6000V1-policy-security-rule-untrust-local]source-address 10.1.1.0 24
[USG6000V1-policy-security-rule-untrust-local]destination-address
202.10.10.0 24
[USG6000V1-policy-security-rule-untrust-local]action permit
[USG6000V1-policy-security-rule-untrust-local]quit
[USG6000V1-policy-security]rule name trust-untrust
[USG6000V1-policy-security-rule-trust-untrust]source-zone trust
[USG6000V1-policy-security-rule-trust-untrust]destination-zone untrust
[USG6000V1-policy-security-rule-trust-untrust]source-address
192.168.10.0 24 [USG6000V1-policy-security-rule-trust-untrust]destination-address
172.16.80.0 24
[USG6000V1-policy-security-rule-trust-untrust]action permit
[USG6000V1-policy-security-rule-trust-untrust]quit
[USG6000V1-policy-security]rule name untrust-trust
[USG6000V1-policy-security-rule-untrust-trust]source-zone untrust
[USG6000V1-policy-security-rule-untrust-trust]destination-zone trust
[USG6000V1-policy-security-rule-untrust-trust]source-address 172.16.80.0 24
[USG6000V1-policy-security-rule-untrust-trust]destination-address
192.168.10.0 24
[USG6000V1-policy-security-rule-untrust-trust]action permit
[USG6000V1-policy-security-rule-untrust-trust]quit
```

(5) 配置 IPSec 策略。

① 创建加密数据流：

```
[USG6000V1]acl number 3000
[USG6000V1-acl-adv-3000]rule 5 permit ip source 192.168.10.0 0.0.0.255 destination
172.16.80.0 0.0.0.255
```

② 创建 IKE 安全提议：

```
[USG6000V1]ike proposal 10
[USG6000V1-ike-proposal-10]encryption-algorithm aes-256
[USG6000V1-ike-proposal-10]authentication-algorithm sha2-256
[USG6000V1-ike-proposal-10]authentication-method pre-share
[USG6000V1-ike-proposal-10]integrity-algorithm hmac-sha2-256
[USG6000V1-ike-proposal-10]prf hmac-sha2-256
[USG6000V1-ike-proposal-10]display this
2023-06-26 08:50:41.740
#
ike proposal 10
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
return
```

```
[USG6000V1 - ike - proposal - 10]quit
```

③ 创建 IKE 协商连接密钥：

```
[USG6000V1]ike peer a
[USG6000V1 - ike - peer - a]pre - shared - key Admin@123
[USG6000V1 - ike - peer - a]exchange - mode auto
[USG6000V1 - ike - peer - a]ike - proposal 10
[USG6000V1 - ike - peer - a]remote - id - type ip
[USG6000V1 - ike - peer - a]remote - id 10.1.1.254
[USG6000V1 - ike - peer - a]local - id 202.10.10.254
[USG6000V1 - ike - peer - a]remote - address 10.1.1.254
[USG6000V1 - ike - peer - a]display this
2023 - 06 - 26 08:56:51.690
#
ike peer a
exchange - mode auto
pre - shared - key %^%#]b%s)A～X$G05}>S;{,/,u4Xz2x.!x,BG%>ZXBDr<%^%#
ike - proposal 10
remote - id - type ip
remote - id 10.1.1.254
local - id 202.10.10.254
remote - address 10.1.1.254
#
return
[USG6000V1 - ike - peer - a]quit
```

④ 创建 IPSec 安全提议：

```
[USG6000V1]ipsec proposal 10
[USG6000V1 - ipsec - proposal - 10]esp authentication - algorithm sha2 - 256
[USG6000V1 - ipsec - proposal - 10]esp encryption - algorithm aes - 256
[USG6000V1 - ipsec - proposal - 10]display this
2023 - 06 - 26 09:00:01.250
#
ipsec proposal 10
esp authentication - algorithm sha2 - 256
esp encryption - algorithm aes - 256
#
return
[USG6000V1 - ipsec - proposal - 10]quit
```

⑤ 创建 IPSec 安全策略：

