阿姆瑞特安全网关
技术白皮书

北京阿姆瑞特软件有限公司

目 录

第一章 前 言

随着网络技术及应用的普及，网络安全问题日益凸现，黑客的攻击方式由以前基于 TCP/IP 协议的漏洞攻击转向基于操作系统和应用软件的漏洞攻击和入侵。例如：黑客可以通过防火墙开放的合法端口进入内部网络，给用户造成巨大的损失；蠕虫病毒、木马可以通过防火墙开放的合法端口进入内部网络，造成网络瘫痪；间谍软件等恶意程序可以通过防火墙开放的合法端口进入内部网络，窃取商业机密。

安全威胁不仅来自外部，企业内部的不当互联网访问、滥用互联网以及泄密行为等等，同样会带来安全问题。据 IDC 报告，70%的安全损失是由企业内部原因造成的，而不当的资源利用及员工上网行为往往是“罪魁祸首”。比如：网页浏览、BT 下载、IM 实时通信、P2P 文件共享等行为。不当的资源利用及员工上网行为带来了间谍软件、恶意程序和计算机病毒，导致了企业网络资源耗尽、机密信息泄漏、内网病毒泛滥等一系列安全问题。

同时，随着互联网的吸引力和互动性与日俱增，员工正花费越来越多的办公时间上网处理私人事务。据公布的最新统计显示，中国员工每周上班花在网上处理私人事务的时间高达 5.6 小时，平均每天超过 1 小时。有 60%的中国员工在工作时间上网浏览个人信件，有 83%中层管理人员由于在办公时间内浏览与工作无关的网站，使得企业遭受到仿冒诈骗、间谍软件和其它网上攻击的威胁增大。在中国，大约有 8%的员工在上班时间上网进入聊天室，大约有 16%的员工上网下载音乐，大约有 12%员工在上班时间玩游戏的。互联网滥用，造成工作效率下降，给中国企业带来了巨大的损失。

面对这些隐藏在 IP 数据包应用层的攻击和信息，传统的防火墙技术显得无能为力。阿姆瑞特安全网关系列产品正是在如此复杂多变的恶意攻击和网络应用下孕育而生的，该产品将防火墙、VPN、入侵检测、防病毒、内容过滤和应用控制等功能结合于一体，提供从物理层到应用层 7 层安全防护的产品。

第二章　阿姆瑞特安全网关介绍

阿姆瑞特安全网关是将防火墙、VPN、入侵检测、防病毒、内容过滤和应用控制等功能结合于一体，提供从物理层到应用层 7 层安全防护的产品。阿姆瑞特安全网关产品内部集成了专用的 ASIC 加速芯片，突破了传统安全设备在进行内容处理方面与性能的矛盾，保证网络的安全性、高效性。

2.1 阿姆瑞特 SOS 设计理念

阿姆瑞特依托强大的研发队伍，在产品设计时候提供阿姆瑞特 SOS(Service Oriented Security)-面向服务的安全设计，只有通过最先进的 SOS 设计理念开发出的产品才能具备高度灵活性、最强大的功能和最卓越的性能。依托阿姆瑞特先进的 SOS 理念，安全网关在产品设计时候，充分考虑到产品的灵活性、安全性、高性能以及扩展性，与其他厂商的安全网关相比，具有以下优点：

- **无操作系统**
  - 没有通用操作系统的漏洞
  - 不需要维护和修补任何操作系统
  - 超短的启动时间
- **最小的受攻击平面**
  - 3Mb 的系统内核比 40Mb 的 Linux 和 70Mb Windows 系统小很多
  - 没有硬盘等需要运转的部件
  - 优异的 MTBF（平均无故障时间）
- **细粒度的灵活服务组合**
  - 能够精确地为不同客户量身定制合适的服务组合
  - 能提供最灵活的接入模式
- **完全自己开发的核心程序**
  - 自己开发的核心系统，包括 IP 栈、TCP 栈、过滤栈等等
  - 没有笨拙的修改和变通，只有优美的、彻底的集成全面和无缝隙的功能整合

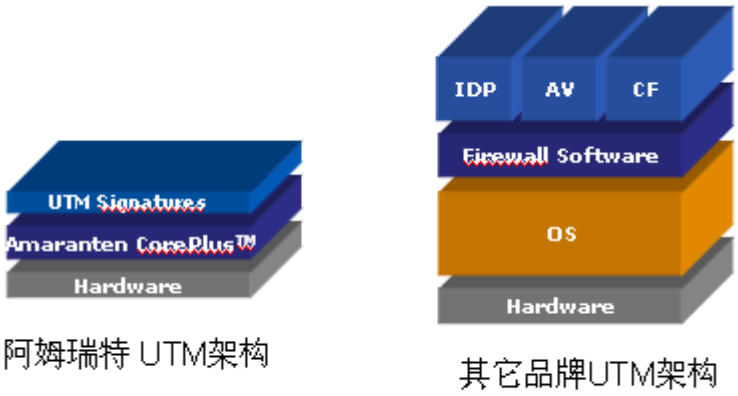
- 优异的可靠性和稳定性
- 可以提供海量的并发、极高的吞吐量和极底的延时

巧妙的结合软件和硬件

- 在必须保证性能的地方使用硬件。硬件可以提供极高的吞吐量和极短的时延，因此保证了产品整体的高性能
- 在需要灵活处理的方面用软件来实现。软件模块更为容易升级和修改，因此可以实现较为复杂的功能。

灵活简单的无缝扩展

- 通过许可证的方式，瞬间升级新需要的功能
- 在同一产品系列中，不需要更换硬件，就可以瞬间扩展到更高的性能



产品架构比较图

2.2 阿姆瑞特安全网关组件

基于 SOS 理念的阿姆瑞特安全网关通过 ASIC 加速，突破了传统安全设备在进行内容处理方面与性能的矛盾，保证网络的安全性、高效性，完成了众多安全产品才能达到的防护作用。而且减少了以前多台设备串连到网络中而引起的“一台设备有问题，网络就中断”的隐患。同时更加便于管理与配置。

阿姆瑞特的全中文、图形化的管理器可以对安全网关设备进行全面管理，构成一个安全统一管理平台。通过合理的配置将各种各样的网络安全威胁消弭于无形之中，以达到防患于未然的目标。

概括地说，阿姆瑞特安全网关产品提供六大关键安全应用。

- 防火墙，从网络层对用户进行保护，实现访问控制、路由、NAT、带宽管理等功能。
- VPN 网关，建立 VPN 隧道，确保与“外部移动用户”、远程传输以及远程办公点的安全。
- 入侵检测，从应用层针对用户进行保护。防御黑客基于操作系统和应用程序漏洞的攻击，预防恶意的网络流量到达服务器。同时对内网用户的 P2P 应用进行控制。
- 防病毒，预防网络边界上流入的病毒和间谍、木马程序，提高计算机桌面安全，预防内部计算机遭到来自企业网络外的病毒感染和木马的损坏。
- 内容过滤，对用户访问的内容过滤提供了细粒度的、基于策略的控制能力，防止违反企业规定的内容通过企业网络出入，防止员工访问违反企业规定的网站。
- 应用控制，提供了高级的、能进行深入分析的应用程序数据控制能力。可以识别即时消息工具和 P2P 应用程序，并控制对一些无益的应用程序的使用。

