防火墙

防火墙作为抵御攻击的第一道防护，责任重大，但是他又肩负着NAT上网的重要职责，性能和稳定性又要求很高。我认为从纯安全角度讲，选择防火墙时需要考虑下列几个功能：

恶意网站过滤

恶意文件过滤

IPS/IDS

IPS/IDS在这里有个非常重要的作用就是识别使用Nday的软件尤其是浏览器、办公网套件漏洞攻击员工的行为。有很多厂商宣称自己的IPS/IDS可以识别0day，我个人认为目前比较成熟的0day识别技术主要依赖沙箱和机器学习，真要识别0day还是需要专业的APT设备来做。

**APT设备**

APT设备通过分析邮件、流量中的文件和流量行为识别APT行为，我知道国外fireeye、趋势、pa、mcafee等都做这块在。

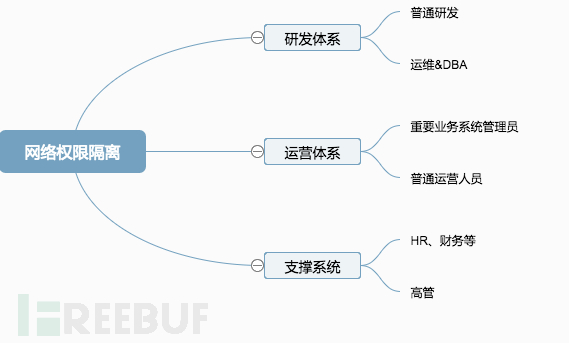
**安全隔离**

安全隔离的主要目的有两个：

按需提供网络访问权限，避免权限滥用

减小黑客在办公网横向渗透以及纵向提权的攻击面，提高攻击成本

出于这两个目的，所以安全隔离通常和准入或者vlan划分结合在一起，不同的地方主要在于准入可以根据用户身份动态调整网络权限，vlan划分相对不够灵活。

[](https://image.3001.net/images/20170313/14893867297720.png)

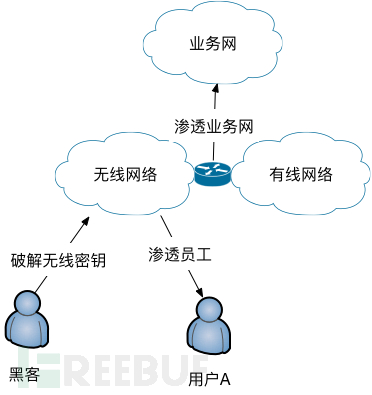
上图是一个简单的分类，其中有几类同学需要重点关注：

运维&DBA，系统权限特别大，纵向提权的最佳目标，有种开玩笑的说法，黑掉一个运维的电脑，把所有文本文件翻个遍，找不到一个密码才是见鬼了。应当尽量限制其他人群对他们的访问。

重要业务系统的管理员，这些同学负责对公司核心业务进行运营管理，对重要后台系统具有很高的权限，一旦他们电脑被入侵，后果会很严重。比如游戏公司充值系统的后台、广告公司的客户广告投放管理系统、招聘公司的后台简历管理系统、电商的订单物流管理系统，出点事都是大事。应当尽量限制其他人群对他们的访问，同时严格限制他们的外网访问权限。

高管、HR、财务，这些同学对办公系统的访问需求比较单一，主要网络访问需求在外网，通常不懂技术，安全防护意识也最弱，也最得罪不起。他们的办公电脑集中大量公司重要数据，一旦被入侵就直接产生损失了。这部分同学可以严格限制跟办公网其他区域以及对内部系统的访问。

## 无线安全

[](https://image.3001.net/images/20170313/14893867453309.png)

