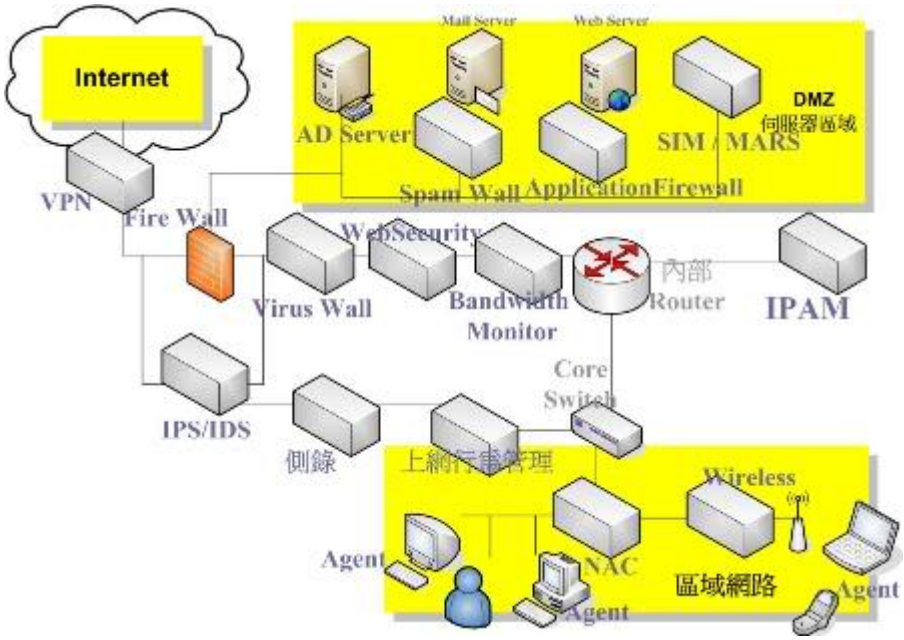
最深入的网络安全设备知识讲解

来源于:互联网

观念:

在网络上，主要的概念是：该如何做才能让封包流量更快、更稳。
在资安上，主要的概念是：如何掌握、比对、判断、控制封包。

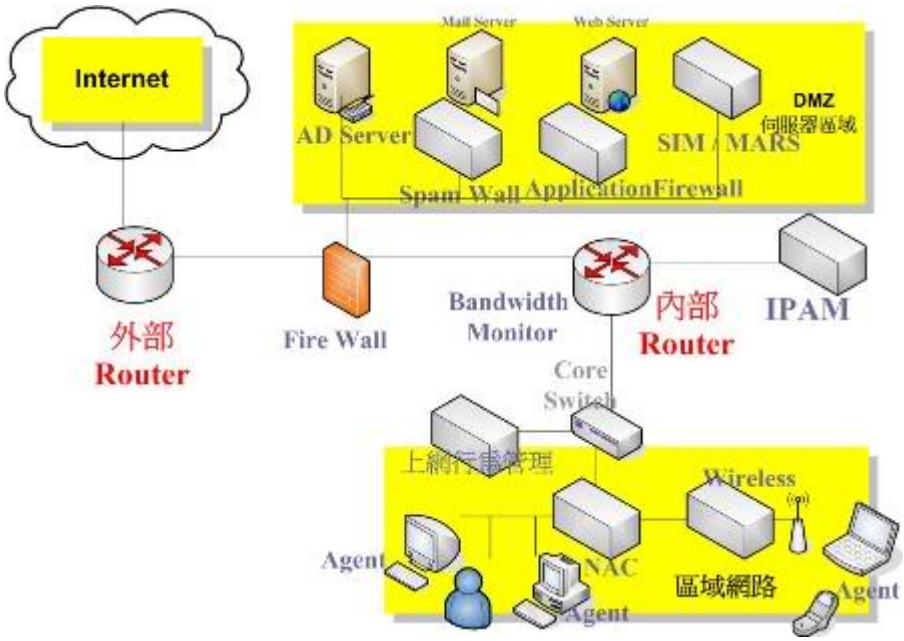
好吧~让我们直接来看在一个网络环境里，我们可以在哪些地方摆入资安设备:



(设备实际摆设位置会因为产品不同与客户环境而有所变动)
是滴~任何网络设备、任何网络位置都可以看见资安设备的踪影!为什么呢?因为上面提过，资安的概念是如何掌握、比对、判断、控制封包!做个有趣的比喻，你可以想象一个原始封包就像个光着身子的美女，随着 OSI 模式各层的设计师帮她穿上合适的衣服之后才让它出门，VPN 只能看见包裹着白布的木乃衣、Firewall 可以看见去掉白布后穿着厚衣服的美女容貌、IPS 可以从外套推测美女内在的三围、该死的 VirusWall 竟然有权可以对美女搜身、上网行为管理可以去掉白色的衬衫看美女身上的内衣裤是否是老板希望的款式…好吧~我们聊的是 Network Security，我必需就此打住!至少我们了解一件事，资安的 Solution 可以存在网络的任何地上(SI 知道一定很开心~生意做不完呀!)

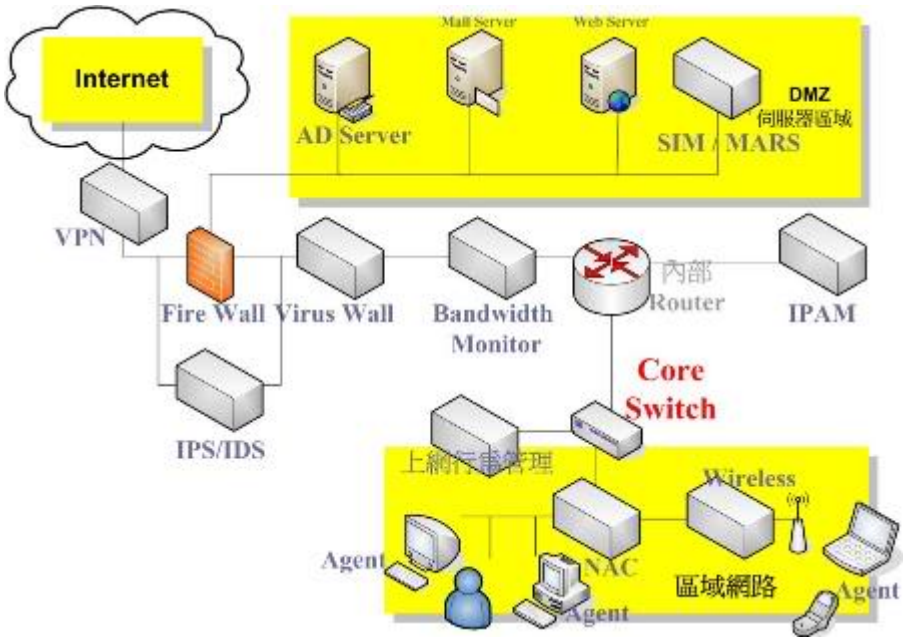
资安设备简介:
接下来是针对各设备做常识性地说明，让大家对资安设备有一个全盘性的概念!
(由于小弟碰的设备有限经验也不足，仅对知道的一小部份说明，任何错误与不足，还望各前辈们指正)