2.2.1 防火墙组件

防火墙是网络安全的基础。阿姆瑞特安全网关 防火墙组件秉承阿姆瑞特 F 系列防火墙的优良特性，具有强大的路由功能、带宽管理功能、抵御 DOS/DDOS 攻击等特性；具有非凡的性能和 NAT 能力；具有海量的并发连接数。该组件功能如下：

- 强大的抗 DOS/DDOS 攻击能力和灵活的访问控制；
- 专业的带宽管理功能。
- 支持 PBR（Policy Based Routing，基于策略的路由），配置主路由表和多个 PBR 路由表，不同的规则采用不同的路由表，支持多个缺省网关；
- 支持静态地址/DHCP/ADSL/xDSL 等多种网络接入；
- 支持多个出口、链路备份；
- 支持静态路由备份，支持浮动路由；
- 支持 OSPF V2 动态路由；
- 支持虚拟路由器/系统；
- 全面支持 802.1Q；
- 透明、路由、混合接入；
- 同一接口下的透明+NAT；
- 源地址、目标地址同时转换；
- 对称式接口设计，多 DMZ 区保护；
- 支持服务器负载均衡；
- 支持用户认证和账号计费；
- 支持 H.323/FTP 等动态端口协议；

2.2.2 VPN 组件

阿姆瑞特安全网关的 VPN 组件提供强大的 VPN 功能，支持点对点 VPN、全网状 VPN 连接和星形 VPN 连接；支持 VPN 客户端；支持多种加密算法和认证算法；支持 IPSEC/PPTP/L2TP 等多种 VPN 隧道方式。具体的技术特点如下：

- 支持 NAT 访问互联网的同时与分（总）公司之间建立 VPN 隧道；

- 支持 VPN 明密结合，灵活网络部署；
- 支持点对点连接和全网状 VPN 连接 ；
- 支持星型拓扑 VPN 接入；
- 动态 IP 地址的 VPN 接入；
- 支持 VPN 的 NAT 穿越；
- 支持 PPTP/L2TP/IPSEC 等多种 VPN 形式；
- 支持 2 台安全网关之间建立多条 VPN 隧道；
- 支持多条 VPN 链路的备份；
- 支持 X.509 证书和共享密钥，支持第三方 CA 认证；
- 支持 AES、DES、3DEC、cast128、blowfish、Twofish 等加密算法；
- 支持 MD5、SHA-1 认证算法；
- 采用 IPSec 国际标准协议，提供传输方式和隧道方式建立 VPN 隧道；
- 可以与第三方支持 IPSEC 协议的产品建立 VPN 隧道 ；
- 可以做 VPN 的访问控制；
- VPN 带宽的 QOS 保证；
- VPN 隧道内传输内容的 QOS 保证。

2.2.3 入侵检测组件

阿姆瑞特安全网关 入侵检测组件提供从网络层到应用层的保护，防御黑客基于操作系统和应用程序漏洞的攻击，预防恶意的网络流量到达服务器。同时对内网用户的 P2P 应用进行控制。具体的技术特点如下：

- 灵活的 IPS 与 IDS 组合；
- 动态 IPS/IDS/应用控制配置界面；
- 阻止黑客对网络上的主机进行端口探测、漏洞扫描以及其它攻击活动；
- 阻止黑客对 Windows、Unix、Linux、FreeBSD 等操作系统漏洞的攻击；
- 阻止黑客对 DNS、FTP、ICMP、IMAP、POP3、SNMP 等协议弱点的攻击；
- 阻止黑客对应用程序攻击，例如：对 WEB 页面中嵌入数据库进行的 SQL 注入攻击、针对某种应用软件漏洞的攻击等；

- 发现扫描或者攻击后，动态添加攻击黑名单；
- 对内部用户通过 MSN 等聊天工具在工作时间聊天进行阻断；
- 对内网用户通过 P2P 工具下载而耗费网络大量带宽进行阻断；
- 遍及全球的 IPS 引擎确保用户随时都能得到最新的 IPS 特征库；
- 支持用户自定义特征库，管理人员可以添加针对于其自身某种特殊应用的威胁特征库；
- 专用 ASIC 芯片防止 IPS 对应用层的控制所引起的性能降低，在进行深度检查的同时确保最大化吞吐量，确保用户的网络安全高效。

2.2.4 病毒防护组件

阿姆瑞特安全网关病毒防护组件内部集成了全球顶级防病毒厂商卡巴斯基的病毒特征库。可以对进出网络的电子邮件进行防病毒保护提供 WEB 防病毒保护，探测并阻止电子邮件与其它网络方式传输的病毒。凭借多元化的探测方法和强悍卡巴斯基病毒标识的数据库，保证其高度的精确性。通过 ASIC 加速卡保证卓越的性能。 具体技术特点如下：

- 扫描通过 SMTP 所携带的电子邮件附件；
- 扫描 WEB 电子邮件服务下载的邮件和通过 HTTP 和 FTP 从浏览器上下载的文件；
- 支持递归扫描，对压缩文档进行解压后病毒扫描；
- 智能的规则能够选择最快的监测机制或将每种文件类型与机制相结合；
- 对扫描文件的大小、平行扫描的文件数量、以及病毒扫描的内存容量都没有限制；
- 全球病毒实时病毒库更新服务器可以确保您的病毒库保持最新；
- 采用硬件 ASIC 技术，保证设备的整体性能。

2.2.5 内容过滤组件

阿姆瑞特在全球部署了网站内容分析探测器，可以实时对互联网上所有页面进行分类，精细的 URL 分类方法保证了对问题网址分类的精确性和全面性。依托强大的 URL 数据库系统，阿姆瑞特安全网关内容过滤组件可以轻松的对内网

用户访问互联网资源进行控制。同时，安全网关设备还支持动态 URL 缓存，对于用户访问过的 URL，记录在 URL 缓存中。这样当来自于内网的数据包到达安全网关设备时，首先匹配 URL 缓存中的数据，如果没有匹配再到数据库进行查询，从而最大可能的保证网络应用的高效性。阿姆瑞特安全网关内容过滤组件具体技术特点如下：

- 全球化网站内容分析探测器，进行 URL 精确分类。例如：游戏、赌博、购物、运动、色情、非法社团等；
- 人工智能对 web 站点进行分类；
- URL 动态缓存功能；
- “审计模式”功能，可以帮助企业对目前的网络应用分类，得出图表化的结果；
- 支持用户自己定义黑名单和白名单；
- 监视非业务性的网上活动；
- 管理非业务性的文件下载；
- 控制色情和非法的 Internet 内容进入工作场所，通过阻止、认证等方法来达到这一点；
- 保护用户免受间谍软件和其它恶意程序的威胁；
- 剥离网页中潜在的恶意对象，如 Java 小程序、Java 脚本/VB 脚本、ActiveX 对象和 cookie 等。