无线情况就特别复杂了，这里讨论比较常见的情况。不少公司的无线依靠静态密码保护，认证通过后即可以访问办公网络。这里有两个甲方常见误区：

**我无线只覆盖公司内部，黑客咋搜到？**

黑客如果真打算黑你，真可以到你公司附近，现在的AP发射能力都很强，黑客如果使用专用设备，接受信号能力也很强。

**我无线密码好复杂，黑客不可能暴力破解**

本本上装个kali，买个好点的usb网卡，wpa/wpa2密码破解只是时间问题。另外现在不少wifi助手有记住密码功能，内部员工一旦误点了记住免费wifi，其他人使用wifi助手连接这个wifi就会自动认证，破解都不用了。所以无线网络最好可以限制仅能访问外网，并且加上类似准入的二次认证机制，也可以使用域密码或者证书认证，降低静态密码被泄露和破解的风险。

## 终端安全

终端安全是办公网安全的重点，涉及面非常广，核心诉求至少包括一下方面：

提高终端安全基线，减小攻击面

基础防病毒能力，具备抵御常见Nday病毒木马的能力，提高攻击成本

基础的终端系统、应用软件资产搜集以及管理能力，针对常见的Nday系统、应用软件漏洞具有发现、修复的能力，提高攻击成本

为了达到以上要求，需要借助一定的商业解决方案。

### 终端安全加固

终端安全加固的目的是提高安全基线，减小攻击面，事半功倍的方法是让PC终端统一加入window域，通过域控策略统一管理终端的安全策略，介绍域策略的文章很多，这里只提下几个比较重要的点：

开启屏保以及锁屏时间

域账户密码复杂度，密码更换时间

禁用guest账户

开启主机防火墙

禁止administror账户远程登录（员工自己域账户是本地管理员，可以正常登录，很多公司喜欢用ghost预装电脑，administror账户的密码绝对是个大坑）

禁止域管理员远程登录（一定要把域控和一般PC放在不同组策略下，不然这个策略害死人）

删除IPC$ C$ D$ admin$（木马经常利用）

开启审计策略，记录登录、账户相关事件

调整事件日志的大小及覆盖策略

关机清理虚拟内存页面文件

### 终端防病毒

终端防病毒肩负着具备抵御常见Nday病毒木马的能力，提高攻击成本的重任，不过传统解决方案基本就是纯粹的黑名单和基于病毒特征，似乎这一领域也是红海中的红海。可喜的是最近两年终端安全又被各大安全厂商重视起来，因为越来越多的有针对性的攻击行为被揭露，跳板都是办公终端，大家对这块越来越重视；另外新的检测技术以及解决思路落地实现，安全厂商提出了EDR的概念，即终端检测与响应。基本思路是默认攻击者始终会渗漏公司网络，让安全人员利用IoC和终端行为来快速检测任何入侵，减小攻击者造成的损害。

### 终端管理

终端管理主要解决两个安全问题：

系统、应用软件版本的管理

系统、应用软件漏洞的自动化修复

微软的WSUS以及SCCM虽然只能搞定微软系软件以及flash的问题，但是已经可以解决大部分问题了，针对类似java、chrome这类常用第三方软件的升级，就需要专业的终端管理解决方案了。

### 准入系统

准入系统可以基于员工身份做到灵活的网络权限限制，保障主机安全基线的强制执行。这部分可以参考我以前的文章《企业安全建设之自建准入系统》。

## 系统安全

办公网的系统安全，出了加固手段，还需要通过漏洞扫描器定期自动化发现。我理解这里的扫描器至少需要解决几方面问题：

各种弱密码

系统级漏洞，比如ms08-067、MS12-020

第三方软件漏洞，比如Cisco WAG120N多个远程命令执行漏洞

## 建设步骤

通过以上努力，我们基本建设起了办公网的纵深防御系统，整个办公网具有了一定的安全防护以及感知能力。公司的预算总是有限，人力也是捉襟见肘，从无到有建设这么个安全防护体系不是一年半载的事，需要拍优先级，下面是一个建议：

