3 防火墙与网关

0x01 实验环境

华为防火墙：ENSP 模拟 USG6000

0x02 原理介绍

防火墙的主要三大功能：拦截、记录、隔离。

五代防火墙分法：

一代包过滤是用一个软件查看所流经的数据包的包头，由此决定整个包的命运。静态。Iptablesip 协议 端口 网络层和传输层

二代代理防火墙[http 代理，socket 代理],应用层(http\smtp\telnet ftp)

三代状态检测防火墙是一种能够提供状态封包检查或状态检视功能的防火墙。跟踪网络连接的状态。又称动态包过滤防火墙。应用层。会话表【七层：网络、传层、会话层】

四代 WAF【应用层】 【最外部状态检测防火墙+WAF】,经典的部署方式

五代 NGFW 基于智能的 NGFW

1)硬件：RISC

内存，架构

2)智能化处理

3)功能多， (状态+WAF+网页防篡改+VPN)

0x03ENSP 的坑

实验环境在搭建的时候遇到了好多的坑，硬是在防火墙这个担误了两个月的时间才继续了再一部分的课程。

坑一：ensp 版本，要用最新的版本

所有相关的软件已经给大家准备好，大家在网盘上下载即可

坑二：ensp 挑环境，不管是 win7 win8 win10 win2003 我均试了一个遍，最终在 win10 成功，但也有许多的问题。

坑三：.dll 重新注册。方法如下

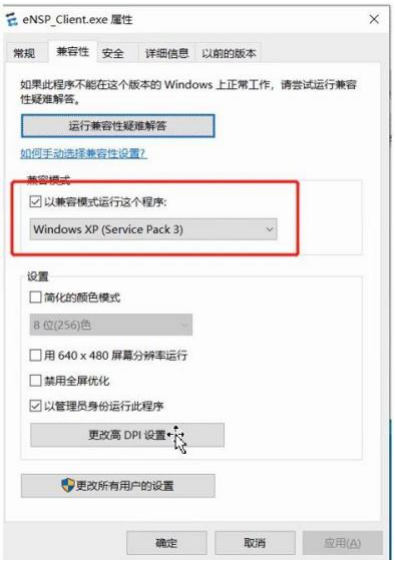
1、开始--运行--输入 smd

2、输入 cd %windir%\system32 (进入 windows 安装目录的 system32 文件夹)

3、输入 Regsvr32 Msxml3.dll

坑四：运行 ensp 要采用兼容模式：

如图所示，我想是因为对 xB.的兼容比较好的原因吧。


eNSP_Client.exe 属性
常规
兼容性
安全
详细信息
以前的版本
如果此程序不能在这个版本的 Windows 上正常工作，请尝试运行兼容性疑难解答。
运行兼容性疑难解答
如何手动选择兼容性设置?
兼容模式
以兼容模式运行这个程序:
Windows XP (Service Pack 3)
设置
简化的颜色模式
8 位(256)色
用 640 x 480 屏幕分辨率运行
禁用全屏优化
以管理员身份运行此程序
更改高 DPI 设置
更改所有用户的设置
确定
取消
应用(A)

0x04 实践