Software Engineering and Applications 软件工程与应用, 2020, 9(4), 278-287
Published Online August 2020 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2020.94031

Hans汉斯

A Site to Site VPN Network Based on IPSec Protocol

Jincheng Huang, Yaheng Zhang, Huihui Xiang, Ming Tian

Yancheng Institute of Technology, Yancheng Jiangsu
Email: huangjincheng@163.com

Received: Jul. 22nd, 2020; accepted: Aug. 5th, 2020; published: Aug. 12th, 2020

Abstract

In order to solve the network security problem between the head office and the branch office, this paper proposes a site to site VPN network based on IPSec protocol. IPSec protocol plays an important role in network security which is used in devices such as firewalls and routers. The virtual machine and simulator is used to realize the topology design and operation of the network; the process of the VPN network configuration is explained in detail.

Keywords

Network Security, VPN Network, IPSec Protocol, Virtual Machine

基于IPSec协议的点对点VPN网络

黄金城，张雅恒，项慧慧，田　明

盐城工学院，江苏　盐城
Email: huangjincheng@163.com

收稿日期：2020年7月22日；录用日期：2020年8月5日；发布日期：2020年8月12日

摘　要

为了解决总公司与分公司的网络安全问题，论文提出了一种基于IPSec协议的点对点VPN网络。IPSec协议在网络安全领域发挥着重要的作用，被应用在诸如防火墙及路由器等设备当中。在本文中运用虚拟机与模拟器实现网络的拓扑设计与运行，并对整个网络的配置进行了详细说明。

关键词

网络安全，VPN网络，IPSec协议，虚拟机

文章引用: 黄金城, 张雅恒, 项慧慧, 田明. 基于 IPSec 协议的点对点 VPN 网络[J]. 软件工程与应用, 2020, 9(4): 278-287. DOI: 10.12677/sea.2020.94031

1. 引言

随着全球化的快速推进，地理位置相隔的企业需要进行私密数据的通信。然而公网的环境十分复杂，并且不安全，一旦被第三方获取私密数据将对企业造成无法挽回的损失。VPN 作为能够在公共网络中建立专用数据通道的一项技术，得到了广泛的使用。企业运用 VPN 技术，使得地理位置不再是传输内网数据的阻碍，因为可以在公网中建立一条隧道，达到直连的效果。隧道技术，就是数据报封装技术，将一种网络协议封装进另一种网络协议中然后再进行传输，隧道技术往往包含着加密、身份认证及访问控制等一系列的措施来保证数据的安全性[1]。隧道技术是推动 VPN 技术发展的关键，也是保证数据安全性的关键。为了保证隧道的安全性，通常会使用隧道协议。常见的隧道协议有 GRE、LT2P、IPSec 等。IPSec 作为最广泛、最经典的技术方案，一直备受关注[2] [3]。IPSec 是用于保障网络安全性的协议族，其内容是在密码学的基础上发展而来的。通过 AH、ESP、IKE 等一系列协议来保证报文的完整性和安全性，对私密数据的传输提供了安全性保障[4]。

为了有效保障公司网络安全，使公司总部免受来自外部公网的攻击，也为了公司总部与分布之间建立安全的网络连接，本文提出了一种基于 IPSec 协议的点对点 VPN 网络。

2. 关键技术

2.1. 隧道技术

由于公用网络的环境十分复杂，并且安全性得不到保证。企业之间通过公网直接传输私密数据十分危险，可在公用网络中架设一条“隧道”来保证数据的安全性[5]。数据包在通过隧道与离开隧道的这段网络中，外界无法查看数据包的具体内容，从而达到数据包加密的目的。隧道除了有加密这个功能，还有模拟隧道两端直连的效果。通过封装技术，在数据包的私有目标地址前封装公有网关地址，使这个数据包能够在公网上进行传输。当这个数据包传到对端的公网网关时，网关就会将这个数据包的公网地址解封装，读取真正的私有地址的数据包，然后将数据包传输给目标网络。