第一步，安全边界建设，风险初步可控，比如IPS、NGFW、杀毒、准入、无线加固

第二步，细化终端安全建设，进一步提高防护能力，比如终端管理、安全加固

第三步，提高安全感知能力，锦上添花，比如蜜罐、漏洞扫描、APT、siem

每个公司安全现状不一样，业务情况也不一样，具体实施步骤和策略需要因地制宜。安全意识教育也是非常重要的一个环节，尤其针对社工，技术防护手段效果一般。

十分典型的安全域划分为，办公区、业务区、外网、办公服务区、开发测试服务区。

办公区：员工办公的区域，主要组成是办公终端，容易被入侵后成为跳板

业务区：对外提供服务的区域，主要组成是业务服务器

外网：主要组成是黑客和用户

办公服务区：支撑员工办公的服务，主要组成是邮件、erp、crm等办公服务服务器，特别要强调的是这部分的员工、运营相关数据有时比线上数据还要敏感和重要

开发测试服务区：支撑员工开发测试的服务，主要组成是开发测试服务器，这部分服务属于灯下一片黑，也非常容易被入侵后成为跳板

安全区域划分后，通过边界访问控制，可以达到以下目的：

最小化各个安全区域的攻击面

单安全区域被攻陷后，控制影响范围，风险可控

### 中型互联网企业安全区域划分

假定所有服务器都部署在IDC或者公有云上。员工和用户访问所有服务都需要通过外网。安全域内的主机互相信任，跨安全区域互相不信任，严格限制访问，我们的基本假设是，每个区域都可能被入侵。区域划分就是为了这个时候提供黑客进一步入侵的成本，为后面的入侵检测和应急响应争取时间。

业务服务器区：强烈建议仅通过负载均衡对外发布服务，业务服务器区对外网仅暴露堡垒机和负载均衡设备的端口，这样可以最小化攻击面，类似mongodb勒索事件可以有效避免，常见的国外负载均衡设备（也叫应用交付）厂商如下,当然也可以用开源的LVS之类。

业务服务器会有各种管理后台，包括但不限于：

业务管理后台

tomcat管理后台

zabbix等运维管理后台

hadoop、docker等开源软件的管理后台

可以限定管理后台的端口段，仅允许办公区的公网IP访问，这样可以有效提高黑客攻击管理后台的成本。当然部分业务的管理后台会给大量代理商、外包使用，无法限制源IP，这个就没失效了。

### 内部服务区域

这个区域包含大量运营、人事、研发相关的重要企业数据，安全等级甚至比业务区域还要高，但是往往容易被甲方忽略，成为入侵的重灾区。原则上这个区域也只允许来自办公区域的访问。

### 测试开发区域

与内部服务器区域类似，这个区域大量开发中的产品，安全基线最差，最容易被入侵，原则上这个区域也只允许来自办公区域的访问。

业务区域、内部服务区域、测试开发区域难免业务上有需要，部分服务需要互通，这个以白名单形式开放。

各个区域针对SSH和远程桌面的访问仅信任堡垒机IP。

混合云模式其实也类似就不再赘述。

## 主机加固

主机加固相关文章非常多，各家实际情况又特别复杂，这里主要列举比较重要的几个点，实际落地的策略还需要大家自行完善。

### linux主机OS层面加固

**禁止root登录**

**vi** /etc/ssh/sshd\_config

PermitRootLogin no

**禁用LKM**

LKM的全称为Loadable Kernel Modules，中文名为可加载内核模块，主要作用是用来扩展linux的内核功能。LKM的优点在于可以动态地加载到内存中，无须重新编译内核。由于LKM具有这样的特点，所以它经常被用于一些设备的驱动程序，例如声卡，网卡等等。当然因为其优点，也经常被骇客用于rootkit技术当中，强烈建议默认关闭，除非必要，不要使用。

