**WINDOWS服务器安全配置**

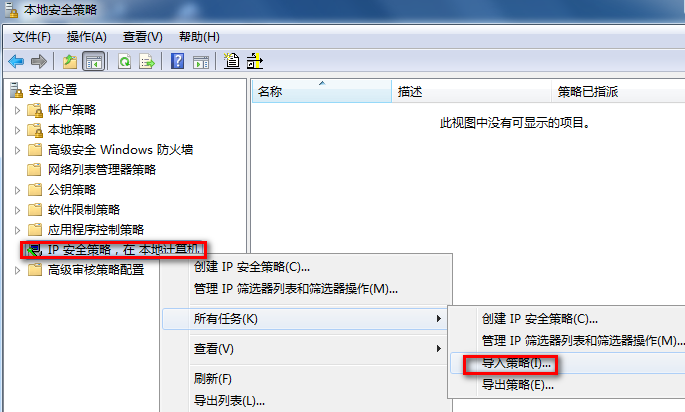
**1：更改RDP端口**

远程桌面端口默认是3389，务必进行更改。如果服务器是在内网，在路由器不要开放3389端口，可以采用其它端口映射到3389方式。最佳方案，更改掉3389防止内网有人中毒被当做肉鸡入侵了服务器。

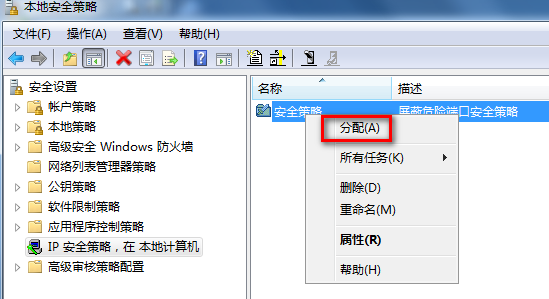
**2：开启WINDOWS自带的防火墙**

WINDOWS自带的防火墙，请开启，除了网站80,443，邮件25,465,110,995,143,993，以及远程桌面端口以外，其它任何端口，都可以屏蔽，当然如果你有其它软件，请根据情况开启相应端口。

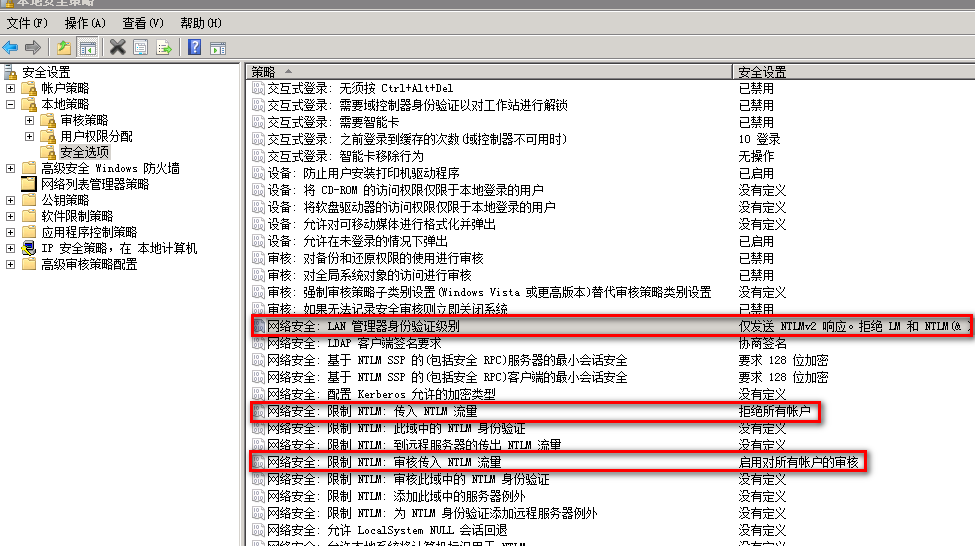
**3：通过本地安全策略**

A: 导入安全策略【本地安全策略20200516.ipsec】，屏蔽危险端口。 

**导入以后，务必右键点击》》分配 这样策略才会启用！**



B: 修改本地安全策略中的安全选项，如下图



**4：网卡的IPV6不用勾选，目前基本用不到，还可能影响性能。**

**5：禁用没用的 服务 ，详情如下**

Application Layer Gateway Service

Background Intelligent Transfer Service

Computer Browser

Diagnostic Policy Service  
Distributed Link Tracking Client  
Distributed Transaction Coordinator

IP Helper

Microsoft .NET Framework NGEN v2.0.50727\_X64

Microsoft .NET Framework NGEN v2.0.50727\_X86

Microsoft .NET Framework NGEN v4.0.30319\_X64

Microsoft .NET Framework NGEN v4.0.30319\_X86

Net.Msmq Listener Adapter

Net.Pipe Listener Adapter

Net.Tcp Listener Adapter

Net.Tcp Port Sharing Service

Remote Registry

Shell Hardware Detection

SSDP Discovery

Server

TCP/IP NetBIOS Helper

UPnP Device Host

Windows Remote Management

Windows Update [**可以设为手动**]

**6：网站IIS安全设置**

A：WEBDAV这个存在安全隐患，可以删除这个功能

B：请求筛选>HTTP谓词，在 **允许谓词**中，添加：HEAD,GET,POST 在 **拒绝谓词** 中，添加：TRACE，PUT，OPTIONS， DELETE网站环境，仅仅GET,POST等就足够了。

**7：利用IPBAN拦截爆破扫描**

WINDOWS 2008至最新的WINDOWS2019服务器，都可以安装IPBAN防止别人扫描远程桌面的密码入侵。将IPBan文件夹复制到C盘，点击：安装IPBAN到服务.bat 即可自动安装并启动IPBAN 【**需要NET4.0，文件夹有，如果没安装的，先安装好NET4.0**】

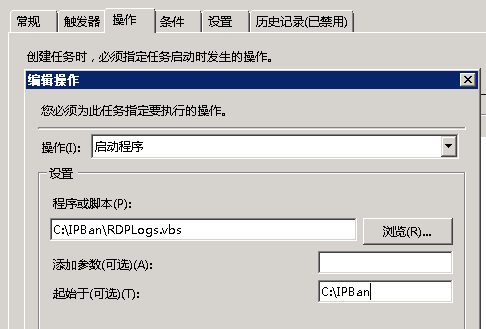
**8：利用任务计划，记录登陆远程桌面的IP**

打开 任务计划程序》创建任务》

常规：输入任务名字，如RDPLOG，勾选 使用最高权限运行

触发器：新建》当连接到用户会话时；当从用户会话断开连接时

操作：启动程序



**备注：更改VBS中的端口**

用记事本打开： C:\IPBan\RDPLogs.vbs

把第6行的 3389 端口，更改为你最新的远程桌面端口