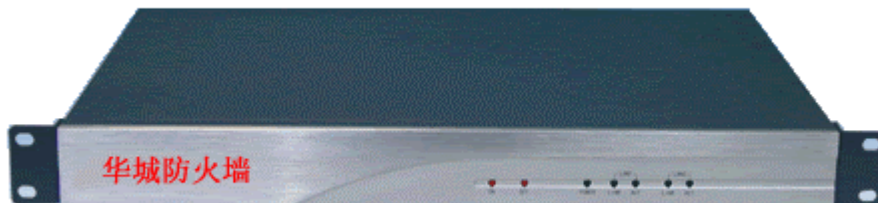


## AppRock® 300 应用防火墙

AppRock 应用防火墙可以阻止将应用行为用于恶意目的的浏览器和 HTTP 攻击。这些攻击包括利用特殊字符或通配符修改数据的数据攻击，设法得到命令串或逻辑语句的逻辑内容攻击，以及以账户、文件或主机为主要目标的目标攻击。

AppRock 应用防火墙安装在传统网络防火墙与应用服务器之间，在 ISO 模型的第七层上运行。所有的会话信息，包括上行和下行的会话信息，都要流经应用防火墙。下行请求经过应用防火墙，并且在积极模型的情况下，进行政策的解析处理。这就要求应用防火墙安装在缓存服务器的前端，以保证请求的有效性。上行请求经过只允许有效请求通过的应用防火墙，因此避免了有害请求进入服务器。应用防火墙知道解析和输出的会话请求，提供与已有应用的联机集成，并与 Web 应用技术相兼容。应用防火墙监听 80 和 443 TCP 端口，并从客户机接收输入的 HTTP/Secure HTTP 请求，然后解析这些请求，将这些请求与会话建立关系或者创建一次会话，然后将请求与会话的政策相匹配。如果这个请求符合安全策略，它就被转发给 Web 服务器，否则请求就被拒绝。



## 系统配置

项 目	AppRock-300 描述
外型尺寸 (mm) 宽×深×高	482×306×45 (mm)
重量	5kg
插槽	PCI 扩展
固定接口	1 个 RS-232 配置口 4 个以太网口

项 目	AppRock-300 描述
处理器	2.4GHz
网络吞吐量 (Mbps)	200
安全过滤带宽 (Mbps)	200
并发连接数	300000
用户数	不限制
固态存储	128MB
SDRAM	512MB
输入电压 DC	额定电压: +5V
工作环境温度	0 ~ 60°C
环境湿度	5~ 90% 不结露
抗冲击	10G 峰-峰加速度 (11ms)
抗震动	5-17Hz, 0.1" 双峰位移; 17-640Hz, 1.5G 峰-峰加速度
电磁干扰	符合 FCC/VDE A 级标准

## 功能介绍

### 主动安全

安全防护一种是寻找出所有网络流量中的攻击行为（主动安全模型），一旦发现不是这些已知的攻击行为，则认为是正常的。这种做法的思路就是构建攻击特征集，拿正常的的数据来匹配。这种做法的问题就是对于未知的攻击，毫无用处。而新攻击恰恰是能造成最大的危害。而且，特征库的挖掘、增长和维护也是非常费时费力的事情。另外一种就是对正常的网络行为建立模型，所有的网络数据拿来和正常模式匹配，如果不是这个正常范围以内，那么认为是攻击。这种做法比较符合人类的思维习惯，而且能够抵御未知的攻击。不管是在局域网中，还是访问一台互联网上的服务器，正常用户的行为是可以枚举的，而且大多情况下是雷同的，通过人工智能、神经网络技术建立其正常网络数据模型，对异常行为立即能够分别出来。

AppRock™应用防火墙使用主动安全模型实现对攻击的防护。与消极安全模型相比，主动安全模型建立正常访问规则，可以识别任何不符合正常访问规则的攻击行为，包括任何未知的攻击。而消极安全模型则是建立已知攻击特征库，来判断网络数据是否具有攻击特征，不能够防范未知和智能化的攻击手段。