```
[USG6000V1]ipsec policy new1 10 isakmp
Info: The ISAKMP policy sequence number should be smaller than the template poli
cy sequence number in the policy group. Otherwise, the ISAKMP policy does not ta
ke effect.
[USG6000V1 - ipsec - policy - isakmp - new1 - 10]security acl 3000
[USG6000V1 - ipsec - policy - isakmp - new1 - 10]ike - peer a
[USG6000V1 - ipsec - policy - isakmp - new1 - 10]proposal 10
[USG6000V1 - ipsec - policy - isakmp - new1 - 10]display this
2023 - 06 - 26 09:01:55.920
#
ipsec policy new1 10 isakmp
 ike - peer a
```

```
 proposal 10
#
return
[USG6000V1 - ipsec - policy - isakmp - new1 - 10]quit
```

⑥ 将 IPSec 安全策略绑定到 g1/0/1 接口：

```
[USG6000V1]interface g1/0/1
[USG6000V1 - GigabitEthernet1/0/1]ip address 202.10.10.254 24
[USG6000V1 - GigabitEthernet1/0/1]service - manage ping permit
[USG6000V1 - GigabitEthernet1/0/1]ipsec policy new1
[USG6000V1 - GigabitEthernet1/0/1]display this
2023 - 06 - 26 09:47:01.590
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 202.10.10.254 255.255.255.0
 service - manage ping permit
 ipsec policy new1
#
return
[USG6000V1 - GigabitEthernet1/0/1]quit
```

2. 配置防火墙 B

(1) 配置接口 g1/0/0、g1/0/1 的 IP 地址并开启 ping 服务：

```
[USG6000V1]interface g1/0/0
[USG6000V1 - GigabitEthernet1/0/0]ip address 172.16.80.254 24
[USG6000V1 - GigabitEthernet1/0/0]service - manage ping permit
[USG6000V1 - GigabitEthernet1/0/0]display this
2023 - 06 - 26 09:07:19.050
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 172.16.80.254 255.255.255.0
 service - manage ping permit
#
return
[USG6000V1 - GigabitEthernet1/0/0]quit
[USG6000V1]interface g1/0/1
[USG6000V1 - GigabitEthernet1/0/1]ip address 10.1.1.254 24
[USG6000V1 - GigabitEthernet1/0/1]service - manage ping permit
[USG6000V1 - GigabitEthernet1/0/1]display this
2023 - 06 - 26 09:08:51.880
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 10.1.1.254 255.255.255.0
 service - manage ping permit
#
return
[USG6000V1 - GigabitEthernet1/0/1]quit
```

(2) 将 g1/0/0 口加入 trust 区,g1/0/1 口加入 untrust 区:

```
[USG6000V1]firewall zone trust
[USG6000V1 - zone - trust]add interface g1/0/0
[USG6000V1 - zone - trust]display this
2023 - 06 - 26 09:15:16.440
#
firewall zone trust
  set priority 85
add interface GigabitEthernet0/0/0
  add interface GigabitEthernet1/0/0
#
return
[USG6000V1 - zone - trust]quit
[USG6000V1]firewall zone untrust
[USG6000V1 - zone - untrust]add interface g1/0/1
[USG6000V1 - zone - untrust]display this
2023 - 06 - 26 09:13:27.470
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet1/0/1
#
return
[USG6000V1 - zone - untrust]quit
```

(3) 添加两条静态路由:

```
[USG6000V1]ip route - static 0.0.0.0 0 g1/0/1 10.1.1.100
[USG6000V1]ip route - static 192.168.10.0 24 g1/0/1 10.1.1.100
```

(4) 配置 local-untrust 区、trust-untrust 区允许放行的安全策略:

```
[USG6000V1]security - policy
[USG6000V1 - policy - security]rule name local - untrust
[USG6000V1 - policy - security - rule - local - untrust]source - zone local
[USG6000V1 - policy - security - rule - local - untrust]destination - zone untrust
[USG6000V1 - policy - security - rule - local - untrust]source - address 10.1.1.0 24
[USG6000V1 - policy - security - rule - local - untrust]destination - address 202.10.10.0 24
[USG6000V1 - policy - security - rule - local - untrust]action permit
[USG6000V1 - policy - security - rule - local - untrust]quit
[USG6000V1 - policy - security]rule name untrust - local
[USG6000V1 - policy - security - rule - untrust - local]source - zone untrust
[USG6000V1 - policy - security - rule - untrust - local]destination - zone local
[USG6000V1 - policy - security - rule - untrust - local]source - address
202.10.10.0 24
[USG6000V1 - policy - security - rule - untrust - local]destination - address 10.1.1.0 24
[USG6000V1 - policy - security - rule - untrust - local]action permit
[USG6000V1 - policy - security - rule - untrust - local]quit