。Router:



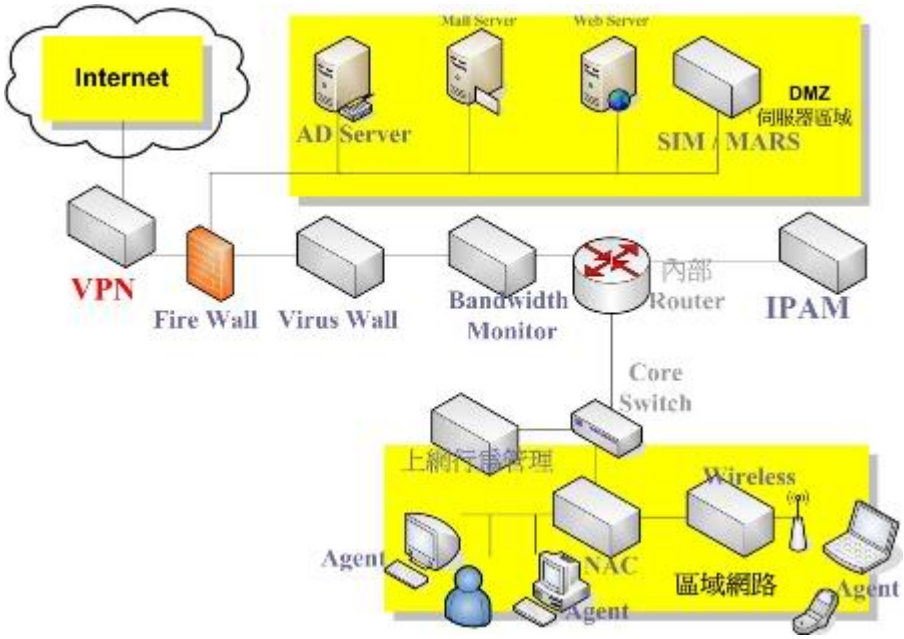
Router 通常是 Cisco 的 Router 才能加上资安的解决方案，Cisco 新一代 Router 都叫 ISR(Integrated Service Router)，可以整合 IPS 或 Voice 模块，在外部的 Router 通常我们希望它扮演好 Router 的角色即可，而内部买不动一台 IPS 设备时，会建议客户从现有的 Router 上加上 IPS 模块。

。Switch:



Switch 一般也要到 Core 等级才可加入 IPS 模块，就如同 Router 一样，主要就是加上入侵侦测的功能，在客户环境 Switch 效能 ok，也不打算多买设备，可以加入模块方式来保护网络。

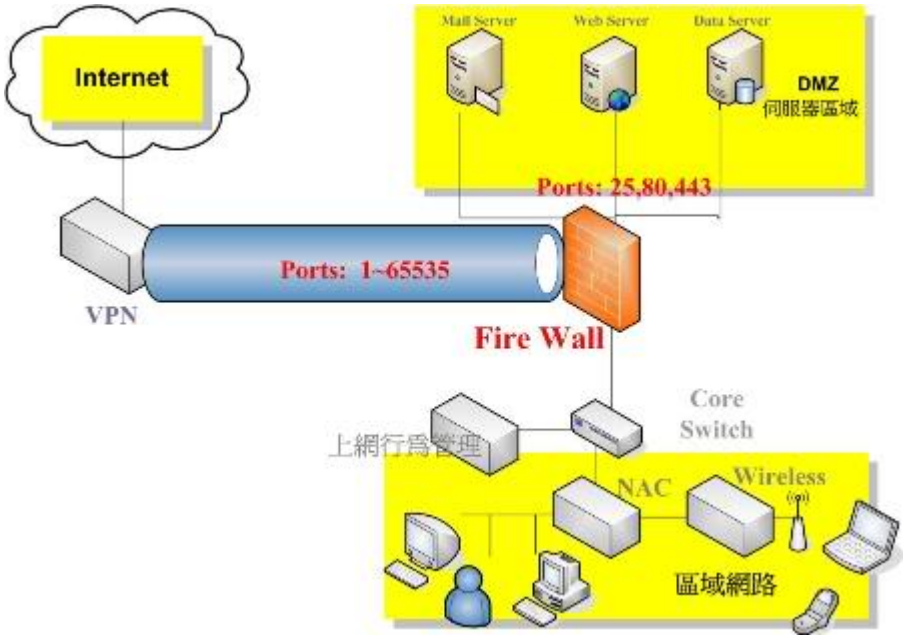
。VPN:



VPN 即 Virtual Private Network，顾名思义即是要达成一个虚拟的私人网络，让在两个网域的计算机之间可以像在同一个网域内沟通一样。这代表的是必需做到外部网络是不能存取或看见我们之间的封包传送，而这两个网域之间是可以轻易的相互使用网络资源。要做到如此，VPN 必需对流经封包进行加密，以让对外传输过程不被外人有机看见传输内容，相对的传过去的目的地需要一台解密的机器，可能也是一台 VNP 或是一个装在 notebook 上的软件。也因为传输过程加密之故，许多希望在传输上更安全的需求，也都会寻求 VPN。

VPN 的发展到现在，主要市场以 SSL VPN 的运作，因为可以利用现有的客户端程序(如 IE)即可完成加密、解密、验证的程序，使用端不需一台 VPN 机器，或是 client 端程序，在导入一个环境最容易，使用上也最简便。

。FireWall:

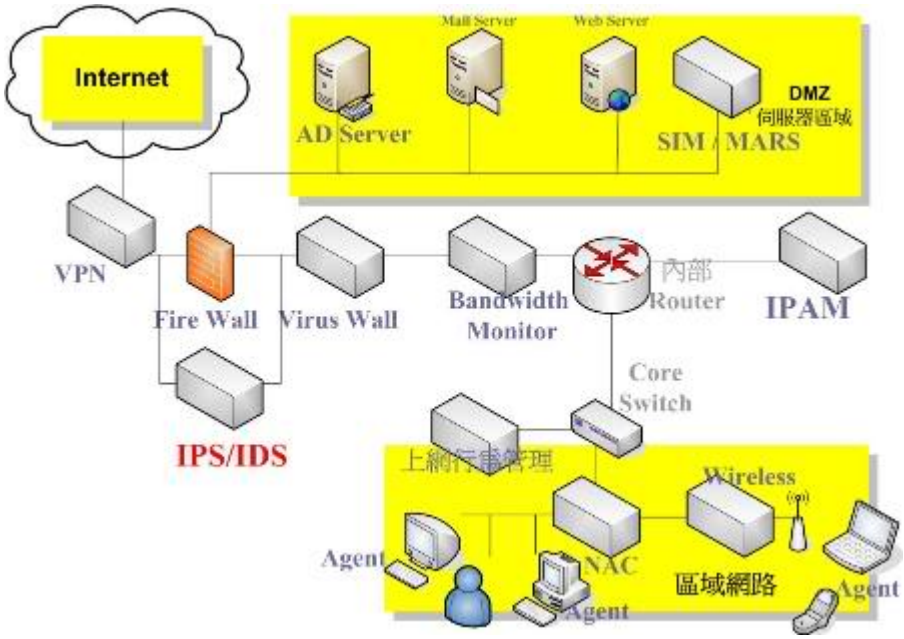


FireWall 肯定是最古老的资安产品，但!也是最经典的产品，简单的说，它就像 Port 的开关,如上图 firewall 左边的 port 可能 1~65535 都有,但封包想流进来~嘿!得先问问 Firewall 老大哥，这里他只开放了 25,80,443 的流量进来，其它都别想!!

Firewall 的第二个大功能就是可以区别网段，如上图的 DMZ 也可以从 Firewall 切出来，如此可以确保网络封包的流向，当流量从外面进来观顾时，只允许流到 DMZ 区，不可能流至内部区网内，避免外部网络与内部网络封包混杂。

第三个功能，也就是能区别从 Router 上设 ACL 的功能，SPI(Stateful Packet Inspection)封包状态检查，可快速地检查封包的来源与目的地址、通讯协议、通讯 port、封包状态、或其它标头信息，以判断允许或拒绝!

。IPS/IDS:



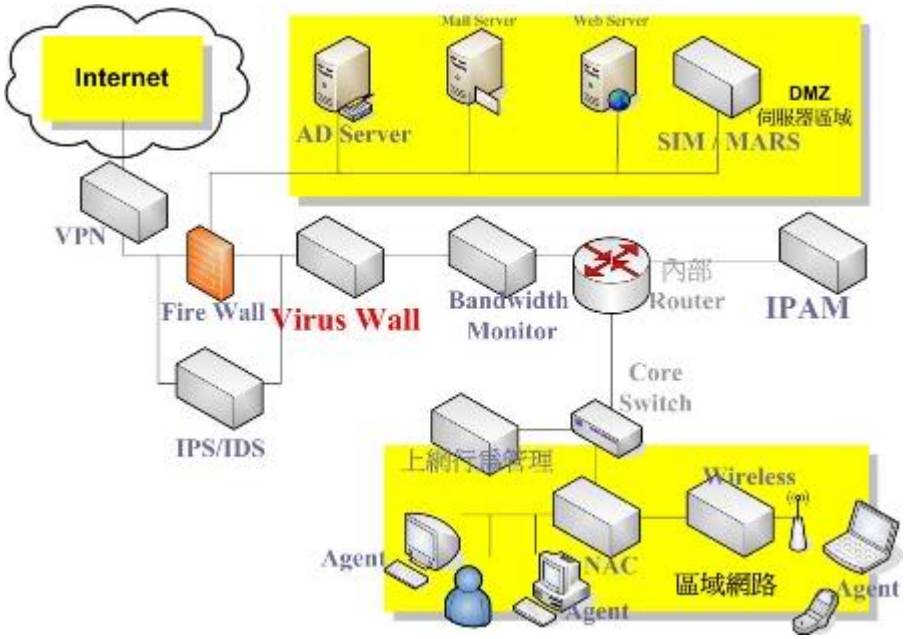
这仍然是很年轻的产品，一开始叫 IDS(Intrusion Detection System)入侵侦测系统，顾名思义:在有人攻击或入侵到我的土地内之后我会知道，是一个可以侦测出有没有人入侵这个事件!后来人们体会到，坏人都跑进我家了我才知道，有没有可能在侦测到的同时做出抵制的动作呢?于是 IPS(Intrusion Prevention System)入侵防御系统就诞生了，在 IPS 中写入 pattern，当流经的封包比对 pattern 后确定为攻击行为，马上对该封包丢弃或阻断来源联机。

一般 IPS 系统都不只一个网段，如上图，可以摆在 Firewall 前面更积极地阻挡对 Firewall 的攻击，或是于 Firewall 之后，直接比对流经合法 port 后进来的流量是否为攻击行为，也可分析流出封包(了解内部员工上网行为、情况)。在真实情况是否要将 IPS 摆在 firewall 之前要看硬件 throughput，看哪一台的效能好就摆前面吧^^

通常 IPS 的测试期比较长，因为在环境内开启 IPS 规则后会有”误判”情形!实属正常，除

非开的规则太宽松，否则有正常的封包被挡是正常不过的，这时我们就需要对规则调校，所以测 IPS 是磨工程师的大好机会!运气不好，要对每一个有问题的计算机、程序手动抓封包来 k~~嘿~就当是练工吧^^

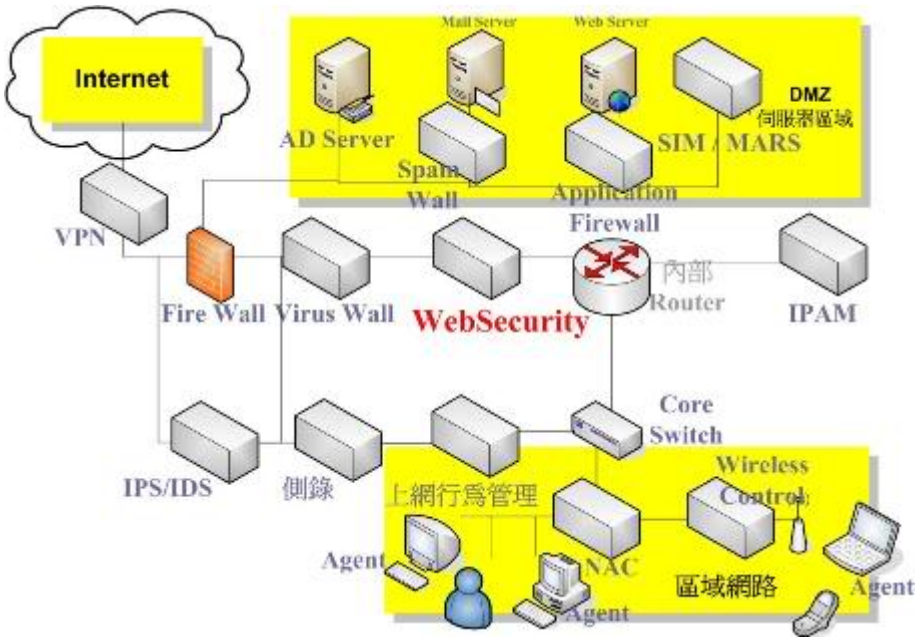
。Virus Wall:



VirusWall 是较简单的产品，概念就是将防毒引擎放在 Gateway，让所有流经的封包都能比对过引擎内的病毒特征。
说到这，大家应该知道评估 ViruWall 的重点了!
。什么防毒引擎
。扫毒速度快或慢
防毒永远没有人敢打包票可以 100%防毒!纯粹是机率问题，每家的防毒率都不一定，能补足的最简单方法就是导入与原有环境不同的防毒引擎!
如原有 client 端用的是 norton，于是 viruswall 就找一家卡巴的^^
或前方 UTM 用趋势的，还可导入 McAfee 的 viruswall

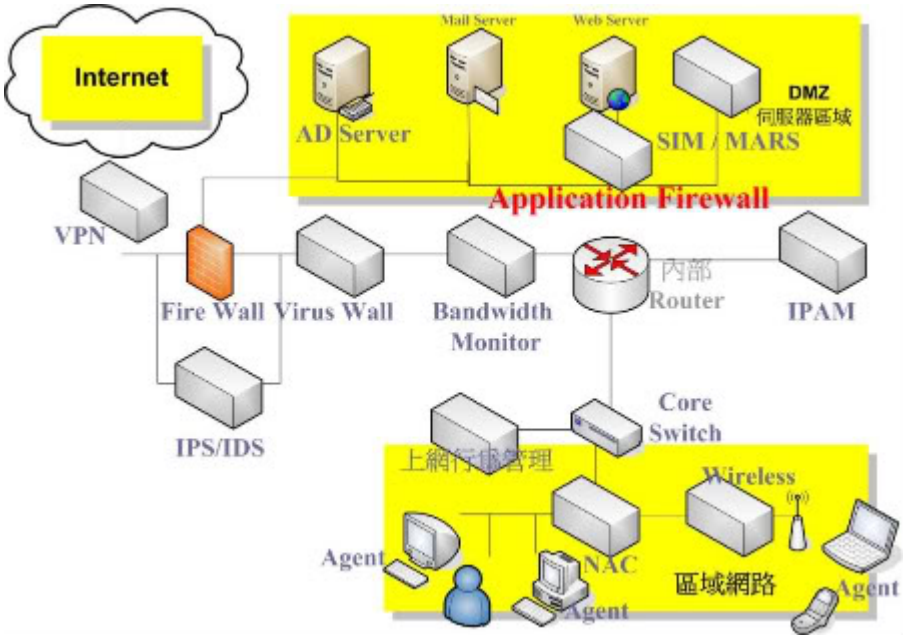
VirusWall 对装机工程师而言是很简单的产品，只需留意客户希望对哪些 Port 的流量进行扫毒，难的是背后更新病毒码的 RD 们~我只能说，RD 们辛苦了!!

。WebSecurity



WebSecurity 单纯地过滤 Web 流量中的封包，针对每个要求的 URL 比对数据库是否为危险、或钓鱼、恶意的目的 URL，是的话就直接阻挡联机。
如果连到了目的地之后，可能因为临时被骇或数据库内没有该笔 URL，回来的封包再经一次病毒引擎的扫描，由于是针对 Web，所以病毒引擎要挑在恶意网站分析较强的引擎。
简单的说，怕 user 上网中毒、或钓鱼网站被受骗，需要导入这个设备^^

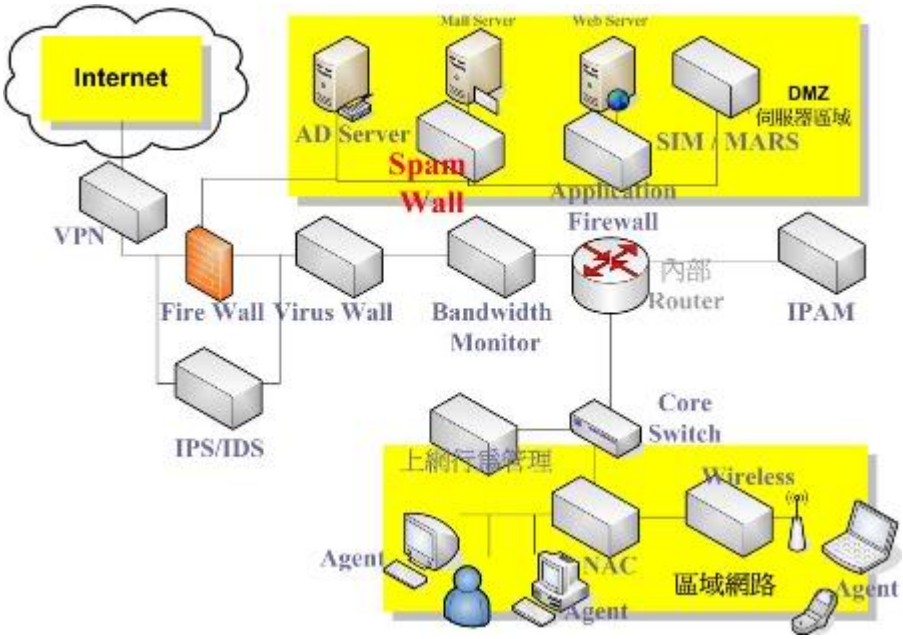
。ApplicationFirewall



对于很重视网页运作服务的公司，对于这项设备应该较有兴趣。
较简单的例子是在做渗透测试时，总是会在客户的 Web 网页可输入的地方 try 一下 SQL 语，当把这设备放在 WebServer 之前，你的语法会顿时失效，好吧~这时会再试一下 XSS、cookie、