## 策略动态学习

与传统网络层的安全设备安全策略的配置相比，应用防火墙的策略非常复杂。安全策略包括允许访问的网页，各种合法表单，提交变量范围等等，如果手工配置，要耗费很多时间，难以考虑周全。真实世界中的 Web 应用非常复杂，而且网站在不断的动态变化。

一个 Web 应用中很可能有上千个 URL（对于新闻、论坛等 Web 应用，这个数目很容易就超过数十万）

每个 URL 中可能含有多个变量个 SQL 查询代码

每个 Web 应用有成百上千个用户

每天都有很多 Web 设计则改变网站

每个应用使用的后台服务器都不一样

如果使用传统的配置方法，那么应用防火墙的管理员必须理解每个应用，每个网页的作用，每次提交的请求，甚至每个提交变量的范围，然后创建针对每个 URL，每个请求串，每个变量的安全规则，并且，时刻都需要根据 Web 应用的变化来改变应用防火墙上的安全规则。这些在现实中做到是非常困难的。由于存在这些问题，传统的配置方式不能够满足应用防火墙策略周全性和变化性的特点，需要应用新的方式来满足应用防火墙的安全策略配置。AppRock™ 应用防火墙实现了动态策略学习，在可信任用户与应用互动时学习合法应用逻辑，然后建立有效的针对 Web 内容交互的安全策略数据库。通过建立的安全策略数据库对应用服务器进行保护。

## 用户行为检测

为何目前部署了大量的安全产品，但是攻击却仍然存在，根本原因就是攻击是发生在人的行为层面的东西，通过键盘，数据 IO，内存，CPU，网络，才表现为网络数据，而目前所有防范工作都是在最底层的网络数据层面去判断，判断数据报文中是否具有某个攻击特征码，或者判断报文的标志是否合法等等，其难度和局限性可想而知。AppRock™应用防火墙的用户行为检测技术（UBC）从网络数据中还原出应用数据流，并在应用数据的技术上归纳用户行为，然后进行用户行为的合法性判断，从而最精确的判断出攻击行为。通过和主动安全模型结合，用户行为检测可以实现只允许发生符合正常用户行为的访问数据通过，任何异常数据都会被阻止。

## 应用攻击防护

AppRock™应用防火墙可以有效的识别和阻止下列已知的针对Web应用的攻击

- ✓ 缓冲区溢出
- ✓ Cookie 假冒
- ✓ 认证逃避理
- ✓ 非法输入
- ✓ 强制访问
- ✓ 隐藏变量篡改
- ✓ 拒绝服务攻击问
- ✓ 跨站脚本攻击
- ✓ SQL 注入

对于目前未知的攻击，AppRock™应用防火墙通过主动安全、策略动态学习和用户行为检测的功能进行防护。

## 黑白名单

AppRock™应用防火墙能够对内外部用户进行区别，并且进一步把内部用户分为可信和不可信用户，分别设置黑白名单进行管理。黑白名单能够提供更大的灵活性，适合于管理人员的工作习惯和职责分工。

## XML 配置支持

AppRock™应用防火墙使用 xml 作为标准的配置语言，用户只需要简单的配置需要保护的站点信息（域名，地址），以及用于学习安全行为策略的信任主机，即可以完成对应用防火墙的配置。由于使用标准的xml语言，能够很容易的对第三方的配置管理系统进行无缝的结合。同时，能够导入其他安全扫描工具或者分析工具生成的xml格式的策略描述文件，从而自动升级安全策略库。

下面是针对一个站点的部分配置示例：

```
<filter type="buffer">
  <rule name="Url" status="valid" description="Maximum URL Length"
length="256"/>
  <rule name="Query" status="valid" description="Maximum Query
Length" length="256"/>
  <rule name="Authorization" status="valid" description="Maximum
Authorization Length" length="256"/>
  <rule name="Cookie" status="valid" description="Maximum Cookie
Length" length="256"/>
  <rule name="Referer" status="valid" description="Maximum Referer
Length" length="256"/>
  <rule name="User-Agent" status="valid" description="Maximum
User-Agent Length" length="256"/>
</filter>
```