[USG6000V1 - policy - security]rule name trust - untrust
[USG6000V1 - policy - security - rule - trust - untrust]source - zone trust
[USG6000V1 - policy - security - rule - trust - untrust]destination - zone untrust
[USG6000V1 - policy - security - rule - trust - untrust]source - address
172.16.80.0 24
[USG6000V1 - policy - security - rule - trust - untrust]destination - address 192.168.10.0 24
```

```
[USG6000V1 - policy - security - rule - trust - untrust]action permit
[USG6000V1 - policy - security - rule - trust - untrust]quit

[USG6000V1 - policy - security]rule name untrust - trust
[USG6000V1 - policy - security - rule - untrust - trust]source - zone untrust
[USG6000V1 - policy - security - rule - untrust - trust]destination - zone trust
[USG6000V1 - policy - security - rule - untrust - trust]source - address
192.168.10.0 24
[USG6000V1 - policy - security - rule - untrust - trust]destination - address
172.16.80.0 24
[USG6000V1 - policy - security - rule - untrust - trust]action permit
[USG6000V1 - policy - security - rule - untrust - trust]quit
[USG6000V1 - policy - security]display this
2023 - 06 - 26 09:21:53.340
#
security - policy
rule name tr - dmz
source - zone trust
destination - zone dmz
destination - zone untrust
source - address 172.16.10.0 mask 255.255.255.0
action permit
rule name local - untrust
source - zone local
destination - zone untrust
source - address 10.1.1.0 mask 255.255.255.0
destination - address 202.10.10.0 mask 255.255.255.0
action permit
rule name untrust - local
source - zone untrust
destination - zone local
source - address 202.10.10.0 mask 255.255.255.0
destination - address 10.1.1.0 mask 255.255.255.0
action permit
rule name trust - untrust
source - zone trust
destination - zone untrust
source - address 172.16.80.0 mask 255.255.255.0
destination - address 192.168.10.0 mask 255.255.255.0
action permit
rule name untrust - trust
source - zone untrust
destination - zone trust
source - address 192.168.10.0 mask 255.255.255.0
destination - address 172.16.80.0 mask 255.255.255.0
action permit
#
return
[USG6000V1 - policy - security]quit
```

(5) 配置 IPSec 策略。

① 加密需要私密发送的数据流:

```
[USG6000V1]acl number 3000
```

```
[USG6000V1 - acl - adv - 3000]rule permit ip source 172.16.80.0 0.0.0.255 destination
192.168.10.0 0.0.0.255
[USG6000V1 - acl - adv - 3000]display this
2023 - 06 - 26 09:28:33.560
#
acl number 3000
rule 5 permit ip source 172.16.80.0 0.0.0.255 destination 192.168.10.0 0.0.0.25
5
#
return
[USG6000V1 - acl - adv - 3000]quit
```

② 配置 IKE 安全提议：

```
[USG6000V1]ike proposal 10
[USG6000V1 - ike - proposal - 10]encryption - algorithm aes - 256
[USG6000V1 - ike - proposal - 10]authentication - algorithm sha2 - 256
[USG6000V1 - ike - proposal - 10]authentication - method pre - share
[USG6000V1 - ike - proposal - 10]integrity - algorithm hmac - sha2 - 256
[USG6000V1 - ike - proposal - 10]prf hmac - sha2 - 256
[USG6000V1 - ike - proposal - 10]display this
2023 - 06 - 26 09:32:14.940
#
ike proposal 10
encryption - algorithm aes - 256
dh group14
authentication - algorithm sha2 - 256
authentication - method pre - share
integrity - algorithm hmac - sha2 - 256
prf hmac - sha2 - 256
#
return
[USG6000V1 - ike - proposal - 10]quit
```

③ IPSec 通信协商连接密钥：

```
[USG6000V1]ike peer b
[USG6000V1 - ike - peer - b]pre - shared - key Admin@123
[USG6000V1 - ike - peer - b]exchange - mode auto
[USG6000V1 - ike - peer - b]ike - proposal 10
[USG6000V1 - ike - peer - b]remote - id - type ip
[USG6000V1 - ike - peer - b]remote - id 202.10.10.10.254
[USG6000V1 - ike - peer - b]display this
2023 - 06 - 26 09:33:56.240
#
ike peer b
exchange - mode auto
pre - shared - key %^%#I0 + <.VWqY1_De\ = z * d`5A $ hK3W3K[CaQXf)E;RJ5 %^%#
ike - proposal 10
remote - id - type ip
remote - id 202.10.10.10.254
#
return
[USG6000V1 - ike - peer - b]quit
```

④ IPSec 安全提议：

