windows系统下IPSec应用 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/140/2021_2022_windows_E7_B3_BB_c100_140570.htm IPSec 首先需要指出的是，IPSec和TCP/IP筛选是不同的东西，大家不要混淆了。TCP/IP筛选的功能十分有限，远不如IPSec灵活和强大。下面就说说如何在命令行下控制IPSec。 XP系统用ipseccmd，2000下用ipsecpol。遗憾的是，它们都不是系统自带的。ipseccmd在xp系统安装盘的 SUPPORT\TOOLS\SUPPORT.CAB 中，ipsecpol在2000 Resource Kit里。而且，要使用ipsecpol还必须带上另外两个文件：ipsecutil.dll和text2pol.dll。三个文件一共119KB。 IPSec可以通过组策略来控制，但我找遍MSDN，也没有找到相应的安全模板的语法。已经配置好的IPSec策略也不能被导出为模板。所以，组策略这条路走不通。IPSec的设置保存在注册表中(HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local)，理论上可以通过修改注册表来配置IPSec。但很多信息以二进制形式存放，读取和修改都很困难。相比之下，上传命令行工具更方便。 关于ipsecpol和ipseccmd的资料，网上可以找到很多，因此本文就不细说了，只是列举一些实用的例子。 在设置IPSec策略方面，ipseccmd命令的语法和ipsecpol几乎完全一样，所以只以ipsecpol为例： 1，防御rpc-dcom攻击 ipsecpol -p myfirewall -r rpc-dcom -f * 0:135:tcp * 0:135:udp * 0:137:udp * 0:138:udp * 0:139:tcp * 0:445:tcp * 0:445:udp -n BLOCK -w reg -x 这条命令关闭了本地主机的TCP135,139,445和udp135,137,138,445端口。 具

体含义如下： -p myfirewall 指定策略名为myfirewall -r rpc-dcom 指定规则名为rpc-dcom -f …… 建立7个筛选器。*表示任何地址(源)；0表示本机地址(目标)； 表示镜像(双向)筛选。详细语法见ipsecpol -? -n BLOCK 指定筛选x作是“ 阻塞 ”。注意，BLOCK必须是大写。 -w reg 将配置写入注册表，重启后仍有效。 -x 立刻激活该策略。 2，防止被ping ipsecpol -p myfirewall -r antiping -f * 0::icmp -n BLOCK -w reg -x 如果名为myfirewall的策略已存在，则antiping规则将添加至其中。 注意，该规则同时也阻止了该主机ping别人。 3，对后门进行IP限制 假设你在某主机上安装了DameWare Mini Remote Control。为了保护它不被别人暴破密码或溢出，应该限制对其服务端口6129的访问。 ipsecpol -p myfw -r dwmrc_block_all -f * 0:6129:tcp -n BLOCK -w reg ipsecpol -p myfw -r dwmrc_pass_me -f 123.45.67.89 0:6129:tcp -n PASS -w reg -x 这样就只有123.45.67.89可以访问该主机的6129端口了。 如果你是动态IP，应该根据IP分配的范围设置规则。比如： ipsecpol -p myfw -r dwmrc_block_all -f * 0:6129:tcp -n BLOCK -w reg ipsecpol -p myfw -r dwmrc_pass_me -f 123.45.67.* 0:6129:tcp -n PASS -w reg -x 这样就允许123.45.67.1至123.45.67.254的IP访问6129端口。 在写规则的时候，应该特别小心，不要把自己也阻塞了。如果你不确定某个规则的效果是否和预想的一样，可以先用计划任务“ 留下后路 ”。例如： c:\>net start schedule Task Scheduler 服务正在启动 .. Task Scheduler 服务已经启动成功。 c:\>time /t 12:34 c:\>at 12:39 ipsecpol -p myfw -y -w reg 新加了一项作业，其作业 ID = 1 然后，你有5分钟时间设置一个myfw策略并测试它。5分钟后计划任务将停止该策略。如果测试结果不理想，