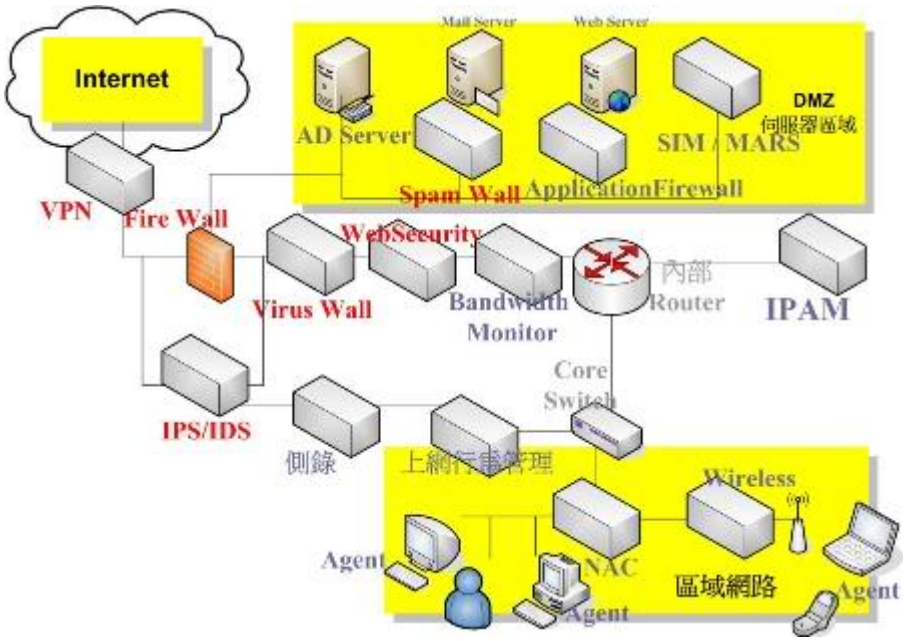
session…呵~时常是没有成效的试验@@
即使 WebServer 运行的 IIS 或 Apache 未更新，拥有众所周知的漏洞，仍然阻挡住该漏洞的攻击。
当然!就如之前提过的，资安是机率问题，它可以降低被攻击机率，但不可能无敌!

。Spam Wall:



电子邮件是一个很棒的广告途径，但随着信息愈来愈发达，越来越多的生意靠着 e-mail 来广告，慢慢的，使用者感受到过多的 e-mail 造成的不便，于是挡垃圾信的设备就诞生啦~可以叫 Anti-spam 或 Spam wall。
一开始的 spam 单纯地阻挡垃圾邮件，但许多黑客发现了这个管道，也利用 mail，大量发送钓鱼连结、附加病毒文件、恶意连结…的信件，于是 anti-spam 也开始重视对 mail 的扫毒。
一台好的 spam 设备在选择上要效能好(承受邮件攻击)，误判率低、有黑、灰、白名单，使用简单^^

。UTM/ASA:

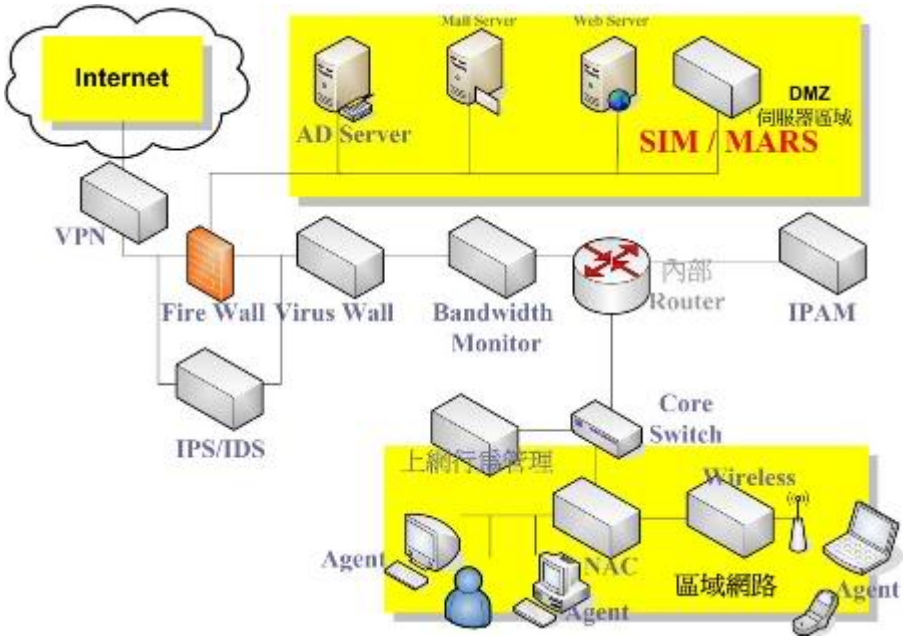


大补帖 UTM(Unified Threat Management)统一威胁管理设备，其功能包山包海，如上图的红色部份为一般 UTM 设备可能拥有的功能，会依厂牌所制定的功能而定。

概念就是以 FireWall 为核心，加入各式资安功能!如 Cisco 的 ASA 就是以 firewall 为中心，可加入防毒模块或是 IPS 模块。

一般是比较建议在 300 人以内的环境使用 UTM，简单又大碗!但，在环境较大的情况下，还是建议将各别功能由各别设备运作。原因很简单，一样的防毒引擎来说好了，UTM 的特征码肯定没有单纯 VirusWall 的特征码来的多!纵使厂商声称一样，实际测试便知高下^^

。SIM/MARS:



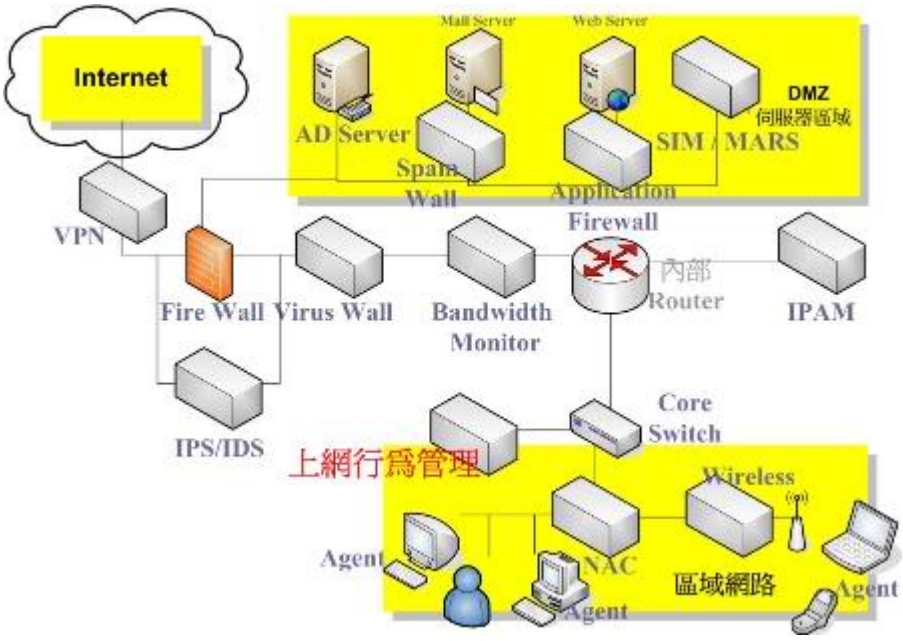
躲在右上角的设备名叫 SIM(Security Information Management)资安讯息管理，或如 Cisco 较贴切的命名:MARS(Monitoring Analysis and Reporting System)，虽然在网络的一小角，却能掌控所有设备情况!

这是一台很了不起的设备!可能会有人觉得各个部份都已有设备进行相关阻挡了!我干麻花大钱来做 Report 呢?

让我们先了解它需做到什么样的功能，第一个就是收 log 的功能，它需要将各设备的讯息收进在一起，Switch,Router,IPS,Firewall,viruswall…，我们必需相信，不可能环境内所有设备都是同一家品牌，所以一定要支持各式阿狗阿猫的牌子!
第二个功能是出 Report，将所有设备的讯息信息串连在一起，做出各式各个阶层或部门看的 Report。较进阶的设备还可做到第三个功能，可以协同防御!!判断威胁在哪里，直接可以对各网络设备、资安设备下达合适的防御指令或政策。

这台设备通常价位相当高!原因是他需要大量的 support(各家厂牌)，除此之外，还需要精确的分析判断、并组织各设备回报讯息什么是误判?什么是威胁?并实时通知相关人员，且建议合适的作法。

。上网行为管理:

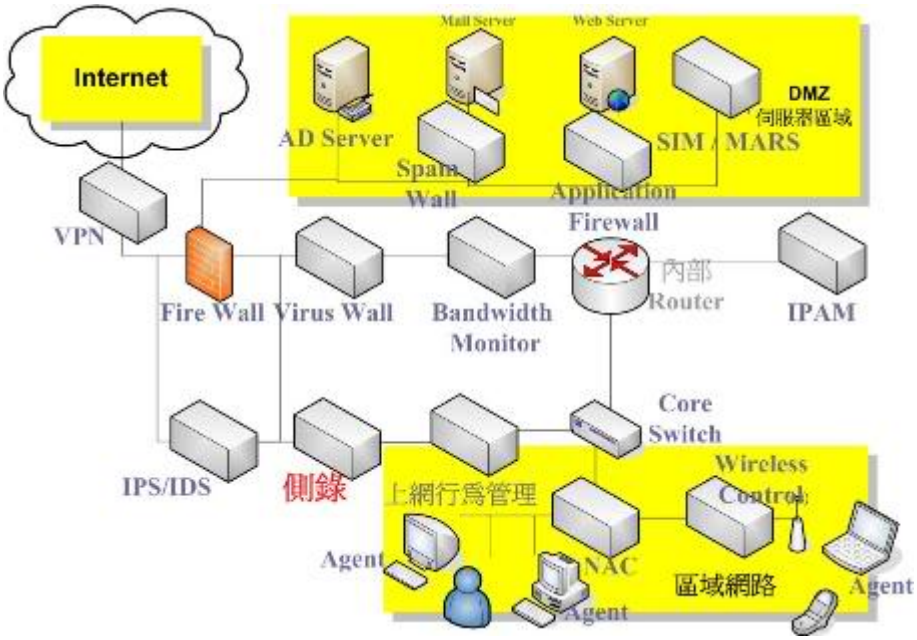


上网行为管理设备在配置上有两种方式，Inline Mode(配置在 GateWay)或是 MirrorMode(配置在 CoreSwitch)，上图是从 CoreSwitch 直接 Mirror 流量的方式，两种方式各有优缺，从 Gateway 在进行阻挡时较快且直接!但设备挂掉时要考虑 hardware bypass 的功力!而 Mirror 好处是完全不改变原有架构导入很容易，但是在进行阻挡时，需同时送封包给远方目的 server 与来源 client 联机，网络频宽资源较吃!到底哪个好，还是依环境而定。

这个设备的主要功能就是要看内部使用者的上网情况，进而进行管理。比如结合内部 AD

Server 之后，可以管制爱搞鬼的 RD 部门不能用 P2P、苦闷的工程部不能上色情类网站、爱事非的会计部们不能开 IM 聊天…。也有公司应用 AD 身份验证功能，没有登入 AD 就没有网络可用^^(真是厉害呀)

。侧录:

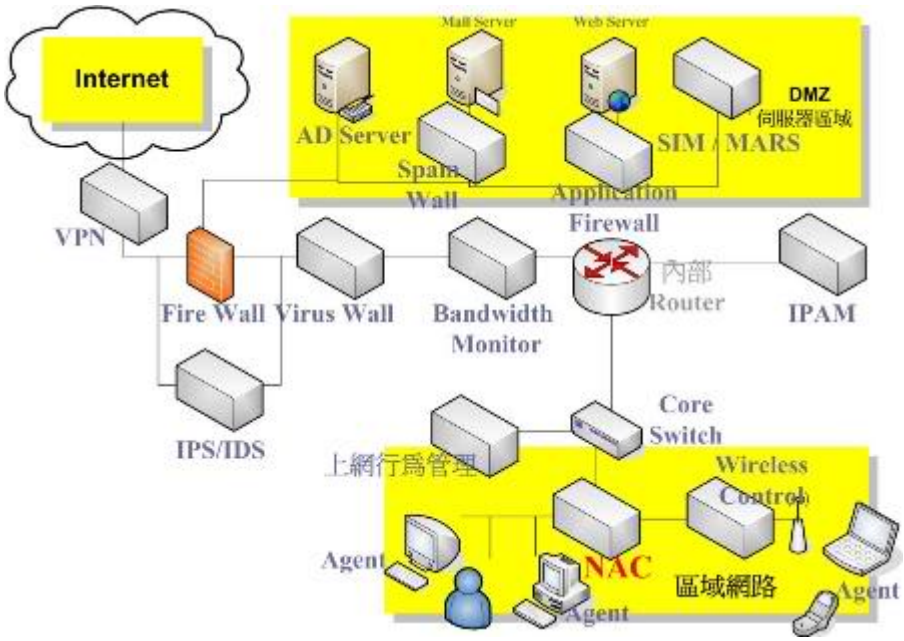


侧录的概念就像你家附近、或银行内的监视系统，将看的见的事情一一记录。这包括了你信箱内的内容、你的聊天记录、你上过哪些网站、抓了哪些图片、即使是 FTP 的档案，全部都能一一还原，全部重现!!