## 文件类型过滤

AppRock™应用防火墙能够针对提交的URL进行分析，对其中的文件类型进行过滤，避免关键的系统数据被非法窃取；同时，管理人员还可以对文件类型进行灵活定制，添加需要保护的文件类型。

## 日志管理

AppRock™应用防火墙提供多种应用日志，包括

访问日志——表示每个用户的访问记录

攻击日志——对阻断的攻击进行全面的日志记录

错误日志——对所有的出错信息进行记录

所有的日志信息以标准的 xml 格式保存，方便第三方的日志分析系统进行高层的分析处理。

## 网络安全

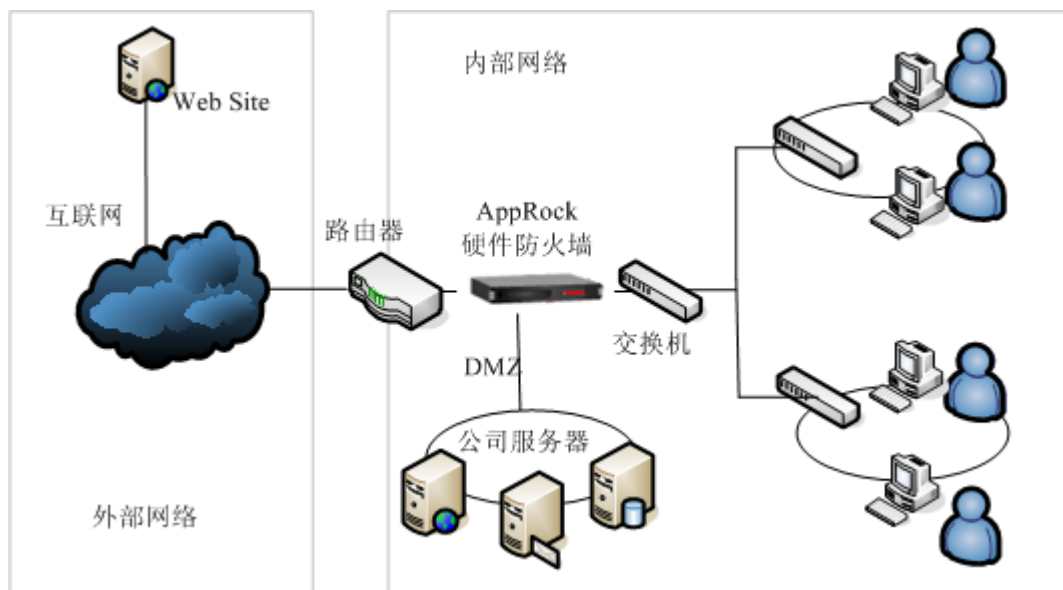
AppRock 硬件防火墙集网络接入、防火墙、VPN、流量整形、认证授权、内容安全控制、ADSL 接入安全等技术于一身的网络安全智能防御系统。AppRock 防火墙基于专门设计的硬件平台，以华城技术自行定制的安全操作系统为核心，提供高度安全、可信和健壮的安全解决方案，真正实现了单一设备对您的网络的全方位防护。它的保护机制的核心是能够提供面向动态连接防火墙功能的智能状态检测技术。智能状态检测技术虽然比较简单，但与包过滤相比，功能却更加强劲；另外，与应用层代理防火墙相比，其性能更高，扩展性更强。智能状态检测技术可以跟踪源和目的地址、传输控制协议（TCP）序列号、端口号和每个数据包的附加 TCP 标志。只有存在已确定连接关系的正确的连接时，访问才被允许通过网络防火墙。这样做，内部和外部的授权用户就可以透明地访问