2.2. IPSec 协议

IPSec 作为常用的 VPN 加密协议，为分组在网络层的安全传输提供保障。在网络层为分组形成保密字段与鉴别字段给予助力。IPSec 的工作方式有两种，众所周知，一种是隧道方式，另一种则是运输方式[6]。隧道方式与运输方式在数据加密上有着很大的区别，运输方式是在运输层的有效数据前加上 IPSec 的头部和尾部，然后再加上 IP 的首地址。隧道方式是在网络层数据包的全部内容前加上 IPSec 的头部和尾部，然后再将这个 IP 数据包与一个新的 IP 首部连接在一起，形成新的数据包，这个首部地址往往是隧道的虚拟地址。当使用隧道方式时，这时候分组像通过一条隧道一样。AH 协议是 IPSec 曾经常用的协议，该协议的功能是对发送方的身份进行识别，除此之外，还能对发送方的数据是否完整进行验证，鉴别首部协议的具体内容和插入位置，由于 AH 不提供保密性，所以 IPSec 后来又定义了一个类似的协议 ESP，ESP 提高发送方的鉴别、完整性和保密性[7]。

2.3. DMVPN

大量实践证明，基于 VPN 的安全架构对于现代分布式基础设计的建设是非常有效的。由于网络需求

的不断变化，通过介质将敏感数据在互联网上进行传输时难以保证安全性，DMVPN (Dynamic Multipoint VPN)动态多点 VPN 能够提高传统星型网络架构的扩展性，通过 IPSec 等动态功能特性对信息进行安全传输，可以降低网络延迟，提高带宽利用率[8]。可扩展性从本质上来说能够帮助网络实现扩展能力，更好地发挥网络基础设计的潜力，为多站点之间流量交换提供更小的延迟和更优的性能。

3. 网络的拓扑设计

3.1. 拓扑图

图 1 为运用虚拟机与模拟器实现的网络的拓扑图[9]。研究的目的是实现点对点的 VPN 网络的数据加密，所以在此模拟出了三个部分的网络，分别是分公司网络、总公司网络与运营商网络。在总公司与分公司的内网中使用 OSPF 协议实现网络互通，运营商使用 EIGRP 协议进行通信。为了对比加密效果，总公司只与一个分公司的通信中采用了 IPSec 加密方式。