2.2.6 应用控制组件

阿姆瑞特安全网关的应用程序控制组件可以对应用程序进行深入分析和控制。可以识别并控制即时消息工具和 P2P 应用程序，以及控制对一些无益的应用程序的使用。具体技术特点如下：

- 基于应用程序的带宽管理；
- 对网络应用全面管理，例如：控制哪个软件可以或者不能访问某个网络，可以确保木马程序不能发送你的敏感信息给那些不法分子；
- 对某种应用程序控制，例如：禁止内网用户玩某种网络游戏；
- 应用程序使用日志还可提供详细地的统计信息；

- 硬件加速，确保网络整体性能。

第三章　阿姆瑞特安全网关技术特点

3.1 最灵活的接入模式

阿姆瑞特安全网关设备提供世界上类似产品最灵活的接入模式，无论安全网关工作在任何模式下，都支持该产品的所有功能。例如，当安全网关产品工作在透明模式下，仍然支持 NAT、VLAN、VPN、OSPF、HA 和虚拟防火墙等功能。

- 支持透明、路由、混合接入；
- 阿姆瑞特安全网关支持同一接口下的透明+NAT；
- 阿姆瑞特安全网关支持源地址、目标地址同时转换；
- 网络接口对称式接口设计，可以作多个内网、外网、DMZ 区；
- 阿姆瑞特安全网关支持 ADSL、DHCP Client、固定 IP 地址接入，支持多条 ADSL 线路拨号，支持 ADSL 按需拨号。
- 阿姆瑞特安全网关支持服务器负载均衡；
- 阿姆瑞特安全网关支持单链路多网关接入。

3.2 强大的路由功能

阿姆瑞特安全网关提供非常强大的路由功能，同时具有非常灵活的 SFP 接口模块，在很多情况下可以替代路由器直接将安全网关设备放置于 ISP 与用户的核心交换之间，节省一个高端路由器，从而为用户节省网络投资。

- 最大支持 4096 条静态路由；
- 策略路由功能。可以根据源地址、目标地址、服务、时间等定义策略路由，同时，可以对数据包向前、返回的方向进行选择策略路由选择。
- 路由备份功能。安全网关可以支持路由备份功能，这样可以保证不会因为一条链路的中断而造成业务的中断。
- 动态路由功能。支持 RFC 1538 和 RFC 2328 定义的 2 中 OSPF 版本；安全网关设备在透明、路由模式下都可以参与 OSPF 运算；支持在 VPN 网络环境下也支持 OSPF 协议的运行。
- 支持虚拟路由器功能。物理上的一台设备，逻辑上可以作多台使用。

3.3 专业的带宽管理

阿姆瑞特安全网关设备的带宽管理功能可以于专业的带宽管理设备去媲美，依托强大的带宽管理功能，为用户提高最合理的网络带宽应用。

- 带宽管理基于“管道”设置，管道数量没有限制，支持多层管道嵌套；
- 可对上传和下载数据分别进行带宽管理，上传和下载的带宽可设置不同带宽；
- 带宽管理设置可以 BPS 或者 PPS，设置精度为 1Kbps 或者 1PPS；
- 基于接口、用户、VLAN、IP 地址、服务、时间等设定带宽限制、带宽保证；
- 动态进行源地址、源网络、目标地址、目标网络、服务等带宽均衡；
- 动态对网络中每一个用户进行统一的带宽限制、带宽保证；
- 支持每个用户每秒新建连接数量进行控制，当阀值被触动后，动态将非法用户添加到黑名单里，直接将非法用户连接进行阻断，并且可以灵活的设置控制黑名单有效时间；
- 大差别带宽管理时，仍然可以进行预定的带宽分配，不会产生大带宽“吃饱”，小带宽“饿死”现象 。

3.4 高可靠性

为了保证网络的高可用性与高可靠性，阿姆瑞特安全网关提供了高可靠连接功能，即在同一个网络节点使用两个配置相同的安全网关设备。当一台安全网关发生意外宕机、链路故障、硬件故障等情况时，另一台安全网关自动切换工作状态，从而保证了网络的正常使用。

- 阿姆瑞特安全网关支持双机热备、链路备份功能；
- 阿姆瑞特安全网关支持不同型号的安全网关设备可以作双机热备、链路备份；
- 支持双机热备、链路备份切换的时间不超过 1 秒；
- 支持状态表同步，双机热备反复切换对应用不产生影响；
- 采用虚拟 IP、虚拟 MAC 技术，切换后安全网关设备周边设备 ARP 列表不变，保证平滑切换；

3.5 灵活的用户认证

阿姆瑞特安全网关支持本地用户任何、CA、LDAP 和 RADIUS 多种认证模式，通过用户认证功能，可以实现对网络更有效的管理。

- 在同一台 PC 上，输入用户名和口令可以访问对应的目标网络，没有用户名和口令无法访问；
- 在同一台 PC 上，输入不同的用户名和口令可以访问不同的目标地址；
- 在同一台 PC 上，输入不同的用户名和口令可以获得不同的带宽对外访问；
- 在同一台 PC 上，分别对不同用户进行计费管理，当超出预定流量后阻断该用户所有对外的访问行为或者特定目标地址的访问行为。

3.6 强悍防火墙防护功能

阿姆瑞特安全网关产品秉承阿姆瑞特 F 系列防火墙的优良特性，具有强悍的抵御 DOS/DDOS 攻击、灵活的访问控制等特性；具有非凡的性能和 NAT 能力；具有海量的并发连接数。

- 灵活的访问控制功能。除了传统的基于地址、端口的访问控制以外，还需要支持防火墙的接口、IP 和 TCP 中的选项和用户访问文件类型进行访问控制。
- 文件类型过滤功能。阿姆瑞特安全网关对 SMTP、HTTP、FTP 协议传输的文件类型进行控制，从而提供根据严格的访问控制手段，通过严格的控制可以更加有效保证用户网络安全和有效防止病毒的扩散。
- 强悍的抵御攻击功能。为了更有效抵御 SYN-flood 攻击，在防范该攻击时候，不采用设置阈值的方法；而采用类似代理技术进行攻击防范，攻击者必须首先与防火墙建立起标准的 TCP 连接，防火墙才会再与服务器进行连接，确保服务器的安全。
- 攻击后“自愈”能力。在任何情况下，防火墙的 CPU 利用率不能到达 100％，不死机，确保攻击停止后，网络正常运行。

