**第11章**

**1.在PGP中，发送方执行签名、加密、压缩操作的顺序是什么？为什么要按这样的顺序进行？**

先签名，再压缩，最后加密。

如果是先压缩，再签名的话，验证签名时就需要对验证签名所得到的结果再进行解压缩，才能知道签名是否正确。

对明文先压缩，后加密能减少明文中的上下文关系，对攻击抵御能力更强。此外若先加密，后压缩，压缩的效果会很差。

**2.在密钥信任方面，X.509和PGP有什么不同？**

X.509 是密码学里数字证书的格式标准。X.509的信任是传递的关系，但PGP中的信任是不可传递的。

**3.PGP为什么要对加密后的报文进行Base64编码？并分析编码对传输性能的影响。**

base64 编码是一种可以将任何二进制数据都用 AZ、az、0~9、+、/ 同 64 个字符再加上 =(用于末尾填充) 来表示的格式。在兼容性方面，加密后的报文使用Base64编码将报文转换成ASCII字符串，主要考虑到很多文件系统只允许使用ASCII字符组成的报文。实际应用中，使用Base64编码转换后将导致消息大小增加33%（每3个字节的二进制数据映射成4个ASCIII字符）。由于加密前对消息进行了压缩，实际的性能下降幅度要小很多

**4.PGP是如何交换会话密码的？这种交换密钥方式与前面学过的那种协议类似？**

A用伪随机数生成器生成会话密钥，用B的公钥密码加密会话密钥并发送给B。

这种用公钥密码加密会话密钥，用对称密码加密消息，称为链式加密或数字信封，在SSL协议中也使用过。

**第13章**

**1、网络防火墙有哪几种常见体系结构？安全性最高的是哪种？**

防火墙体系结构一般有三种：

双穴主机或双宿主机结构 (Dual Homed Gateway)

屏蔽主机或主机过滤结构(Screened Host Gateway)

过滤子网或屏蔽子网结构(Screened Subnet)

安全性最高的是屏蔽子网结构.

**2、从采用的技术来分，网络防火墙主要有哪几种类型？**

包过滤技术防火墙，状态检测技术防火墙，应用网关防火墙防火墙，下一代防火墙

**3、随着云计算的广泛应用，企业网络的边界越来越模糊，对传统网络防火墙有什么影响？**

过去，企业自建“可信”内网，采购“可信”的终端设备，“可信”的员工通过“可信”设备连接“可信”的网络进行办公，自然是“安全可信”的。

但是现在，进入企业城墙的早已不再仅仅是“可信”设备，每个员工甚至除了智能手机之外，还会携带更多可以连接网络，并且未经过企业授权的“不可信”智能设备。每一台设备的每一次网络连接，都可能成为内部数据外泄或是外部攻击入侵的源头，就连无线路由器、智能摄像头等IoT设备，也会变成攻击者顺着网线爬进企业内部的“帮凶”。

基于“企业边界正在瓦解，基于边界的安全防护体系正在失效”这一大背景应运而生的“零信任安全”（Zero Trust）概念，可以说是当前网络安全界内最热门的话题之一，它最早由Forrester研究机构于2010年提出。

Forrester“零信任安全”将“永不信任，始终验证”作为其指导原则，由以下三个支柱构建：确保所有资源安全地访问，无论处在任何位置；应用最小权限策略，并严格执行访问控制；检查所有流量并记录。

换句话说，企业不再有受信任区域，所有用户最初都是“不受信任”的，即使是来自内网的流量也要被检查。

“人”用来访问系统以及连接网络的工具是什么？是设备。那么如果“可信”的人使用了“不可信”的设备该怎办？

所以，除了证明“人”的身份以外，设备也同样需要辨明“身份”，这就是“零信任安全”在“端”侧的验证。

比如很多员工会使用非企业采购的移动设备接入网络，包括笔记本电脑、手机、BYOD设备等，那么企业首先要能够准确识别哪些设备是“自己的”，哪些设备是“别人的”。

其次，对于任何准备接入的设备，制定“合规性”的策略——满足某些硬性条件，如升级新版本杀毒软件，或升级新系统补丁的的设备，才有“资格”接入网络。

**第14章**

**1、什么是VPN的隧道（封装）技术？**

隧道技术是指包括数据封装、传输和解包在内的全过程，是构建VPN的核心技术，叠加在IP主干网上运行。

1）通过加密和鉴别以确保安全

2）由VPN封装成IP包的形式

3）通过隧道在Internet上安全传输

4）离开隧道后，进行解封装，数据便不再被保护

**2.SSL VPN和IPSec VPN主要有哪些不同？哪些情况下适合使用SSL VPN？SSL VPN如何与IPSec VPN结合使用？**

SSL VPN与IPSec VPN的最大不同是无客户端，使用支持SSL的Web浏览器，就可以建立安全通道访问远程应用；SSL费用低，IPSec费用高；SSL适用于基于WEB的应用，IPSec适用于所有基于IP协议的服务。

以IPSec VPN作为远程接入和点对点连接方案，辅以SSL VPN作为远程访问Web服务的方案。

**第15章**

**1、有了防火墙，为什么还需要入侵检测？**

防火墙是根据规则对进出网络的信息进行过滤

本身问题：可能存在安全漏洞成为被攻击的对象

配置不当：起不到作用

网络边界：有缺口（如 Modem，无线）

不是万能：入侵教程、工具随处可见，攻击模式的多样性，并不能阻止所有攻击

内部攻击(Abuse)：并不是所有攻击均来自外部

综上，防火墙还存在有一定缺陷，所以需要入侵检测：通过从计算机系统或网络的关键点收集信息并进行分析，从中发现系统或网络中是否有违反安全策略的行为和被攻击的迹象作为防火墙的有效补充。

**2、与入侵检测相比，网络欺骗防御技术有什么优势？**

网络欺骗防御是一种体系化的防御方法，它将蜜罐、蜜网、混淆等欺骗技术同防火墙、入侵检测系统等传统防护机制有机结合起来，构建以欺骗为核心的网络安全防御体系

网络欺骗防御技术（蜜罐）的优势有使用简单，只是检测并记录；占用资源少；数据价值高，能分析攻击者的攻击行为。

**3、比较分析特征检测与异常检测方法的优缺点。**

特征检测是根据定义好的入侵模式，通过判断这些入侵模式是否出现来检测，是一个比较死的方法，也需要有经验的专家的参与。

异常检测是在众多样本中，通过统计的方法或机器学习来区分正常样本和异常样本。这种是很灵活的，检测的严密程度可以自己制定，当然也存在有一些误报率。

对于基于标识的检测技术来说，首先要定义违背安全策略的事件的特征，如网络数据包的某些头信息。检测主要判别这类特征是否在所收集到的数据中出现。此方法非常类似杀毒软件。

而基于异常的检测技术则是先定义一组系统“正常”情况的数值，如CPU利用率、内存利用率、文件校验和等（这类数据可以人为定义，也可以通过观察系统、并用统计的办法得出），然后将系统运行时的数值与所定义的“正常”情况比较，得出是否有被攻击的迹象。这种检测方式的核心在于如何定义所谓的“正常”情况。