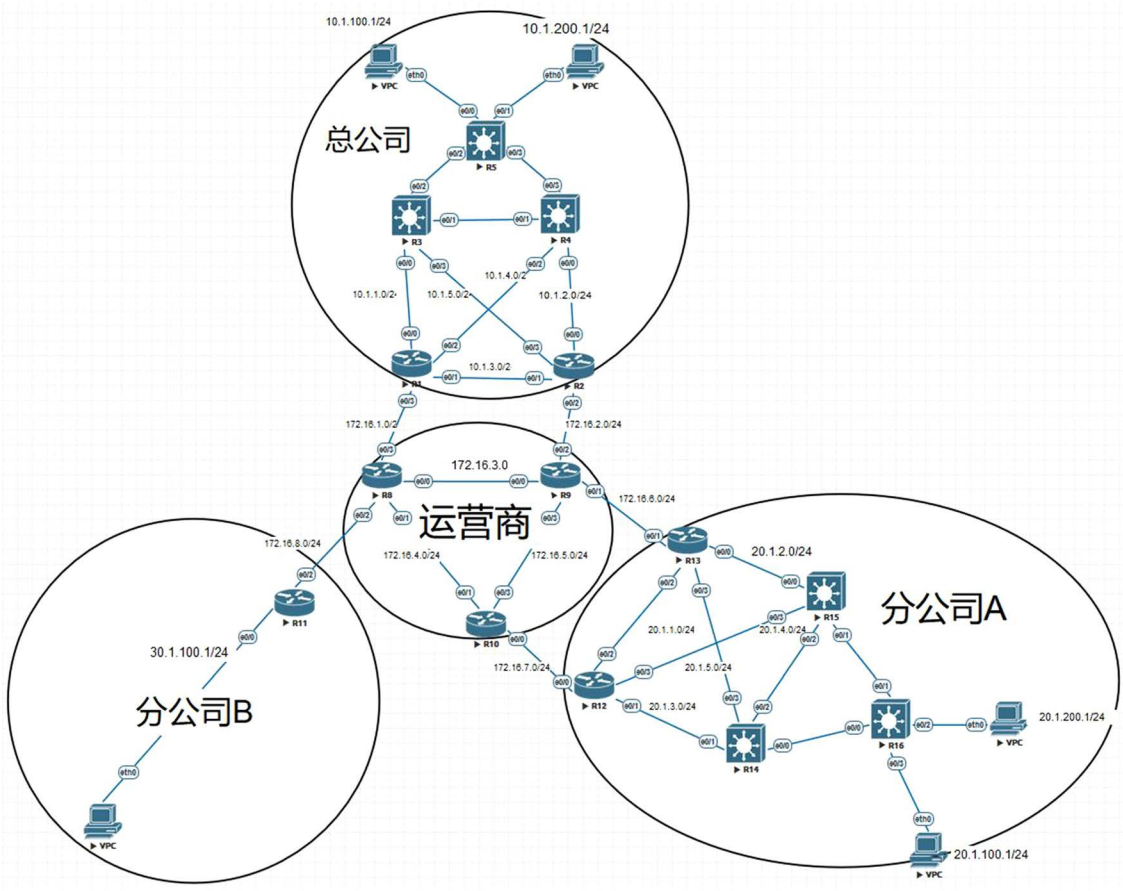

Figure 1. The topology of the network
图 1. 网络拓扑图

3.2. IP 规划

企业网内部采用的是普通的 TCP/IP 协议，总公司采用的网段是 10.1.0.0/16，运营商网段是 172.16.0.0/16，分公司 A 的网段是 20.1.0.0/16，分公司 B 的网段是 30.1.0.0/16，它们的掩码均为 24 位。主要设备之间的 IP 分配如表 1 和表 2 所示。

Table 1. The IP address and type of devices
表 1. 各个设备的 IP 地址与设备类型

设备名称	接口	IP 地址	描述
R1	E0/0	10.1.1.1/24	路由器
R1	E0/1	10.1.3.1/24	路由器
R2	E0/0	10.1.2.2/24	路由器
R2	E0/1	10.1.3.2/24	路由器
R3	E0/0	10.1.1.3/24	交换机
R3	E0/3	10.1.5.3/24	交换机
R4	E0/0	10.1.2.4/24	交换机
R4	E0/2	10.1.4.4/24	交换机
R8	E0/0	172.16.3.8/24	路由器
R8	E0/1	172.16.4.8/24	路由器
R9	E0/0	172.16.3.9/24	路由器
R9	E0/1	172.16.2.9/24	路由器
R10	E0/0	172.16.7.10/24	路由器
R10	E0/1	172.16.4.10/24	路由器
R11	E0/0	30.1.100.11/24	路由器
R12	E0/1	20.1.3.12/24	路由器
R12	E0/0	172.16.7.12/24	路由器
R13	E0/0	20.1.2.13/24	路由器
R13	E0/1	172.16.6.13/24	路由器
R14	E0/3	20.1.5.14/24	交换机
R14	E0/1	20.1.3.14/24	交换机
R15	E0/0	20.1.2.15/24	交换机
R15	E0/3	20.1.4.15/24	交换机
R8	E0/3	172.16.1.8/24	路由器
R9	E0/2	172.16.2.9/24	路由器
R10	E0/3	172.16.5.10/24	路由器
PC1	E0/0	10.1.100.1/24	PC
PC2	E0/0	10.1.200.1/24	PC
PC3	E0/0	20.1.100.1/24	PC
PC4	E0/0	20.1.200.1/24	PC
PC5	E0/0	30.1.100.1/24	PC