也由于要对全部数据、流量、封包，对储存系统是很大的负担!录的愈多，备份的时间就愈短。所以实务上会将侧录设备装置如上图，可能是从 IPS 过滤封包后，从 IPS 强力的封包比对能力后，挑选只想侧录的封包内容，如只录 Web 流量、或只录 FTP 流量。另一种方式是从上网行为管理设备上，得知某个 ip 或是某个使用者老是在看色情网，嘿~就来把它上的过程全录下吧!!我们也常开玩笑，如果 MIS 知道公司内谁是股市好手，可以跟着下单!哈~

当然!这也牵涉到了隐私权的问题，导入时常需与公司政策搭配。

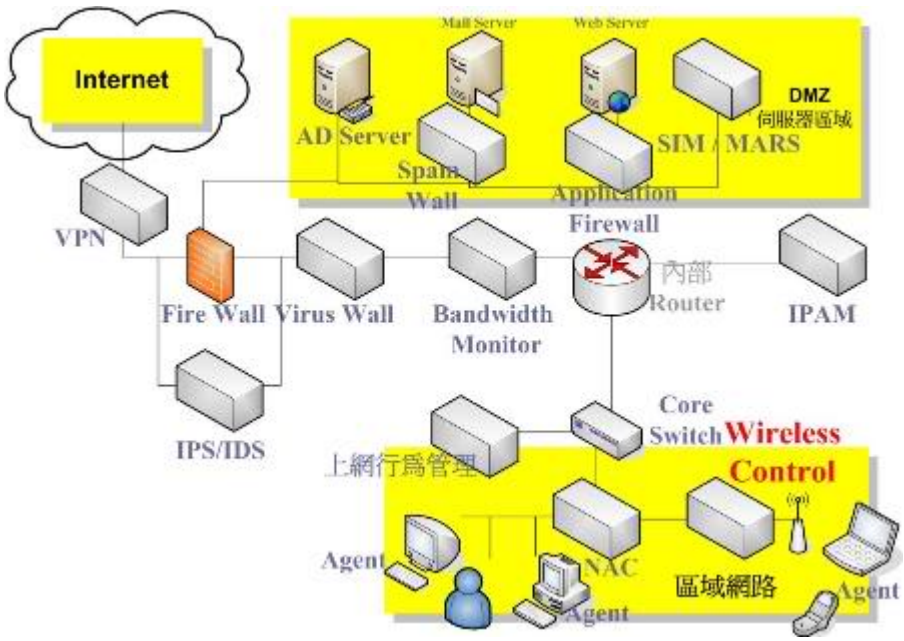
。NAC:



NAC(Network Access Control)网络存取控制设备，通常设置在 Gateway 与 client 的交界处，目的是让所有从 Client 进来的设备，想存取其上方的网络时，都要经过它的允许(可能是结合 AD 的认证或是网页验证)，这就是最原始 NAC 在做的事。

随着市场的发展，通常还需外加新的功能，才能让客户接受。需拥有可以保护 client 端的能力，本身可以上一些 patch 让 client 来更新，如 Windows 的更新 patch、或是某些防毒软件的 patch，以保设 End User 的安全，进而保护整个网络。呵~我猜想未来可会看到类似的新名词，叫 CAP(Client Access Protect)。

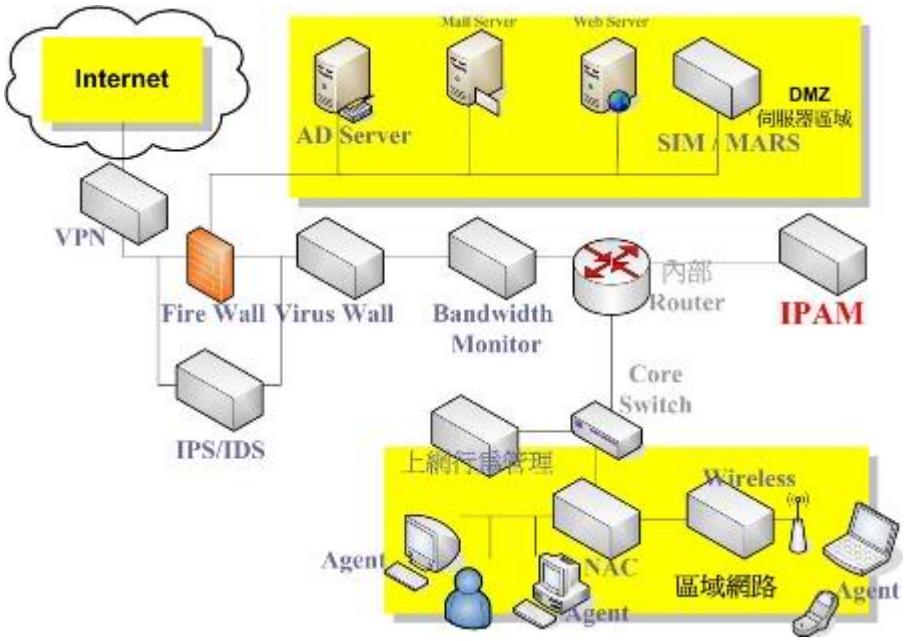
。Wireless Control:



对于无线的管理可能是许多人的痛，这种设备的目的就是要掌控你领空的封包流量。

可能做法有许多种，我仅以我碰过的例子说明。在 ServerGroup 找一台 Server 安装主控端软件，再于想侦测的边界点放置 Sensor，比如在公司的楼的三个点摆了三个 Sensor，再搭配 goolge map 抓下公司的卫星图，再给予适当的比例尺寸后，可以在 Server 上看见，在地图的什么地方有什么样的无线讯号、讯号强弱、SSID…等相关信息，要终止其与 AP 联机时，只需各送出一个 reset 封包即可，真是屌呀!(不过价位不低~呵~)

