IPSec VPN实验的教学探究

周合军
常德职业技术学院

[摘　要]本文在基于教学实验的基础上，深入剖析了IPSec VPN的原理、配置和应用。教学和实验表明，封装是本质，隧道技术是关键，IPSec VPN两个工作阶段是重点，查验是不可缺少的环节。借助公共网络来搭建私人专用网络，采用IPSec VPN便捷、安全、省钱。

[关键词]IPSec VPN; 封装; 隧道
【DOI】10.12252/j.issn.2096-6261.2021.10.565

VPN，是Virtual Private Network的缩写，即虚拟专用网络。简单地说，虚拟专用网络我们可以理解成是虚拟出来的企业内部专线，可以跨越千山万水。利用互联网传送私有的、安全的数据，费用不大，这就是VPN美妙的地方。

1 VPN基本概念

VPN是一条穿过混乱的公用网络的安全、稳定的隧道，在这条安全隧道上可以进行安全、高效的数据传输。VPN连接两个终端系统，也可连接多个网络，VPN使用隧道和加密技术来组建的。VPN是一种WAN基础设施替代品，可用于替代或拓展现有的私有网络，在很多情况下，VPN有很多由于传统WAN连接的地方，如费用低廉、易于安装、能够迅速增加带宽等。VPN有三个方面的作用：数据加密，通过网络传输分组之前，发送方可对其进行加密，即使有人窃听，也无法读懂其中的信息；数据完整性，接收方可检查数据通过Internet传输的过程中是否被修改；身份合法性，接收方可验证发送方的身份，确保信息来自合法的地方。

理解VPN术语，这个是基础，VPN复杂的地方就是术语稍微多了点。封装：VPN核心技术，对要保护的数据进行封装。隧道：网络中的虚拟点到点连接，用于传输以一种协议封装的（如IP）另一种协议数据流（如加密后的密文）。加密/解密：加密技术是电子商务采取的主要安全保密措施，是最常用的安全保密手段，利用技术手段把重要的数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密），加密技术包括算法和密钥。加密系统：执行加密/解密、用户身份验证、散列算法和密钥交换的系统。加密系统可使用一种或多种方法，这取决于用户数据安全需求的策略。散列算法：一种单向函数和数据完整性技术，使用一种公式/算法来将不定长的消息和共享密钥转换为长度固定的比特串，消息/密钥和散列值通过网络从信源传输到目的地，在目的地，重新计算散列值，以核实消息和密钥通过网络传输时没有被修改。身份验证：用来验证实体或对象是谁或它的要求是什么的过程，确认信息的来源和完整性。授权（Authorization）：对于通过了身份验证的用户或进程，授予其访问计算机系统或网络连接资源的权利。密钥管理：一个管理和控制进程，用于生成、存储、保护、传输、加载、使用和销毁密钥，包括了从产生到消失的各方面。验证报头（Authentication Header）：AH是IPSec的一种重要的数据封装方式，它为IP数据包提供完整性、数据源身份验证以及抗重放攻击服务，但不提供数据的加密性保护。封装是VPN核心技术，就是对数据进行再包装。封装安全有效载荷（ESP）：一种安全协议，提供数据保密、数据完整性和保护服务，还可提供数据来源验证、重发服务。Internet秘钥交换（IKE，Internet Key Exchange Protocol）：一种IPSec体系结构中的一种主要协议，是一种混合协议，它创建在Oakley和ISAKMP协议之上，使用UDP端口500。ISAKMP：Internet安全联盟和密钥管理协议，只对认证和秘钥交换提出了结构框架，但没有具体定义，它是与密钥交换相对独立的。

2 两个IPSec实体之间的IKE协商分为两个阶段

2.1 IKE协商第一阶段（主模式）

第一阶段无论是使用main mode还是aggressive mode，目的都是产生ISAKMP/IKE SA，用ISAKMP/IKE SA为产生第二阶IPSec SA的ISAKMP消息交互过程进行保护。第1、2个ISAKMP报文：IPSec实体双方交互SA载荷，选择相同ISAKMP消息的保护策略及认证方式，双方必须达成一致，否则第一阶段协商失败。第3、4个ISAKMP报文：IPSec实体双方交互DH算法的公共值及密钥计算材料，从而双方计算出一系列相同的密钥 第5、6个ISAKMP报文：第5、6个报文使用第3、4个报文交互后产生的相关密钥进行验证及加密处理。IPSec实体双方分别对对方进行验证，若使用pre-share key的验证方式，即判断对方是否拥有与本地相同的pre-share key。双方的Key配置必须一致，否则第一阶段协商失败。

2.2 IKE协商第二阶段总结（快速模式）

第二阶段交互的ISAKMP消息均被第一阶段产生的ISAKMP/IKE SA保护。确定IPSec SA的保护策略，使用AH还是ESP、传输模式还是隧道模式、被保护的数据是什么等等，IPSec通信实体双方对于这些安全策略必须达成一致，否则IKE第二阶段协商将无法通过。为降低密钥之间的关联性，第二阶段采用PFS重新进行DH交换，并计算出新的共享密钥，从而计算出IPSec SA中用于加密和验证的密钥。第二阶段协商的目标就是产生真正用于保护IP数据的IPSec SA。