Table 2. IP address assignment of VLAN
表 2. VLAN IP 地址分配

VLAN 号	网段 IP	设备名称	描述
10	10.1.1.0/24	R3	用于连接 R1
20	10.1.5.0/24	R3	用于连接 R2
100	10.1.100.0/24	R3	用于虚拟网关
200	10.1.200.0/24	R4	用于虚拟网关

4. 路由器与交换机的配置

4.1. 接口参数配置

无论是路由器还是 PC 机，想要在网络上通信的前提是自身必须拥有 IP 地址，这个 IP 地址可以使固定的 IP 地址，由工作人员配置。也可以是 DHCP 动态获得 IP 地址，不失一般性，本拓扑的所有 IP 地址都是手动配置，如下所示：

```
Router(config)#int e0/0                                    //进入接口
Router(config-if)#no sh                                    //开启接口
Router(config-if)#ip address 10.1.1.1 255.255.255.0    //配置 ip 地址
Router(config-if)#exit
Router(config)#int e0/1
Router(config-if)#no sh
Router(config-if)#ip address 10.1.3.1 255.255.255.0
Router(config-if)#exi
```

4.2. 封装 trunk 和划分 VLAN

对于每一个交换机而言想要进行数据的传输都需要进行 VLAN 的划分和 trunk 的封装，其配置如下所示：

```
Switch(config)#int e0/1
Switch(config-if)# switchport trunk encapsulation dot1q
                                                    //将接口封装成 IEEE 802.1Q
Switch(config-if)# switchport mode trunk      //将接口变为 trunk  模式
Switch(config-if)# switchport nonegotiate     //本接口不发送协商信息
Switch(config-if)#exi
Switch(config)#int e0/0
Switch(config-if)# switchport access vlan 10   //将 e0/0 接口划入 VLAN10 下
Switch(config-if)# switchport mode access     //将接口变为接入模式
Switch(config-if)#exi
```

4.3. NAT 配置

对于每一个企业来说，它的内部网络地址是不可能出现在公网上的，常常需要用到 NAT 技术，将内部网络地址转换成一个公网的地址，这样才能够去外界实现通信。NAT 的主要原理是用 ACL 访问控制链表来抓取内部网段，再将内部网段转换成一个公网地址。配置如下：

```
Router(config)#int e0/0
Router(config-if)#ip nat inside            //进入接口后打上接口为 nat 内部的标记
Router(config-if)#int e0/3
Router(config-if)#ip nat outside          //进入接口后打上接口为 nat 外部的标记
Router(config-if)#exi
Router(config)#access-list 1 permit 10.1.0.0 0.0.255.255
                                          //用 ACL 来抓取内部网段
```

Router(config)#ip nat inside source list 1 interface Ethernet0/3 overload
//将这条内部网段用 nat 外部接口的地址(公网地址)来覆盖

4.4. 路由协议的配置

在网络中，路由分为两种：静态路由和动态路由。静态路由不会自动更新，需要工作人员手动配置路由条目，相对复杂。但是，由于静态路由相对于动态路由很稳定，适用于路由条目较少的情况，常常被用在银行等对稳定性需求高的机构。动态路由是基于路由协议的路由，这类路由在配置完协议后可以自动更新，无需工作人员进行操作，但是稳定性不如静态路由。在 IGP 路由协议中，RIP 由于不适用于较大规模的网络而逐渐淘汰，而 EIGRP 作为思科专有路由协议，只能在思科的设备上配置，也没有得到很好的应用。OSPF 协议作为各大厂商的设备广泛使用的协议受到了人们的青睐。本研究中，公司内网采用的就是 OSPF 协议，拓扑中的公网采用 EIGRP 协议来实现网络互通。其各自的配置如下：