3.7 IPS 与 IDS 有效的统一

为了达到对服务器最佳保护，阿姆瑞特安全网关可以针对服务器同时开启IPS规则和IDS规则。IPS与IDS对应不同的特征库，当数据包进入安全网关设备，首先经过IPS检查，可以确定100％的攻击，安全网关可以对该攻击进行阻断；如果数据包疑是攻击，进行IDS检查，安全网关对该数据进行审计，从而达到IPS和IDS的统一，保证服务器的同时不会产生因为误报而将正常数据包阻断现象。同时通过硬件加速保证系统的性能。

3.8 灵活的应用控制

阿姆瑞特安全网关不但能够实现对TCP/UDP端口的控制，并且可以实现对同一端口不同应用控制的功能。当数据包通过TCP/UDP某一端口进行传输时候，阿姆瑞特安全网关可以对数据包的应用层作深度检查，达到对于应用进行控制的目的。例如：对BT这种耗费带宽的控制、对经过HTTP访问流媒体的控制、对HTTP不同命令和使用代理服务器控制；对FTP不同命令的控制、对访问数据库登陆的控制、对SMTP/POP3命令的控制、对H.323/SIP视频的控制等。

3.9 动态 IPS/IDS/应用控制配置界面

用户在进行IPS/IDS等设备管理时候，面对复杂、专业的配置可能无从下手；同时因为IPS/IDS特征库是不断升级的，而配置界面无法实现时时升级，导致动态的特征库与静态的配置界面无法对应起来。

阿姆瑞特安全网关的IPS/IDS/应用控制的配置界面来源于IDP特征库的索引，当IDP特征库升级后，由安全网关设备内核PUSH(下推)到管理器中，从而实现时时更新的IPS/IDS/应用控制的专业分组配置界面，将用户需要做的IPS/IDS/应用控制分组工作转化为由专业的厂商来做。将IPS/IDS/应用控制在配置上最大的难题彻底解决，最大程度的减少管理员的工作压力，使得配置界面更加人性化、专业化、合理化。

3.10 独特的内容过滤，反“钓鱼”功能

为了防止员工在上班时间访问与工作无关的网站，避免员工浏览不适当的网站产生相应的违法行为或者遭受间谍软件/网络钓鱼程序攻击导致企业的机密数据被窃取，企业的名誉受损。阿姆瑞特安全网关可以对各种危险网站进行阻隔。

由于互联网上各种危险网站层出不穷，用户根本无法手动更新相应的网站，阿姆瑞特在全球各个地方有专人负责对全球的URL进行分类。通过阿姆瑞特厂家对全球网页时时进行分类，安全网关产品通过在线自动更新网站列表，可以灵活的设置员工访问网页的内容，从而避免了员工在上网时候访问于工作无关的网页，增加企业的生产力；同时通过对Internet上“钓鱼”网站的分类屏蔽，阻止用户访问“钓鱼”的网站，保证员工上网的安全性。

3.11 实时病毒保护

阿姆瑞特安全网关病毒防护组件内部集成了全球顶级防病毒厂商卡巴斯基的病毒特征库，提供网关级实时病毒监控功能，能够对所有WEB、FTP和E-mail流量进行实时监控，保护网络免受病毒、木马、反钓鱼式攻击、网络蠕虫、以及其它恶意软件的危害。凭借多元化的探测方法和强悍卡巴斯基病毒标识的数据库，保证其高度的精确性。通过ASIC加速卡保证卓越的性能

3.12 零日(zero-day)安全威胁防御功能

为了能最快速度的发现互联网上的最新威胁，阿姆瑞特在全球部署可以捕获最新威胁的传感器，通过遍布全球的传感器网络不断地检测Internet上新的威胁，并将这些威胁加入到特征库中，阿姆瑞特安全网关通过遍布于全球的升级服务器在这些威胁爆发或攻击发生之前向用户提供这些威胁的特征，进行实时IPS、IDS、反病毒、应用控制、网页分类特征库的升级，从而保证用户网络免受新的攻击、现有攻击的变种和未知攻击的侵扰，提供对于最新攻击零日(zero-day)防御功能。当一个新的漏洞出现时候，由于安全网关的特征库升级速度远远快于服务器补丁的升级速度，此时可以对服务器提供最有效的零日(zero-day)防御功能，对服务器提供虚拟的补丁，在没有得到最新补丁升级时候对服务器进行提前

的保护，阻止黑客针对于服务器漏洞的攻击。

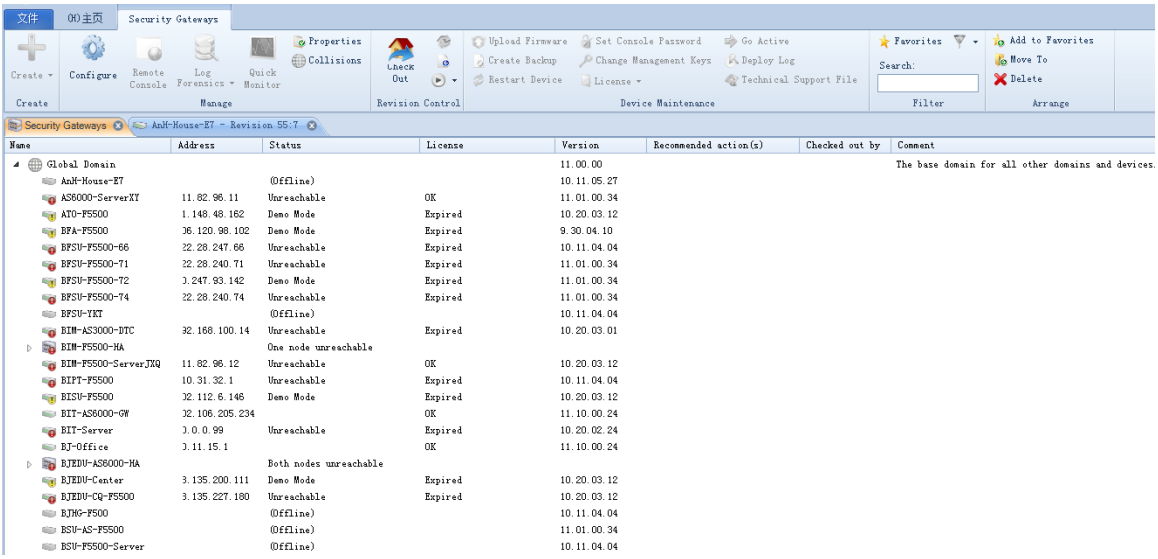
3.13 卓越的性能保证

阿姆瑞特安全网关是基于ASIC的硬件产品，对于IPS、IDS、应用控制、反病毒都有专门的ASIC芯片进行处理；对于内容过滤功能，通过本地URL Cache存储最常用的URL，用于存储最经常被请求的页面，通过缓存机制提供性能保证。通过相应的技术手段，阿姆瑞特安全网关突破了传统安全设备在进行内容处理方面与性能的矛盾，保证网络的安全性、高效性。