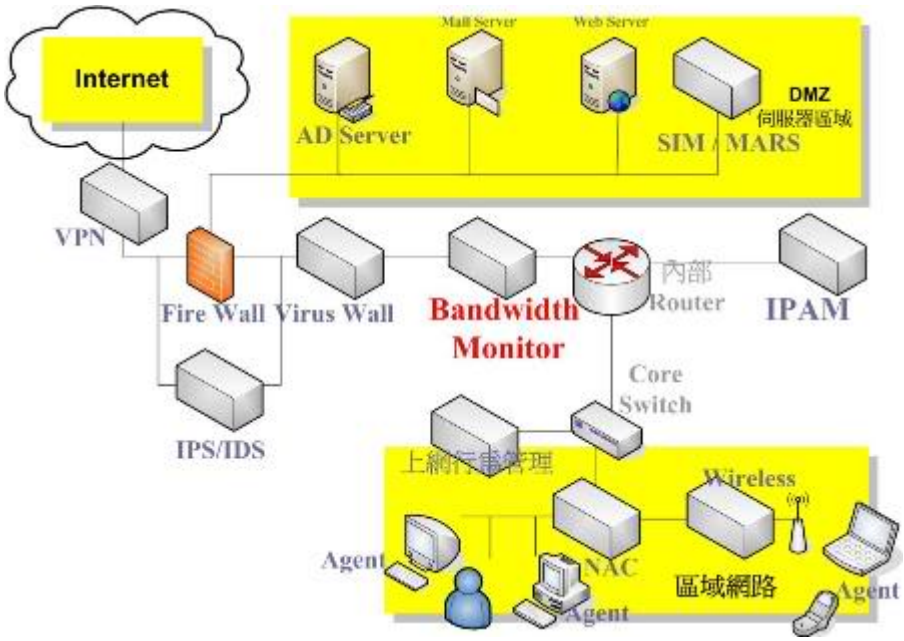
。IPAM:



对于一些环境较大，需要动态的让 user 使用网络资源，或是…或是 MIS 太懒，使用 DHCP 环境时，要管理动态 IP 是哪一台计算机在用、或是哪一个人在用，这就是很棒的解决方法。

IPAM(IP Analysis Management) IP 分析管理设备，提供 DHCP 环境内，Mac 与 IP 存取的列表，当环境中有 AD 或是 RADIUS 时，可以看见的记录将是:
时间-Mac-IP-User
资料表的关链可以让管理者快速追纵谁在用这个 IP，所以设备中也常将环境中的 DNS Server、DHCP Server 整合在一起，加强信息的连贯性。

。Bandwidth Monitor:

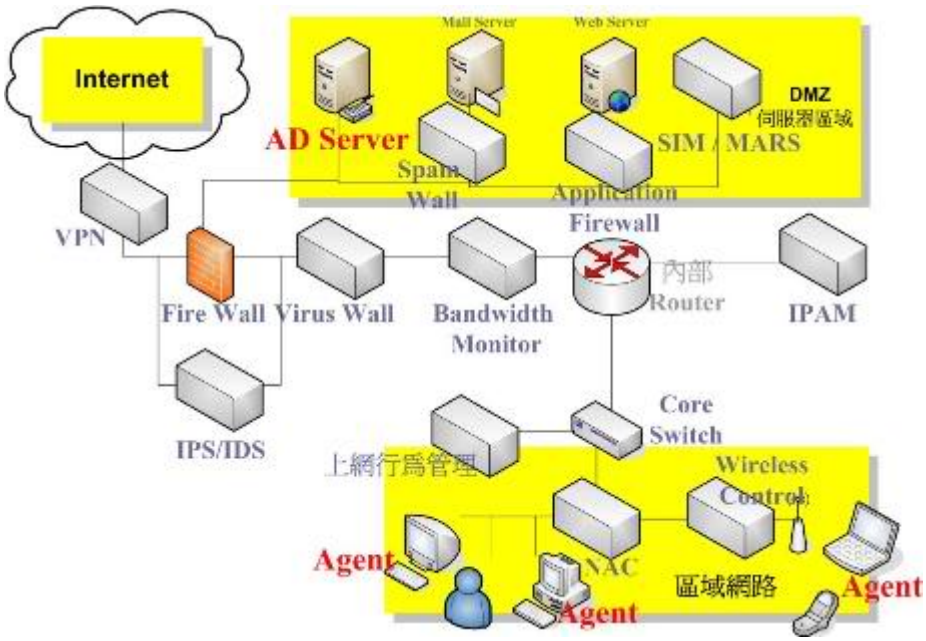


你可以试着问 MIS，我们环境平常的流量大概是多少?时常得到不知道怎么测之类的答案。BandwidthMonitor 这项设备的功能就是提供 MIS 所有网络环境的频宽使用量。

由于专攻频宽使用量的分析，可以细致到如:
总频宽使用量、各软件使用量、各 ip 使用量、单独 ip 频宽用量、单独 ip 软件使用量、protocol 的流量、User 名称的使用量、群组的使用量、Domain 的使用量。

对于 MIS 分析网络的频宽都被谁占据、或什么软件用掉，很有帮助。

。软件:



使用软件来进行资安设备管理，主要是因为一些封包到了应用层，还是要靠操作系统、与应用程序来分析，才有办法进行管理与分析或保护;另一个原因是 EndUser 的使用状况永远无法掌握，透过如资产管理软件。

一般常见的资安软件如 DRM，用来对环境内的特定文件进行加密，比如公司专门设计 CAD 的图档，每张图都是公司的心血，这时需要的就是将这些图档全部加密以保护公司信息外泄的可能。在布属上需一台 Server，再利用如 AD 套用 GPO 将数据布到登入网域的计算机上，未来只要 user 一开启要加密的档案格式就直接加密!!

另一个常见的软件是资产管理软件，常 Agent 布属在 Client 端计算机后，Agent 会自动收集所有计算机上的软、硬件信息，再回传给资产软件 Server 端，这是最初的资产软件所做的事，可以统整资料进行环境内的软、硬件资产管理。
喜爱掌控所有信息的 MIS 提出了需求，能了解 user 端所有东西，有没有可能对这些软、硬件直接进行控制呢?是滴!产品往往因为需求而产生,所以现在的资产管理软件不仅收集客户端数据，还可直接限制 User 端的使用情况，比如只能读取 USB 不能写入、禁止上班时间打接龙，也可直接把你的计算机当自己的用。(专业一点的说法叫远程叫修功能)
所以啦~也可以直接对 user 端的桌面使用情形进行录像!!真是 MIS 最爱呀!

以上的产品仅是小弟接触过的一小部份，相信科技仍有许多的可能!任何不足与错误再请大家直接指正!谢谢^^