echo 1 > **/proc/**sys**/kernel/**modules\_disabled

需要写到开机启动项里面，这个比直接内核编译时禁用LKM具有可操作性，因为一旦手工关闭LKM应用异常后，只需要开启即可。

**开启ASLR**

ASLR，即Linux 内存地址随机化机制，可以在linux服务器遭受缓冲区溢出攻击时提高攻击成本。

分为三个级别

0 – 表示关闭进程地址空间随机化

1 – 表示将mmap的基址，stack和vdso页面随机化

2 – 表示在1的基础上增加栈（heap）的随机化

echo 2 >**/proc/**sys**/kernel/**randomize\_va\_space

需要写到开机启动项里面

### window主机OS层面加固

**开启window防火墙**

默认只开放web服务以及远程桌面端口。window最容易出事的就是139、445、135这三个端口的服务，除非万不得已，默认一定要干掉这些端口。

## 痛点

基于历史教训，我们上准入系统想解决的痛点简单归纳就是：

身份认证：wifi和有线接入到情况下能设备／IP与人绑定，调查安全事件可以定位到人

权限限制：不同职能的人群网络权限不一样，权限最小化

安全加固：满足公司安全基线要求的设备才能接入内网，没装杀毒没打补丁就禁止接入

调研了国外几家准入厂商的产品，总结了下它们的优点：

认证授权与微软域SSO集成

有线无线切换时自动认证

网络控制在三层减少对网络基础设施的依赖

PS：策略服务器，负责用户认证，权限下发

AAA：3A服务器，存储用户信息，这里就是微软的AD域控

enforcer：执行器，负责控制网络权限

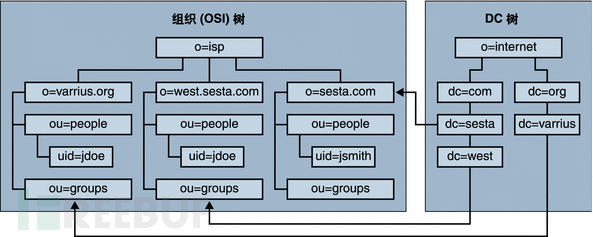
agent：客户端程序，安装了办公PC上，负责上传用户认证信息，执行主机检查策略

## 权限模型

权限模型是个非常基础但是非常重要的模型。我们先来看下公司的组织模型：

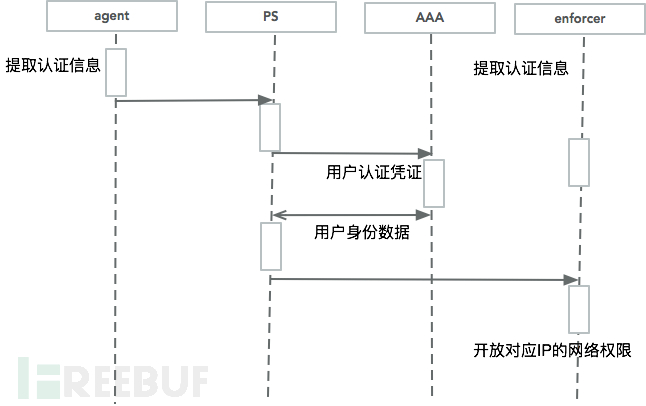
[](https://image.3001.net/images/20170207/148644506287.png)

员工的网络权限往往和他的工作内容相关，对应的就是部门属性，所以最简化的模型就是直接从组织模型转化，用户对应到不同的角色，角色对应一个或者多个部门。角色的定义就是具有相同网络访问权限的员工的集合。对应的微软域控也是这种层次结构：uid对应用户名，ou对应部门。

[](https://image.3001.net/images/20170207/14864450764875.png)

## 准入流程

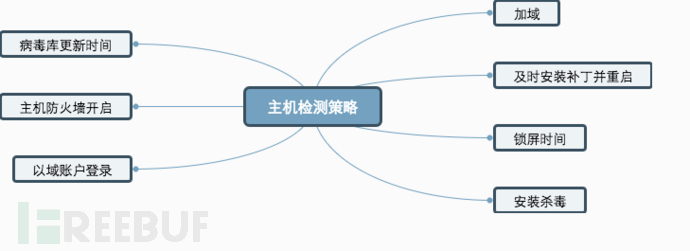
简化的准入流程如下：

[](https://image.3001.net/images/20170207/14864450886994.png)

其中主机安全合规检测在认证之前，不满足主机安全策略的连认证都不会发起。

## 主机检查策略

主机检测策略需要结合公司实际情况，我简单描述下比较通用的几个：

[](https://image.3001.net/images/20170207/14864450981709.png)