3.14 免费提供安全网关集中管理器

阿姆瑞特公司免费为用户提供全中文集中管理器，该管理器可以对多台安全网关进行统一的、集中的管理，方便用户在一台管理器上对多个安全网关设备的远程管理（可以管理阿姆瑞特所有型号的安全网关设备）。并且可以定义全局的服务、对象名称，提供对所有安全网关设备策略修改、上传、下载功能。这样具有共性的设置在全局配置中统一设置，每台安全网关只需定义个性的配置就可以了，从而减少规则数量、简化管理。

阿姆瑞特安全网关设备所有的管理都是通过密钥进行加密传输，而且密钥随机生成，保证了远程管理的安全性。同时我们通过在安全网关设备上定义只可以从安全网关设备的那个接口进行管理以及只可以从某一个网络甚至从某一个IP来管理安全网关设备进一步加强安全网关管理的安全性。



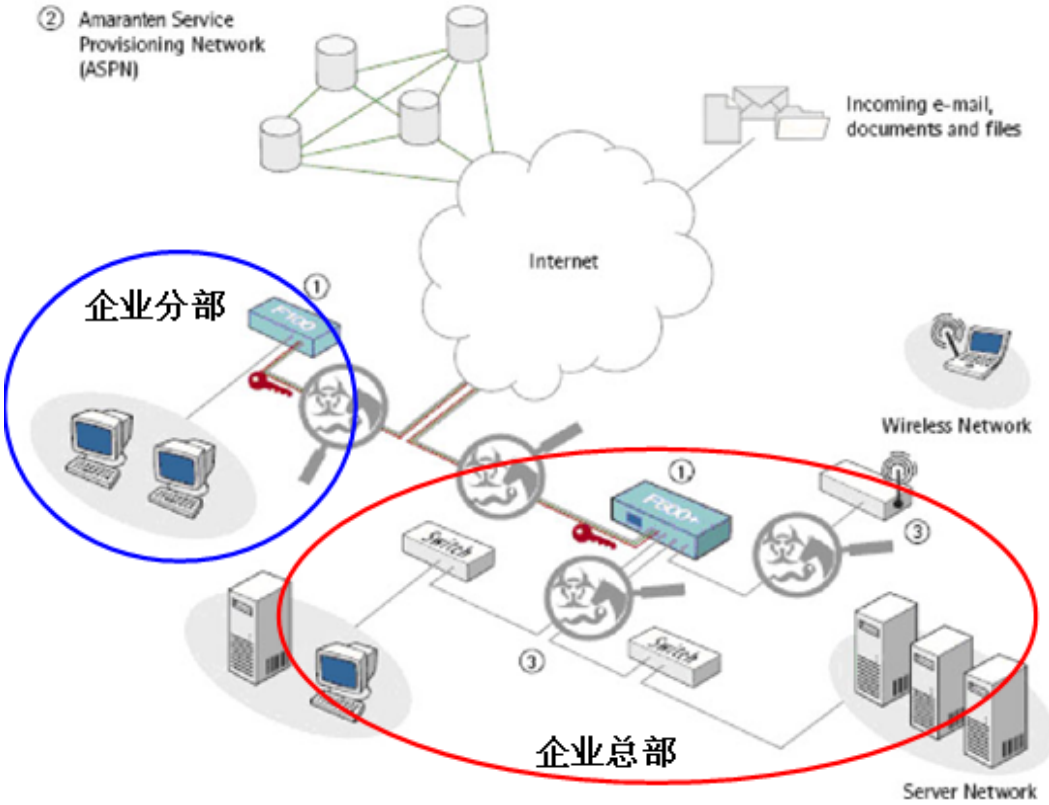
Name	Address	Status	License	Version	Recommended action(s)	Checked out by	Comment
Global Domain				11.00.00			The base domain for all other domains and devices.
AnH-House-E7		(Offline)		10.11.05.27			
AS6000-ServerXY	11.82.96.11	Unreachable	OK	11.01.00.34			
ATO-P5500	1.148.48.162	Demo Mode	Expired	10.20.03.12			
BFA-P5500	36.120.98.102	Demo Mode	Expired	9.30.04.10			
BFSU-P5500-66	22.28.247.66	Unreachable	Expired	10.11.04.04			
BFSU-P5500-71	22.28.240.71	Unreachable	Expired	11.01.00.34			
BFSU-P5500-72	3.247.93.142	Demo Mode	Expired	11.01.00.34			
BFSU-P5500-74	22.28.240.74	Unreachable	Expired	11.01.00.34			
BFSU-YKT		(Offline)		10.11.04.04			
BIM-AS3000-DTC	32.168.100.14	Unreachable	Expired	10.20.03.01			
BIM-P5500-HA		One node unreachable					
BIM-P5500-ServerJXQ	11.82.96.12	Unreachable	OK	10.20.03.12			
BIPT-P5500	10.31.32.1	Unreachable	Expired	10.11.04.04			
BISU-P5500	32.112.6.146	Demo Mode	Expired	10.20.03.12			
BIT-AS6000-GW	32.106.205.234		OK	11.10.00.24			
BIT-Server	3.0.0.99	Unreachable	Expired	10.20.02.24			
BJ-Office	3.11.15.1		OK	11.10.00.24			
BJEDU-AS6000-HA		Both nodes unreachable					
BJEDU-Center	3.135.200.111	Demo Mode	Expired	10.20.03.12			
BJEDU-CQ-P5500	3.135.227.180	Unreachable	Expired	10.20.03.12			
BJHG-P500		(Offline)		10.11.04.04			
BSU-AS-P5500		(Offline)		11.01.00.34			
BSU-P5500-Server		(Offline)		10.11.04.04			

第四章 阿姆瑞特安全网关典型应用

4.1 阿姆瑞特安全网关在企业的应用

阿姆瑞特的安全网关解决方案提供了业内最佳的入侵检测和防御、网页内容过滤、反病毒和反钓鱼功能以保护您的业务和珍贵的IT资产。该综合的解决方案特定为易于使用、维护成本低，并可以允许您随意扩展自己的网络。

下图是一个典型的企业网络，该企业的总部使用阿姆瑞特安全网关-600千兆设备，分部使用阿姆瑞特安全网关-100百兆设备。通过IPSEC协议，总部与分部建立起一条穿越Internet的隧道，用于企业内部数据交换；同时为了对企业的服务器和员工进行最好的保护，开启了IPS和防病毒规则；为了保证工作效率，开启了内容过滤功能，对员工上网进行控制。



图中标注说明：
① 高性能的扫描引擎可以保护您不受病毒、蠕虫、间谍软件、广告软件以及其它风险的威胁
② 自动地更新IDP和反病毒特征以及用于网页内容过滤的分类服务
③ 同时对内部和外部的网络数据流进行保护