企业资源，而同时保护了内部网络不会受到非授权访问的侵袭。提供了丰富的安全特性：

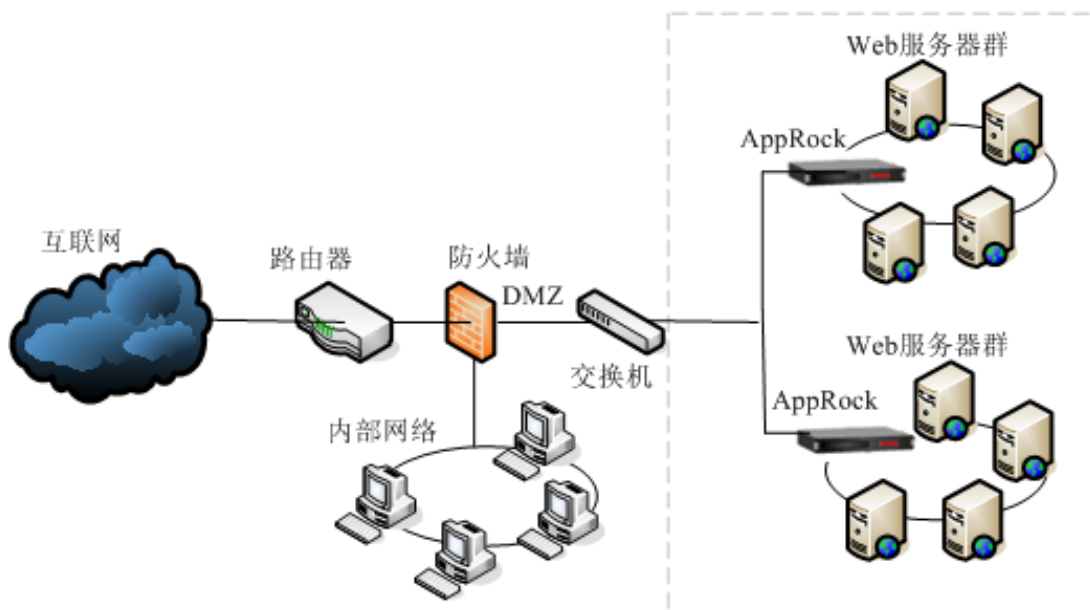
- ✓ 提供基于 IPSEC、PPTP 和 SSL 的 VPN 支持
- ✓ 状态检测包过滤技术
- ✓ 流量整形
- ✓ 支持路由模式、透明模式、NAT 模式及混合模式
- ✓ 提供透明方式的接入
- ✓ 支持 IEEE 802.1Q 的 VLAN
- ✓ 支持静态路由、RIP 动态路由、OSPF 动态路由
- ✓ 简单智能的管理方式
- ✓ 功能强大的 NAT
- ✓ 认证和授权
- ✓ 接入控制和计费功能
- ✓ 强大的系统监控能力
- ✓ 基于地址对象的访问控制
- ✓ 多协议支持
- ✓ 多种接入能力

## 部署方法

这是最为普通的企业环境防火墙部署案例。利用防火墙将网络分为三个安全区域，企业内部网络，外部网络和服务器专网(DMZ 区)。内部网络一般采用私有的 IP 地址，DMZ 的服务器可以采用公网地址，也可以采用私有地址，但是需要在防火墙上做相应的地址转换来保证外部用户对服务器的正常访问。一般常用的安全策略是：外部网络不允许访问内部网络，内部网络用户可以根据不同的权限访问 Internet 资源；内部用户和外部用户只允许访问 DMZ 区指定服务器的指定服务。具体的环境如下图：



在 Web 服务器机房中，对 Web 服务器群进行应用层保护，防范网站被黑，主页篡改等应用攻击。组网如下：



通过 AppRock 的 VPN 功能，可以快速通过互联网建立 VPN 隧道，同时硬件中的安全防护功能为互连应用提供安全保障，不需要再购买其他安全设备