Router(config)#router ospf 1
//进入 ospf 协议，ospf 的进程号为 1
Router(config-router)# router-id 1.1.1.1 //建立邻居，唯一标识 OSPF 区域的路由器
Router(config-router)# network 10.1.1.1 0.0.0.0 area 0
//将接口地址宣告进 OSPF 协议中，区域号为 0
Router(config-router)# network 10.1.3.1 0.0.0.0 area 0
Router(config-router)# network 10.1.4.1 0.0.0.0 area 0
Router(config-router)# exit
Router(config)#router eigrp 1 //进入 EIGRP 协议，进程号为 1
Router(config-router)# network 172.16.1.8 0.0.0.0 //宣告地址进 EIGRP (反掩码)协议
Router(config-router)# network 172.16.3.8 0.0.0.0
Router(config-router)# network 172.16.4.8 0.0.0.0
Router(config-router)# network 172.16.8.8 0.0.0.0：
Router(config-router)# exit

4.5. VPN 的配置

VPN 技术，就是运用公网来假设专线的技术。在本拓扑中的 R2 与 R15 采用 GRE 隧道技术来实现 VPN 技术。其具体配置如下：

Router(config)#interface Tunnel0 //创建一条隧道，虚拟直连链路，两端的编号可不同
Router(config-if)# ip address 192.168.2.1 255.255.255.0
//为该隧道配置地址，由于虚拟直连链路，所以两端的地址要保证在同一网段
Router(config-if)# tunnel source Ethernet0/2
//指定隧道的源地址，通常为本路由器的公网地址
Router(config-if)# tunnel destination 172.16.6.13
//隧道的终点地址，通常为对端路由器的公网地址
Router(config-if)#exi

4.6. DMVPN 的配置

DMVPN 又称为动态多点 VPN。相较于普通 VPN 来言，在增加新的分支站点时不用添加新的配置，

分支站点无需再建立 VPN 就能通信等好处。从某种意义上来说，DMVPN 是升级版的点对点 VPN。本拓扑中的 R1、R11、R12 采用 DMVPN 进行通信。其具体配置如下：

在中心站点 HUB 端：

```
Router(config)#interface Tunnel 0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no ip redirects              //关闭重定向功能
Router(config-if)# ip nhrp network-id 100   //标识下一跳解析协议的进程号
Router(config-if)# ip nhrp redirect
Router(config-if)# tunnel source Ethernet0/3
Router(config-if)# tunnel mode gre multipoint     //将隧道的模式定义为 GRE，并且允许多点接入
Router(config-if)#exi
```

在分支站点 SPOKE 端：

```
Router(config)#interface Tunnel0
Router(config-if)# ip address 192.168.1.3 255.255.255.0
                                        //配置隧道的 IP 地址，要保证与中心站点在同一网段
Router(config-if)# no ip redirects
Router(config-if)# ip nhrp map 192.168.1.1 172.16.1.1     //下一跳解析协议
Router(config-if)# ip nhrp map multicast 172.16.1.1       //NHRP 映射广播到公用网络接口
Router(config-if)# ip nhrp network-id 100          //标识解析协议，必须与 HUB 端保持一样
Router(config-if)# ip nhrp nhs 192.168.1.1         //配置隧道的下一跳地址
Router(config-if)# tunnel source Ethernet0/0
Router(config-if)# tunnel mode gre multipoint
```

4.7. IPSEC 的配置

在本拓扑中的 R1 与 R11 和 R12 的 DMVPN 采用了 IPSec 数据加密，保证数据通信的安全性，在 R2 与 R13 没有数据加密。目的是用 wireshark 抓包时比较二者数据包的区别。IPSec 的配置如下：

```
Router(config)#crypto isakmp policy 10   //设置主要 IKE 加密，加密配置的优先级
Router(config-isakmp)# encr aes       //运用对称加密 aes
Router(config-isakmp)# hash md5      //哈希算法
Router(config-isakmp)# authentication pre-share //共享认证
Router(config-isakmp)# group 2    //霍夫曼算法组 2
Router(config-isakmp)# lifetime 10800      //生存期为 10800s
Router(config-isakmp)#crypto isakmp key ycit address 0.0.0.0    //设置 DMVPN 的调用密码
Router(config)#crypto IPSec transform-set AAA ah-md5-hmac esp-aes
          //进行双重加密，对数据的传输进行摘要加密，防止篡改，加密方式的名字将为 AAA
Router(cfg-crypto-trans)# mode tunnel          //将模式改为隧道模式
Router(cfg-crypto-trans)#crypto IPSec profile DMVPN    //将 IKE 加密的文件名命名为 DMVPN
Router(config)#interface Tunnel0
Router(config-if)# tunnel protection IPSec profile DMVPN    //在隧道下调用 IKE 文件
```