总体来说，通过阿姆瑞特安全网关的部署，提高如下安全功能：

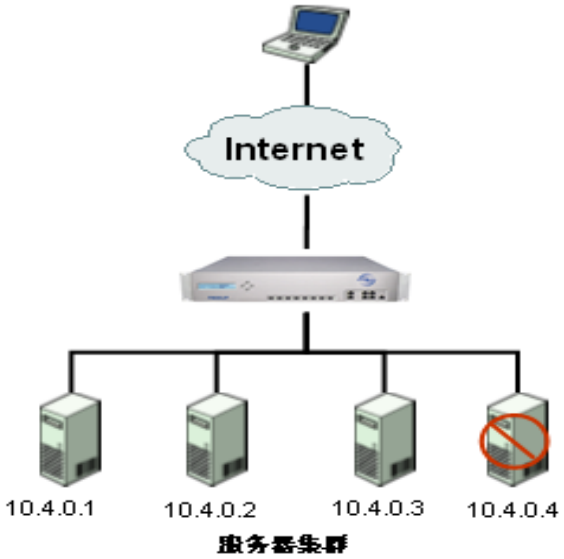
- **防火墙**：通过防火墙组件，提供强大的抵御 DOS/DDOS 功能和访问控制功能；通过接口、IP 地址、协议、端口、时间、用户等参数对数据包进行过滤，提供网络安全的第一层保障。
- **VPN 功能**：企业的总部使用阿姆瑞特安全网关-600 千兆设备，分部使用阿姆瑞特安全网关-100 百兆设备。通过 IPSEC 协议，总部与分部建立起一条穿越 Internet 的隧道，用于企业内部数据交换，通过进行数据加密，保证数据在传输过程中的安全性。
- **流量整形**：通过阿姆瑞特安全网关专业的带宽管理功能，对用户的网络进行流量整形，例如：对企业生产数据和 ERP 数据等业务性非常强服务进行带宽保证、对于员工浏览网页、FTP 下载等非生产数据进行带宽限制、对非重要部门的每一个员工进行带宽控制、以及通过 VPN 传输数据的带宽管理等。
- **入侵防御（IDP）**：阿姆瑞特安全网关内置数以千计的攻击定义，保护企业网络免受应用程序和操作系统漏洞的攻击以及蠕虫和病毒的侵扰；同时开启 P2P 限制功能，对员工聊天、BT 下载等进行控制；
- **实时的反病毒网关**：依托卡巴斯基强大的病毒特征库和基于特征和启发式的扫描阿姆瑞特安全网关可以在网关处过滤各种已知和未知病毒,提供针对未知病毒、蠕虫、特洛伊木马和其它恶意内容的高性能保护。
- **内容过滤**：网页内容过滤则为企业提供了一个管理服务，使得企业可以控制员工对 Internet 资源的访问方式，同时屏蔽互联网上恶意网站和“钓鱼”网站，最小化了恶意内容所带来的危险。通过提高生产力并降低带宽成本，它有助于帮您节约资金，同时使得您的网络更加安全。

自从该企业使用阿姆瑞特安全网关安全解决方案以来，困扰其已久的病毒、攻击、员工访问不良内容网站、BT下载等安全威胁大大减少，网络流量得以净化，带宽得到最合理的应用，企业的安全水平和工作效率得到了明显的提高。

4.2 阿姆瑞特安全网关在某大型网站中的应用

某大型网站使用4台的服务器对外提供服务，为了保证服务器的安全性同时满足使每台服务器的负载相差不大，使用阿姆瑞特安全网关作安全防护的同时，

开启安全网关设备的负载均衡功能。



该方案技术特定如下：

- IPS 与 IDS 有效统一

在该应用中，阿姆瑞特安全网关可以针对服务器同时开启IPS规则和IDS规则。IPS与IDS对应不同的特征库，当数据包进入安全网关设备，首先经过IPS检查，可以确定100%的攻击，安全网关可以对该攻击进行阻断；如果数据包疑是攻击，进行IDS检查，安全网关对该数据进行审计，从而达到IPS和IDS的统一，保证服务器的同时不会产生因为误报而将正常数据包阻断现象。同时通过硬件加速保证系统的性能。

- 动态 IPS/IDS 配置界面

阿姆瑞特安全网关的IPS/IDS的配置界面来源于IDP特征库的索引，当IDP特征库升级后，由安全网关设备内核PUSH(下推)到管理器中，从而实现时时更新的IPS/IDS的专业分组配置界面，将用户需要做的IPS/IDS分组工作转化为由专业的厂商来做。将IPS/IDS在配置上最大的难题彻底解决，最大程度的减少管理员的工作压力，使得配置界面更加人性化、专业化、合理化。

- 服务器负载均衡

阿姆瑞特安全网关智能地根据客户源IP地址、客户的网络地址、连接率等因素把所有来自Internet的访问数据流均衡地分配到每台服务器上去，既保证了每台服务器都工作在一个合适的压力之下，又保证了客户不论被连接到哪台服务

器，得到的响应速度都是相同的。

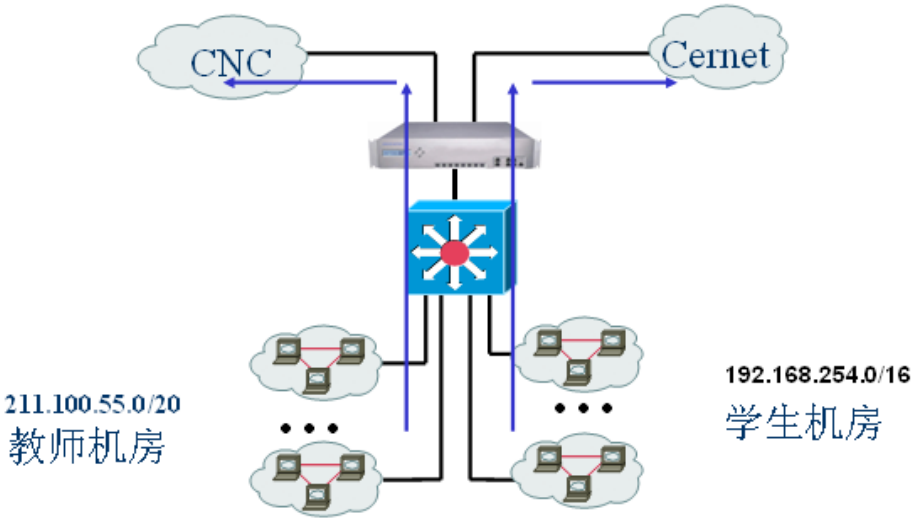
同时，利用阿姆瑞特安全网关的“服务器状态检测功能”，对每台服务器的工作状态进行检测，如果某台服务器宕机，或者响应速度较低时及时把流量向其它服务器进行分配，确保用户访问服务器在任何时候都不会中断。