```
[USG6000V1]ipsec proposal 10
[USG6000V1-ipsec-proposal-10]esp authentication-algorithm sha2-256
[USG6000V1-ipsec-proposal-10]esp encryption-algorithm aes-256
[USG6000V1-ipsec-proposal-10]display this
2023-06-26 09:36:37.020
#
ipsec proposal 10
esp authentication-algorithm sha2-256
esp encryption-algorithm aes-256
#
return
[USG6000V1-ipsec-proposal-10]quit
```

⑤ IPSec 策略：

```
[USG6000V1]ipsec policy new1 10 isakmp
Info: The ISAKMP policy sequence number should be smaller than the template poli
cy sequence number in the policy group. Otherwise, the ISAKMP policy does not ta
ke effect.
[USG6000V1-ipsec-policy-isakmp-new1-10]security acl 3000
[USG6000V1-ipsec-policy-isakmp-new1-10]ike-peer b
Info: No remote address configured in IKE peer.
[USG6000V1-ipsec-policy-isakmp-new1-10]proposal 10
[USG6000V1-ipsec-policy-isakmp-new1-10]display this
2023-06-26 09:38:39.540
#
ipsec policy new1 10 isakmp
security acl 3000
ike-peer b
proposal 10
#
return
[USG6000V1-ipsec-policy-isakmp-new1-10]quit
```

⑥ 接口 g1/0/1 绑定 IPSecVPN：

```
[USG6000V1]interface g1/0/1
[USG6000V1-GigabitEthernet1/0/1]ip address 10.1.1.254 24
[USG6000V1-GigabitEthernet1/0/1]ipsec policy new1
[USG6000V1-GigabitEthernet1/0/1]display this
2023-06-26 09:40:41.010
#
interface GigabitEthernet1/0/1
undo shutdown
ip address 10.1.1.254 255.255.255.0
service-manage ping permit
ipsec policy new1
#
return
[USG6000V1-GigabitEthernet1/0/1]quit
```

3. 配置路由器 g0/0/1 和 g0/0/2 接口 IP 地址

```
<Huawei>sys
[Huawei]sys AR1
[AR1]interface g0/0/1
[AR1-GigabitEthernet0/0/1] ip address 202.10.10.100 24
[AR1-GigabitEthernet0/0/1]quit
[AR1]interface g0/0/2
[AR1-GigabitEthernet0/0/2] ip address 10.1.1.100 24
```

4. 配置 PC1、PC2 主机 IP 地址

配置主机 PC1、PC2 的 IP 地址如图 5-18 所示。

5. 测试

PC1 ping PC2 和 PC2 ping PC1，如图 5-20 所示。

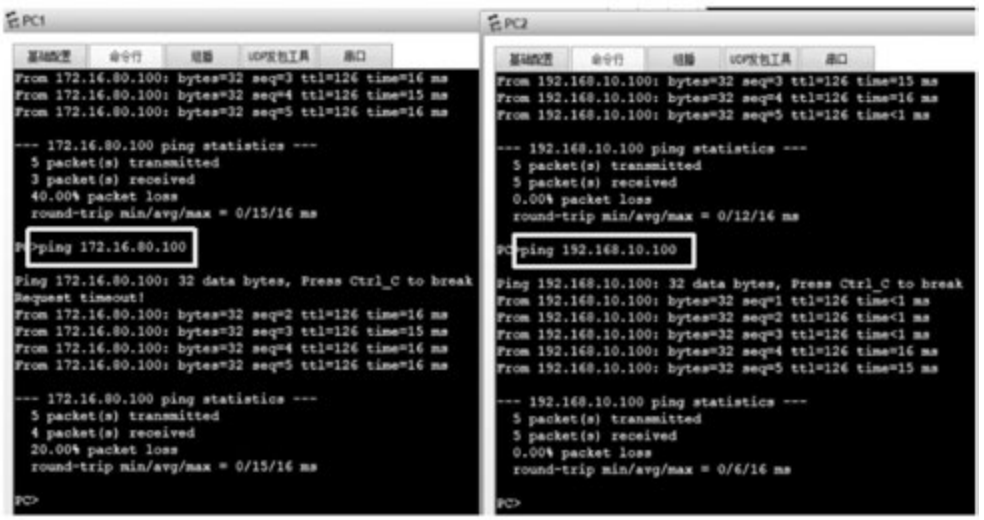

图 5-20　ping 测试

6. 在防火墙上查看会话和 IPSec 状态

(1) 查看防火墙 A。

① 查看会话表：