5. Wireshark 抓包分析

本节将 Wireshark 与 EVE 仿真软件相关联，抓取通过 IPSec 加密的数据包与没有通过 IPSec 加密的 VPN 数据包，比较二者区别。

如图 2 所示。在网络拓扑中，R1 为 DMVPN 的中心站点和总公司内网的网关。R11 与 R12 作为 DMVPN 的分支站点和各自内网的网关。在 R1、R11 和 R12 上配置 IPSec 数据加密协议，并调用在隧道上。PC1 位于总公司的内网中，当 PC1 向分公司 B 中的 PC3 发送 PING 包时，经过了各自的网关。由于在 R1 和 R11 上配置了 NAT 网络地址转化，使得各自的源目 IP 地址是各自的公网网关地址。数据包被 ESP 封装，看不到原始的源地址与目的地址，这也就是在抓取的数据包中源地址为 172.16.1.1 和 172.16.8.11 的原因。在 Protocol 那一栏，看到有 ESP 协议字段，表明该数据包经过了 ESP 封装和加密。进入具体数据包查看，结果如图 3 所示，在 ESP 这一栏发现有一个 SPI 字段。SPI 字段是用来保证加密的正常进行。ESP 的序列号为 116，在上图的数据包中无法看到更多的相关信息，并且数据部分查看不了，表明数据包已经被 IPSec 加密了。