4.3 阿姆瑞特安全网关在高校应用

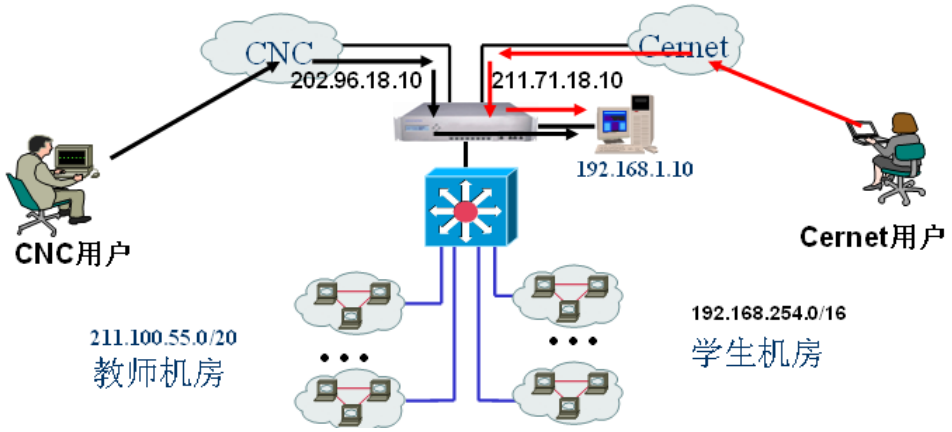
XXXX大学现有教职工总数1000多人，在校学生总数10000多人。学校的校园网络建设比较发达，网络接口到每一个学生宿舍，因此上网用户非常多，校园内共有32个合法的C类地址用于教职工网络，用1个私有的B类地址用于学生上网。校园共有两个出口——中国教育网和网通网络或者电信网络，同时该学院有大量Cernet地址的服务器对外提高服务。

阿姆瑞特安全网关具有强大的策略路由功能，可以将安全网关设备放置与核心交换机与 CNC/Cernet 之间。放置在 CNC 接入和 Cernet 接入于核心交换机之间的安全网关设备产品除了具有吞吐量、并发、NAT 能力强大的性能要求以外，该产品还需要支持基于策略的路由功能，否则无法完成接入。

通过阿姆瑞特安全网关卓越的性能保证网络正常使用；通过阿姆瑞特安全网关基于策略的路由功能，不同的数据包选择高校不同的出口；通过阿姆瑞特安全网关完善的功能保护校园网和服务器不受黑客的攻击和蠕虫的侵扰。产品部署示意图如下：



对于学校的服务器，建议放置在阿姆瑞特安全网关的 DMZ 区域，这样保证 Internet 用户和内网用户访问它的安全性。对于有多个出口的学校，在部署服务器的时候，建议在 CNC 和 Cernet 上配置对于的 IP 地址，通过阿姆瑞特安全网关的地址映射功能映射到服务器上。通过这样的部署，CNC 用户可以通过 CNC 地址访问服务器，Cernet 用户通过 Cernet 地址访问服务器，保证用户最快速度访问到服务器。安全网关设备部署示意图如下：



在高校应用中，阿姆瑞特安全网关部署策略如下：

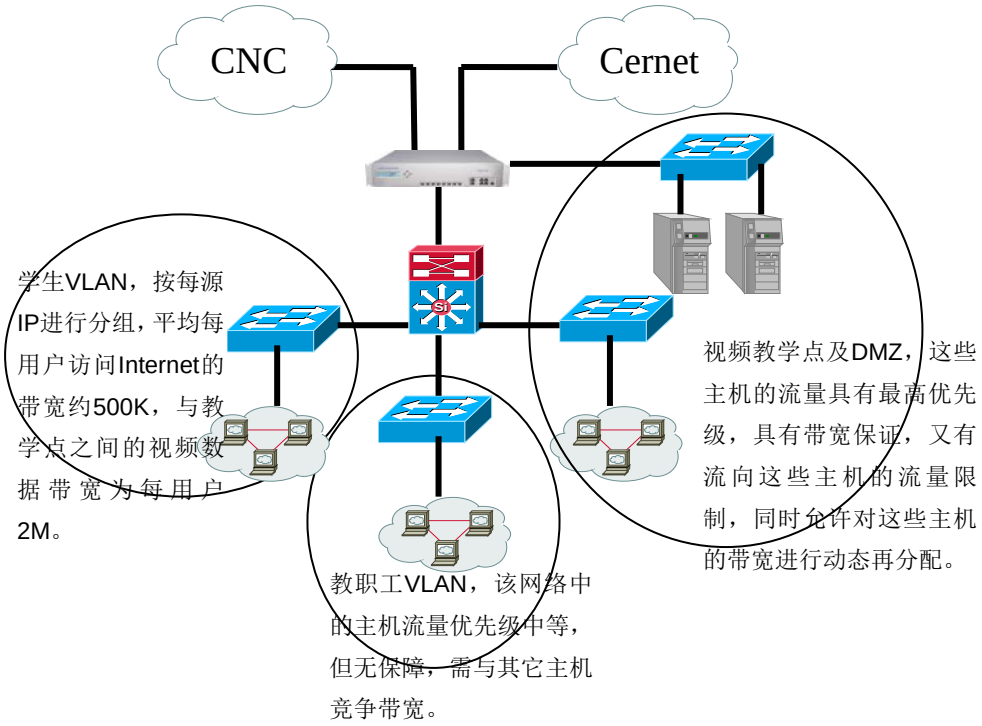
- NAT 转换，保证老师、学生上网；
- 访问控制，保证网络访问的安全性；
- 抵御黑客攻击规则，保证网络的安全性；
- 策略路由功能，保证不同地址不同出口；
- 地址映射功能，保证服务器正常对外提供服务；
- 正常情况下，CNC 用户通过访问 CNC 地址，访问到高校服务器；
- 正常情况下，Cernet 用户通过访问 Cernet 地址，访问到高校服务器；
- 访问 Internet 链路备份功能，当一台链路有问题时候，由内到外访问可以动态切换到另一台链路；
- 访问服务器链路备份功能，当一台链路有问题时候，由外到内访问服务器可以动态切换到另一台链路；
- 对于高校服务器开启 IPS/IDS 功能，保护服务器的安全
- 通过 BT 控制，限制学生通过 BT 下载耗费学校的带宽。

4.4 阿姆瑞特安全网关“流量控制”的应用

阿姆瑞特安全网关通过定义管道的方式提供 COS/QOS 功能，并且管道没有数量的限制，可以基于 IP、基于协议、基于接口、基于组信息、基于 Vlan 信息、VPN 连接等信息进行带宽管理。

在该校园网中，师生所使用的终端共计超过 1.7 万台，出口带宽 1G。启用了阿姆瑞特的流量控制功能后，对一些重要实验室、视频教学点得到了最高的优先级，具有最低 100M 的带宽保障，这使得即使在网络使用的高峰期，视频教学也可以流畅地进行。同时，对于学生访问 Internet 采用了带宽限制，有效地减轻了线路负荷。

在实际使用过程中，还开启动态带宽均衡功能，对带宽进行最合理的利用。动态带宽均衡是阿姆瑞特安全网关设备的重要亮点之一，当高优先级的业务所占带宽少的时候，它们所占的带宽便可被智能地用于其它业务传输，而一旦当重要业务再次进入活动期的时候，被其它业务所占用的带宽便又会归还给重要业务。