3 IPSec VPN工作过程和配置（见图1）

4 测试与验证

4.1 在运用VPN的路由器上查看show crypto isakmp sa是否协商成功。当状态IKE_IDLE为时，说明第一阶段协商成功。

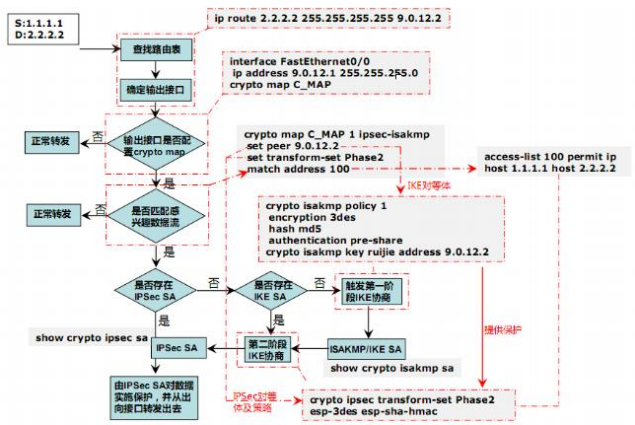

图1

4.2 在运用VPN的路由器上查看show crypto ipsec sa是否协商成功。可以查看到接口下加密图的名称、进行isakmp/ipsec协商时所用的ip地址、感兴趣流的源地址/目标地址、ipsec sa 入方向的spi、ipsec加密转换集形式、采用隧道模式还是传输模式、ipsec sa出方向的spi等。能看到：#pkts encaps：4，#pkts encrypt：4，#pkts digest 4//成功封装、加密、摘要报文个数、#pkts decaps：4，#pkts decrypt：4，#pkts verify 4//成功解封装，解密、检验报文个数，有数据通过IPSEC加密进行通信时，重复执行show crypto ipsec sa命令可以看到以上统计个数会不断增加。封装、解封装是关键的参数，如果这个数字是0或从没变化，说明IKE协商第二阶段还是有问题。这个地方容易出问题，也容易疏忽。只有看到了inbound spi和outbound spi才说明ipsec sa已经协商成功。不能简单说ping得通就行，关键看ipsec是否起作用。

5 易错点

5.1 路由可达。ipsec通道两端的路由器能够正常访问互联网、互相能ping通。有的学生以为配了ipsec就不考虑路由可达了，实际上路由可达是根本。Ipsec 中ESP，ip协议号50；AH的IP协议号是51，所以IP可达是前提，ipsec才能运行。

5.2 配置步骤清晰。如在路由器上配置静态IPSEC VPN隧道，配置ipsec感兴趣流→配置isakmp→配置预共享密钥→配置ipsec加密转换集→配置ipsec加密图→将加密图应用到接口，前后是有一定的关联性，随意改变顺序可能会出错。

5.3 走IPSEC VPN和NAT数据流各不相同。访问公网的数据流走nat出接口，访问远方公司私网走IPSEC VPN隧道。抓取数据不能把数据流范围扩大、也不能缩小，更不能抓错数据流。一点，就是要准确抓取数据流。

5.4 散列（HASH，也称作哈希）算法是确保消息的完整性，不是加密算法。哈希就是把任意长度的输入（又叫做预映射，pre-share），通过散列算法变换成固定长度的输出，是单向的。常用的散列算法有MD5、SHA-1两种，而加密算法有DES、3DES等，常常有学生弄混淆。

5.5 IPSEC VPN第一阶段（IKE）SA协商失败。需要检查是否已经在双方指定了正确的peer（对端peer的ip地址必须是对端配置了crypto map接口的IP地址，不可为loopback地址。）；双方是否能够互相ping通配置了crypto map接口的IP地址；隧道两端IKE安全提议配置是否一致；隧道两端预共享密钥配置是否一致等。

5.6 IPSEC VPN第二阶段（IPSEC）SA协商失败。需要检查IPSEC VPN第一阶段（IKE）SA是否已经建立成功；双方的transform-set配置是否一致；双方所配置的ipsec感兴趣流是否一致（如果中心为动态，则不需要手动配置ipsec感兴趣流）等。

5.7 IPSEC VPN一、二阶段SA协商成功，但感兴趣流通信异常。确认IPSEC VPN第一、二阶段SA是否已经正确建立；确认双方的感兴趣流配置是否一致；双方接口下配置的crypto map删除后，感兴趣流是否能够正常通信（如果无法正常通信，则请检查路由配置）；确认发往对端的感兴趣流，在本端路由表中的下一跳是否为已经配置了crypto map的接口（比如：感兴趣流为192.168.10.0 →

192.168.20.0，interface fastethernet 0/1配置了crypto map，那么在本地路由表中，去往192.168.2.0的下一跳出口则应该为fastethernet 0/1接口）。

6 反思

6.1晦涩的术语概念浅显生动。例如：隧道技术涉及了三种协议，支撑隧道协议的承载协议、网络隧道协议和隧道协议所承载的被承载协议，把这三种协议比作在隧道里穿行的汽车、长长的隧道、连绵的山脉，学生理解这三个协议的关系就轻松多了。

6.2 大多学生对英语不敢兴趣，但让学生记住关键词并不难。他们打起游戏来，英语脱口而出。Crypto是秘密、密码的意思，我会现场百度，听标准读音，现场读5遍、慢慢解释。每天记住2个计算机网络技术专业英语单词，化整为零、化难为易。关键词记住了，再理解的英文句子也不是难事了。

6.3 培养学生独立解决问题的能力。原理懂了，配置也记住了，未必能解决实验中出现的问题，碰到故障，让他自己分析（或老师和他一起分析）、一步一步拨开云雾，找到问题的真相，然后再解决。碰到问题是好事情，是检验学生学以致用的好机会。

参考文献

[1]华为技术有限公司编著.网络系统建设与运维：高级.北京：人民邮电出版社，2020.9

[2]梁广民，徐磊，谢晓广编著.思科网络实验室CCNP（路由技术）实验指南.北京：电子工业出版社，2019.3

作者简介：

周合军，1976.2.6，男，本科，高级工程师，研究方向：计算机网络技术。