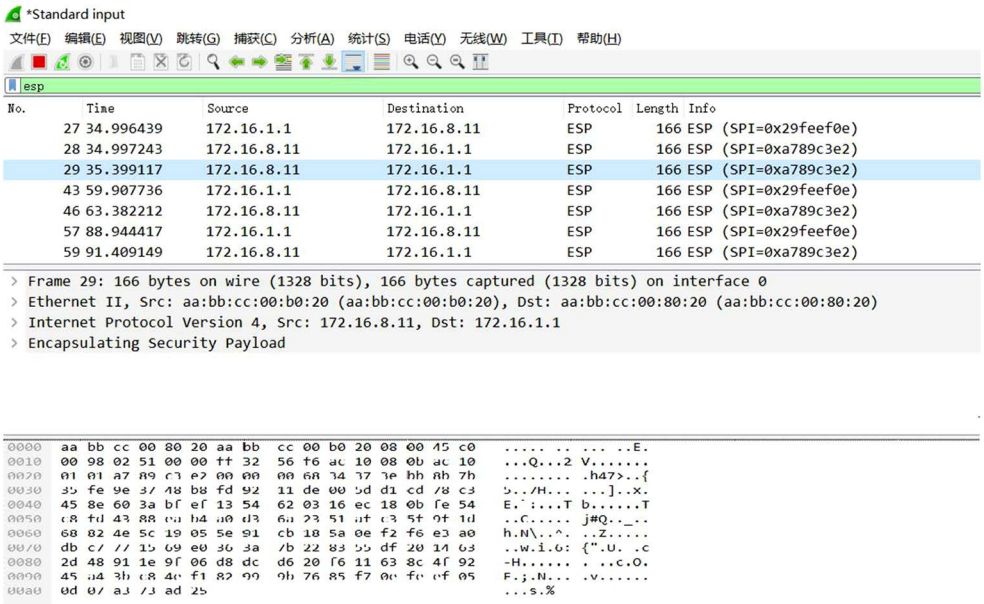

Figure 2. Packets of R1 and R11
图 2. 通过 R1 与 R11 的数据包

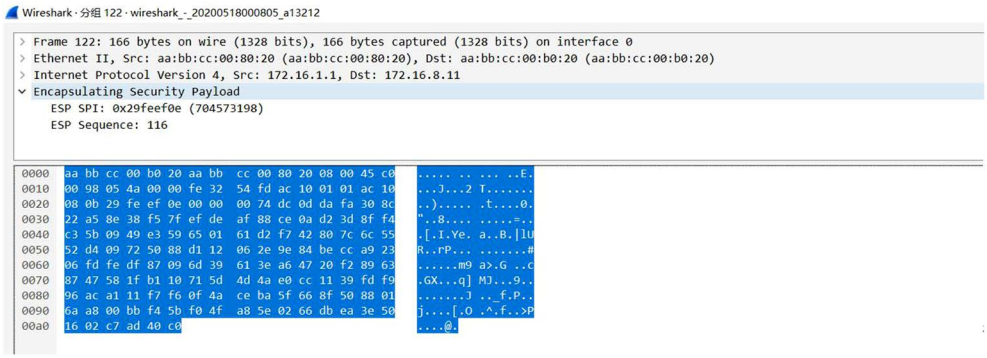

Figure 3. The contents of encrypted packets
图 3. 加密数据包的具体内容

R2 与 R13 建立的是普通的 GRE 隧道，并没有使用 IPSec 数据加密协议，单纯的虚拟出一条直连链路。当位于总公司的 PC1 去 PING 分公司 A 的 PC2 时，期间由于 OSPF 协议路由优先级的问题，数据包并不没有通过 R2 与 R13 建立的隧道，需要对 R2 隧道中的 OSPF 优先级进行增加，降低 OSPF 的 cost 值，使得 PING 包能够通过隧道。在图 4 中可以看到，数据包的源地址为 10.1.100.1，目的地址是 20.1.100.1。

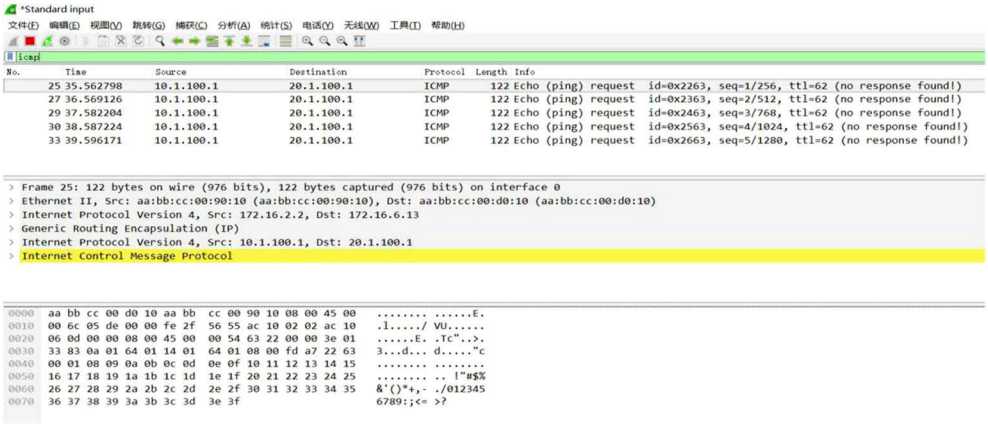

Figure 4. Packets of R2 and R13
图 4. 通过 R2 与 R13 的数据包

图 5 是将通过 R1 与 R11 的数据包展开的结果，可以看出显示的内容比 ESP 加密的数据包要多。能清楚的看到数据占了 56 比特，以及因特网控制信息协议的版本号等许多信息，说明了数据没有被 IPSec 加密。数据包没有 ESP 加密，能看到原始的 IP 地址。回包的协议是 ICMP，在过滤器中输入 ICMP 筛选数据包，在图片的中间位置可以看到两个源地址与目的地址。其中一对是 PC 实际的 IP 地址，另一对则是隧道的网关地址。