4.5 阿姆瑞特安全网关“内容过滤”的应用

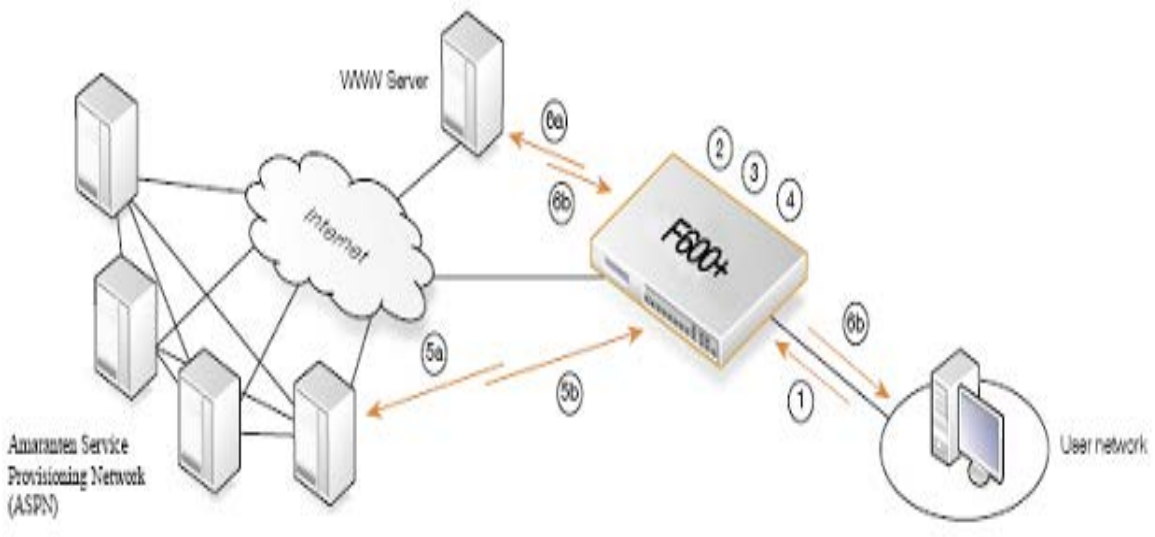
随着互联网的发展，越来越多的办公场所为员工提供了上网条件。据调查统计，2005 年全美国共有超过 6800 万员工在工作时使用互联网。然而，随着互联网的吸引力和互动性与日俱增，员工正花费越来越多的办公时间上网处理私人事务。一项新的调查统计表明，由于员工在工作时间滥用互联网，导致美国企业的损失每年高达 1780 亿美元。

那么中国的情况如何呢？据公布的最新统计显示，中国员工每周上班花在网上处理私人事务的时间高达 5.6 小时，平均每天超过 1 小时。有 60%的中国员工在工作时间上网浏览个人信件，有 83%中层管理人员由于在办公时间内浏览与工作无关的网站，使得企业有更多机会遭受到仿冒诈骗、间谍软件和其它网上攻击的威胁。在中国，约有多于其它地区 8%的员工在上班时间上网进入聊天室，约有多于拉美 16%的员工上网下载音乐，而在上班时间玩游戏的员工这个比例会比其他地区多 12%。值得注意的是，中国员工比其它地区的员工每周多花 7.6 小时的时间来使用 IM、玩游戏、P2P 软件或流动媒体。互联网滥用，给中国企业带来了巨大的损失。

据一家权威的调查机构的报告，Internet 发展之初促进了企业生产力的增长，是企业增长促动因素，或者甚至是一个工具，给予企业更大的竞争优势。但是随着互联网滥用，员工在上班时间经常浏览与工作无关的网页、网上聊天、玩网上游戏，造成生产力下降。同时，网页数据流也是安全问题的一个主要来源，同时也是滥用公司时间和资源的主要因素。不恰当的网上冲浪行为可以把您的网络暴露在众多的安全威胁之前，同时也会引起法律法规方面的问题。因此，生产能力和 Internet 带宽将被浪费。

如何有效地解决这些问题，以便提高员工的工作效率，降低企业的安全风险，减少企业的损失，成为企业迫在眉睫的紧要任务。阿姆瑞特安全网关的内容过滤功能可以有效的对员工上网行为进行管理，屏蔽与工作无关的网页和具有威胁隐患的网页、“钓鱼网页”，保证员工上网的安全性和提高企业的生产力。

阿姆瑞特安全网关“内容过滤”工作原理如下：



1. URL 请求

一名员工或用户请访问一个 URL。

2. 缓存查询

URL 被阿姆瑞特安全网关获得，并与本地缓存中的条目进行比较。

1)在缓存中找到了 URL

如果在缓存中找到了该 URL，就会立即与为该用户所指定的策进行比较并采用指定的动作（3）。

2)在缓存中没有找到 URL

如果在缓存中没有找到该 URL，就会向位于阿姆瑞特服务提供网络中的分类服务器发送一个请求（5a）。该 URL 则会被在 ASPN 数据库中 进行查找然后其类型信息就会被返回到阿姆瑞特安全网关（5b）。

3. 策略查询

在用户所请求的 URL 的分类信息被正确识别后，为该用户所指定的策略就会被执行被采取相应的动作（4）。

4. 动作

根据所请求的 URL 的分类信息以及您已经定义好的策略，一个指定的动作就会被采取。如果该 URL 属于一个被允许的分类，用户就可以继续把对该 URL 的请求发送到含有该 URL 的服务器（6a），并且其内容就会被返回给用户（6b）。如果该 URL 所属的类别不被允许，用户就会得到一个不同的响应，具体会是什

么样的响应，取决于您为该用户定义的策略。 可选的响应选项为：

- 一个管理人员可自定义的阻止页面，并不可能继续后续的访问进程。
- 一个管理人员可自定义的页面，具有策略指导消息，并有可能继续后续的访问。
- 一个管理人员可自定义的页面，该页面可以发送 URL 以进行重分类，进行重新检查。

企业通过使用阿姆瑞特安全网关“内容过滤”功能后，给企业带来的好处如下：

增加生产力

阿姆瑞特网页内容过滤使得您可以强化对网上冲浪行为的约束策略。这意味着您可以阻止与业务无关的浏览，因此可以增加您雇员的生产力。

增加安全性

通过阻止包含如可编程内容、游戏、暴力以及其它相似的网页，您也可以阻止对含有恶意内容如病毒、蠕虫和间谍软件的资源的访问。

免受钓鱼攻击

一个特别的任务组在不断地探查可以被用于进行钓鱼攻击的 Internet 内容，并可以保证这样的内容已被进行了分类，并将在下一个小时的更新时把它记入数据库。

性能保证

为了保证设备的性能，在阿姆瑞特安全网关在本地URL Cache存储最常用的URL，用于存储最经常被请求的页面，通过缓存机制提供性能保证。同时，在全球主要国家，部署URL分类服务器，以便用户通过最快的路径获得最新URL分类。