强烈建议PC都加入域，这样主机检查可以非常简化，大量的安全加固策略可以通过域的组策略强制下发给终端。

我们采用了一个折衷的方案，就是把用户名和硬件做了绑定，指定的用户名只能在指定的硬件上使用，其中核心的是硬件的识别，具体思路就是获取若干硬件信息，形成一个硬件向量，任意一个影响向量变化都判定硬件改变，需要后台重新绑定，否则即使密码正确也会判定认证失败，这个是提高硬件伪造的成本，其中任一变量其实都是可以伪造的，大家不要太纠结。下面列举各个厂商经常使用的一些硬件信息，具体实现时建议大家增加一些其他变量：

### CPU序列号

目前存在的CPU几乎都支持CPUID指令。这个指令不仅可以获取CPU生产厂商等基本信息，还可以获取其他有关CPU的硬件信息，包括CPU序列号。

### MAC

网卡MAC是具有国际标准的地址编号，能够确保世界上的每一块网卡具有唯一的序列号。

### 硬盘序列号

除了一些特殊硬盘外，大部分硬盘都有自己唯一的硬件序列号，而且不可修改。

### 硬盘分区序列号

首先要说明，硬盘分区序列号和硬盘物理序列号是不同的东西。硬盘物理序列号是硬盘厂商指定的，而分区序列号是分区软件指定的。每次重新分区的时候，这个序列号会变动。对于GPT硬盘分区来说，每一个分区都使用全球唯一的UUID来标识，具有良好的唯一性和可用性。另外对于RAID设备来说，分区序列号同样存在并可用。

### 主板序列号

## 其他

### 蜜罐

部署一定数量的蜜罐，可以起到事半功倍的效果，最简单的就是用类似honeyd之类开源的伪装成window终端即可。

### siem

办公网数据量基本不大而且商业产品居多，使用ossim就可以很好解决数据搜集、展现、自定义报警、关联分析的功能了。

## 建设步骤

通过以上努力，我们基本建设起了办公网的纵深防御系统，整个办公网具有了一定的安全防护以及感知能力。公司的预算总是有限，人力也是捉襟见肘，从无到有建设这么个安全防护体系不是一年半载的事，需要拍优先级，下面是一个建议：

第一步，安全边界建设，风险初步可控，比如IPS、NGFW、杀毒、准入、无线加固

第二步，细化终端安全建设，进一步提高防护能力，比如终端管理、安全加固

第三步，提高安全感知能力，锦上添花，比如蜜罐、漏洞扫描、APT、siem

每个公司安全现状不一样，业务情况也不一样，具体实施步骤和策略需要因地制宜。安全意识教育也是非常重要的一个环节，尤其针对社工，技术防护手段效果一般。

满足审计，唯一身份

**这里列举一般办公主机的需求项：**

* 病毒防御（本地查杀选用国外厂商的产品，能接受云查杀选用国内厂商的产品，没有重要机密的内容的）；
* 入侵检测防御（说白了就是HIDS或者HIPS产品，一般国内都是和杀毒软件集成的）；
* 漏洞防护（打补丁，一般国内也是集成在杀软里面的）；
* 软件管控（软件中心功能，一般对win平台比较常见）；
* 日志记录；
* 管控场景（禁止起SSID等、数据防泄漏DLP）

**这里用来解释一下日志需求：**

* 日志记录一般可以做两件事情被攻击的响应追查和主动攻击的追踪溯源；
* 日志可以记录邮件、进程、服务、命令等等；

### 办公主机安装和在线率提高方案

* 全员检查
* 内网做准入
* 虚拟桌面后台强制安装

### 工作三部曲

* 推全员安装
* 做准入推全员再现
* 推漏洞补丁自动安装并接受实时日志

### 重点管控对象

* 人力资源部门
* 法务财务部门
* 高管要职群体
* 助理秘书群体
* 投资融资部门
* 其他关键人员

### 重点效果预期

* 自主防御能力提升化
* 漏洞补丁修复自动化
* 敏感数据传存安全化
* 病毒爆发场景预知化
* 攻击失陷发现简单化