网络环境下的信息安全实验

一、实验名称：

网络环境下的信息安全实验

二、实验目的：

（1）掌握防火墙的工作原理，采用WinRouter代理服务器进行防火墙配置

（2）掌握IPSec 协议的工作原理及xp系统下的配置方法

三、简述问题：

1. 什么是防火墙? 防火墙的基本特性有哪些？

在网络中，所谓“防火墙”，是指一种将内部网和公众访问网分开的方法，它实际上是一种隔离技术。防火墙是在两个网络通讯时执行的一种访问控制尺度，它能允许你“同意”的人和数据进入你的网络，同时将你“不同意”的人和数据拒之门外，也可以“允许”或“拒绝”内网的用户使用某种网络服务和协议，不和外网沟通，避免产生危险的数据连接。最大限度地阻止网络中的黑客来访问你的网络。  
  通常人们认为：防火墙是位于两个(或多个)网络间，实施网络之间访问控制的一组组件集合。它具有以下三个方面的基本特性：  
 1、内部网络和外部网络之间的所有网络数据流都必须经过防火墙。这是防火墙所处网络位置特性，同时也是一个前提。因为只有当防火墙是内、外部网络之间通信的惟一通道，才可以全面、有效地保护企业网部网络不受侵害。  
  2、只有符合安全策略的数据流才能通过防火墙。这是防火墙的工作原理特性。防火墙之所以能保护企业内部网络，就是依据这样的工作原理或者说是防护机制进行的。它可以由管理员自由设置企业内部网络的安全策略，使允许的通信不受影响，而不允许的通信全部拒绝地内部网络之外。  
 3、防火墙自身应具有非常强的抗攻击免疫力。这是防火墙之所以能担当企业内部网络安全防护重任的先决条件。就像公安干警一样，如果自己都没有“百毒不侵”的过硬意志和本领，又如何经得住罪犯的种种诱惑和攻击呢？防火墙处于网络边缘，它就像一个边界卫士一样，每时每刻都要面对黑客的入侵，这样就要求防火墙自身要具有非常强的抗击入侵本领。它之所以具有这么强的本领防火墙操作系统本身是关键，只有自身具有完整信任关系的操作系统才可以谈论系统的安全性。其次就是防火墙自身具有非常低的服务功能，除了专门的防火墙嵌入系统外，再没有其它应用程序在防火墙上运行。当然这些安全性也只能说是相对的。

1. 防火墙有哪些功能特点?

防火墙具有如下功能特点：  
  1. 保护那些易受攻击的服务。  
  防火墙能过滤那些不安全的服务。只有预先被允许的服务才能通过防火墙，这样降低了受到非法攻击的风险性，大大地提高了企业内部网的安全性。  
  2. 控制对特殊站点的访问。  
  防火墙能控制对特殊站点的访问。如有些主机能被外部网络访问而有些则要被保护起来，防止不必要的访问。通常会有这样一种情况，在内部网中只有Mail服务器、FTP服务器和WWW服务器能被外部网访问，而其他访问则被防火墙禁止。  
  3. 集中化的安全管理  
  对于一个企业而言，使用防火墙比不使用防火墙可能更加经济一些。这是因为如果使用了防火墙，就可以将所有修改过的软件和附加的安全软件都放在防火墙上集中管理；而不使用防火墙，就必须将所有软件分散到各个主机上。  
  4. 对网络访问进行记录和统计  
  如果所有对Internet的访问都经过防火墙，那么，防火墙就能记录下些访问，并能提供网络使用情况的统计数据。当发生可疑操作时，防火墙能够报警并提供网络是否受到监测和攻击的详细信息。

3、根据防火墙技术分类，防火墙大致可以划分为哪几类？

根据防火墙技术分类，防火墙大致可以划分为三类：包过滤防火墙、代理服务器防火墙、状态监视器防火墙。  
4、包过滤防火墙的工作原理是什么？  
  包过滤防火墙是最简单的防火墙，通常只包括对源和目的的IP地址及端口的检查。  
  包过滤防火墙的工作原理。采用这种技术的防火墙产品，通过在网络中的适当位置对数据包进行过滤，根据检查数据流中每个数据包的源地址、目的地址、所有的TCP端口号和TCP链路状态等要素，然后依据一组预定义的规则，以允许合乎逻辑的数据包通过防火墙进入到内部网络，而将不合乎逻辑的数据包加以删除。  
5、代理服务器防火墙的工作原理是什么？  
  代理服务器防火墙使用一个客户程序与特定的中间结点（防火墙）连接，然后中间结点与服务器进行实际连接。代理服务器技术是防火墙技术中最受推崇的一种安全技术措施，它可以将被保护的网络内部结构屏蔽起来，增强网络的安全性能，同时可以用于实施较强的数据流监控、过滤、记录和报告等功能。  
  代理服务器防火墙的工作原理。代理服务器运行在两个网络之间，它对于客户来说像是一台真的服务器一样，而对于外界的服务器来说，它又是一台客户机。当代理服务器接收到用户的请求后，会检查用户请求的站点是否符合公司的要求，如果公司允许用户访问该站点的话，代理服务器会像一个客户一样，去那个站点取回所需信息再转发给客户。  
  代理服务器通常都拥有一个高速缓存，这个缓存存储有用户经常访问站点的内容。在下一个用户要访问同样站点时，代理服务器就用不着重复地去查取同样的内容，这样做既节约了时间，也节约了网络资源。代理服务器会像一堵真的墙那样挡在内部用户和外界之间，从外面只能看到代理服务器而看不到任何的内部资源，诸如用户的IP地址等。  
6、状态监视器防火墙的工作原理包括哪些？  
  状态监视器防火墙的工作原理。这种防火墙的安全特性是非常好的，它采用了一个在网关上执行网络安全策略的软件引擎，称之为检测模块。检测模块在不影响网络正常工作的前提下，采用抽取相关数据的方法对网络通信的各层实施监测，抽取部分数据，即状态信息，并动态地保存起来作为以后指定安全决策的参考。  
  当用户访问到达网关的操作系统前，状态监视器要抽取有关数据进行分析，结合网络配置和安全规定做出接纳、拒绝、鉴定或给该通信加密等决定。一旦某个访问违反安全规定，安全报警器就会拒绝该访问，并被记录，向系统管理器报告网络状态。

1. 总结：

防火墙是一种被放置在自己计算机与外界网络之间的防御系统。在与监视和控制进出企业内部网络的所有通信。防火墙是由一组进程实现的，做为通向企业内部网络的网关。防火墙是一种用于监控入站和出站网络流量的网络安全设备，可基于一组定义的安全规则来决定是允许还是阻止特定流量。防火墙既可以纯硬件或纯软件，也可以是硬件和软件的组合。它可通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况， 以此来实现网络的安全保护。在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，有效地监控了内部网和Internet之间的任何活动， 保证了内部网络的安全。