```
[USG6000V1]display firewall session table
2023-06-30 07:12:48.080
Current Total Sessions:1
esp VPN:public --> public 10.1.1.254:0 --> 202.10.10.254:0
```

② 查看 IPSec 状态：

```
[USG6000V1]display ipsec statistics
2023-06-30 07:15:18.990
IPSec statistics information:
```

```
Number of IPSec tunnels:1
Number of standby IPSec tunnels:0
the security packet statistics:
input/output security packets:26/29
input/output security bytes:1560/1740
input/output dropped security packets:0/0
the encrypt packet statistics:
send chip:29, recv chip:29, send err:0
local cpu:29, other cpu:0, recv other cpu:0
intact packet:29, first slice:0, after slice:
```

(2) 查看防火墙 B。

① 查看会话表:

```
[USG6000V1]dis firewall session table
2023-06-30 07:13:54.710
Current Total Sessions:1
esp VPN: public --> public 202.10.10.254:0 --> 10.1.1.254:0
```

② 查看 IPSec 状态:

```
[USG6000V1]dis ipsec statistics
2023-06-30 07:17:11.760
IPSec statistics information:
Number of IPSec tunnels:1
Number of standby IPSec tunnels:0
the security packet statistics:
input/output security packets:29/26
input/output security bytes:1740/1560
input/output dropped security packets:0/0
the encrypt packet statistics:
send chip: 26, recv chip: 26, send err:0
local cpu: 26, other cpu: 0, recv other cpu:0
intact packet: 26, first slice: 0, after slice:0
the decrypt packet statistics:
```

在线测试

习题

一、选择题

1. 以下说法正确的是(　　)。
   A. 数据的完整性是指数据没有被非法篡改
   B. 使用对称加密算法可以对用户进行身份验证
   C. 对称加密算法安全性比非对称加密算法要高
   D. HASH 函数可以加密数据,保障数据的安全性
2. 以下关于载荷协议的说法,正确的是(　　)。
   A. IP、ATM 属于载荷协议
   B. 载荷协议又称为被封装的协议,如 PPP、SLIP 等
   C. 用于隧道的建立、维护和断开的协议称为载荷协议

D. L2TP、SSL 属于载荷协议

3. 以下属于身份认证的是(　　)。

A. 对称加密　　B. 非对称加密

C. 数字证书　　D. HASH 校验

二、填空题

1. VPN 虚拟网络具有_____、_____、身份认证和访问控制等功能。
2. VPN 技术主要有_____技术、_____技术和高层 VPN 技术。
3. 一个隧道协议包含从高层到低层,分别是_____、隧道协议和_____。
4. IPSec 工作在_____层。
5. 对称加密算法有_____个密钥。
6. 非对称加密算法有_____和_____密钥对。

三、简答题

1. 简述载荷协议、承载协议和隧道协议的含义。
2. 举例描述数字签名过程。

四、实践题

试参照图 5-8 相关参数设计其网络拓扑图,并在 eNSP 模拟器中用图形界面模式完成 IPSec VPN 的配置。实现步骤提示如下。

(1) 借助 AI(如 DeepSeek)进行深度搜索,在搜索框中输入“在以下参数中配置 USG6000V 的 IPSec VPN,并画出网络拓扑图:防火墙 FW_A(公网地址为 202.10.10.254/24)和防火墙 FW_B(公网地址为 10.1.1.254/24)通过 Internet 相连,两者公网路由可达。防火墙 FW_A 与内网主机处于 192.168.10.0/24 网段,防火墙 FW_B 与内网主机处于 172.16.80.0/24 网段。试在防火墙 FW_A 和防火墙 FW_B 之间搭建 IPSec VPN ,实现数据的安全通信”。

(2) 根据 AI 搜索结果和图 5-8,在 eNSP 中画出 USG6000V 的网络拓扑图,完成配置和测试。