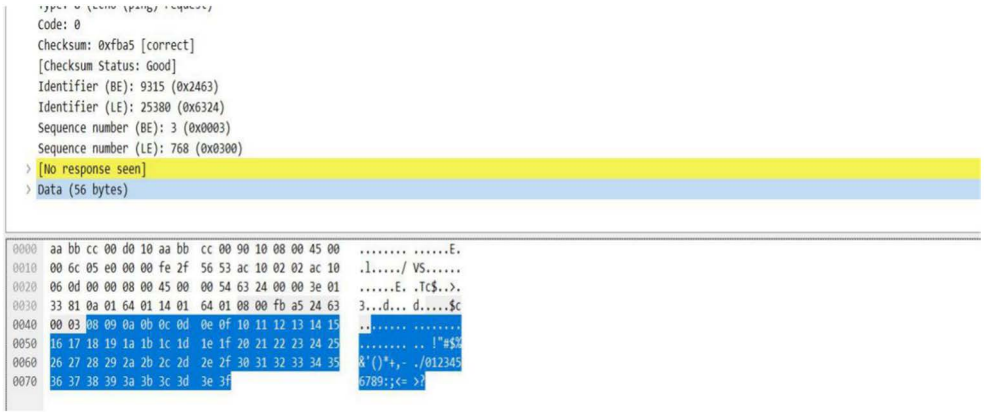

Figure 5. The contents of unencrypted packets
图 5. 未加密数据包的详细内容

通过对以上数据包的分析，发现经过 ESP 加密的数据包不仅隐藏了实际的 IP 地址，只能看到公网的 IP 地址。而且数据内容被加密了，达到了预期的效果。

6. 结语

本文提出了一种基于 IPSec 协议的点对点 VPN 网络，并用虚拟机与模拟器实现了网络的拓扑设计。文中对网络的各种配置进行了详细说明。通过 Wireshark 抓包分析，发现经过 ESP 加密的数据包只能看

到公网的 IP 地址，不仅隐藏了实际的 IP 地址，而且对数据内容也进行了加密。这种采用 IPSec 协议的 VPN 网络可有效避免来自公网的攻击，从而可以为公司总部与公司分部之间的数据传输建立安全保密的传输通道。

参考文献

[1] 林烈青. 无线局域网通信安全机制的研究[J]. 实验室研究与探索, 2012, 31(8): 257-260+284.

[2] 罗智勇, 多智华, 乔佩利. VPN 网络中 IPSec 安全策略的形式化描述[J]. 华中科技大学学报(自然科学版), 2011, 39(4): 65-68.

[3] 李湘锋, 赵有健, 全成斌. 对称密钥加密算法在 IPsec 协议中的应用[J]. 电子测量与仪器学报, 2014, 28(1): 75-83.

[4] 蔡思飞, 彭新光. 基于 VPN 的安全网关研究[J]. 太原理工大学学报, 2006(S1): 122-125.

[5] 付承彪, 田安红, 于龙, 马美. 高校网络在虚拟仿真器中的设计与实现[J]. 实验室研究与探索, 2018, 37(6): 91-95+128.

[6] 王铁松. 企业虚拟专网的应用与搭建[J]. 给水排水, 2014, 50(S1): 411-414.

[7] 王志刚, 石颖. 基于 IPSec 协议的 VPN 安全网关设计[J]. 计算机工程, 2009, 35(17): 146-148+151.

[8] 孙耀文, 杨屹, 高建亭. 浅谈 DMVPN 技术及其应用[J]. 信息通信, 2012(2): 144-146

[9] 陈建锐, 何增颖. 基于虚拟机的 VPN 实验环境构建[J]. 实验室研究与探索, 2010, 29(1): 59-61.