产品白皮书

安全威胁

随着 web 应用的日益增多，如电子商务，交流论坛，公司网站等等都使用 web 作为应用的平台，如何保证 web 应用的安全性也成为当前日益重要、必须解决的问题。

由于 Web 架构在成本与应用能力方面的优势，使得越来越多的企业和机构将应用迁移到基于 Web 的基础架构。Web 服务器与 Web 应用已经从最初提供简单的静态内容演变到提供丰富的动态内容。现在，Web 服务器与应用除了可以创建动态页面和启动应用程序外，还可以同数据库进行通信以生成对用户有用的内容。大多数 Web 服务器平台都将应用程序与服务器捆绑在一起，这些都为攻击提供了机会。要构建安全的 Web 应用平台，Web 设计人员必须在 Web 应用的每个层面精心设计安全性。运行 Web 应用的服务器也必须不断更新。但是，许多企业在设计 Web 应用时，Web 设计人员并未全面考虑安全性。更糟的是，有的用户只为 Web 服务器中可从外部访问的那部分设计了安全性，而忽略了内部访问 Web 应用的安全性。

很多用户认为，在网络中不断部署防火墙，入侵检测系统（IDS），入侵防御系统（IPS）等设备，可以提高网络的安全性。但是为何基于应用的攻击事件仍然不断发生？其根本的原因在于传统的网络安全设备对于应用层的攻击防范，作用十分有限。目前的大多防火墙都是工作在网络层，通过对网络层的数据过滤（基于 TCP/IP 报文头部的 ACL）实现访问控制的功能；通过状态防火墙保证内部网络不会被外部网络非法接入。所有的处理都是在网络层，而应用层攻击的特征在网络层次上是无法检测出来的。IDS，IPS 通过使用深包检测的技术检查网络数据中的应用层流量，和攻击特征库进行匹配，从而识别出以知的网络攻击，达到对应用层攻击的防护。但是对于未知攻击，和将来才会出现的攻击，以及通过灵活编码和报文分割来实现的应用层攻击，IDS 和 IPS 同样不能有效的防护。

常见的 Web 攻击分为两类：一是利用 Web 服务器的漏洞进行攻击，如 CGI 缓冲区溢出，目录遍历漏洞利用等攻击；二是利用网页自身的安全漏洞进行攻击，如 SQL 注入，跨站脚本攻击等。常见的针对 Web 应用的攻击有

- ü 缓冲区溢出——攻击者利用超出缓冲区大小的请求和构造的二进制代码让服务器执行溢出堆栈中的恶意指令
- ü Cookie 假冒——精心修改 cookie 数据进行用户假冒
- ü 认证逃避——攻击者利用不安全的证书和身份管理
- ü 非法输入——在动态网页的输入中使用各种非法数据，获取服务器敏感数据
- ü 强制访问——访问未授权的网页
- ü 隐藏变量篡改——对网页中的隐藏变量进行修改，欺骗服务器程序
- ü 拒绝服务攻击——构造大量的非法请求，使 Web 服务器不能相应正常用户的访问
- ü 跨站脚本攻击——提交非法脚本，其他用户浏览时盗取用户帐号等信息
- ü SQL 注入——构造 SQL 代码让服务器执行，获取敏感数据

下面列举简单的两个攻击手段进行说明。

SQL 注入：对于和后台数据库产生交互的网页，如果没有对用户输入数据的合法性进行全面的判断，就会使应用程序存在安全隐患。用户可以在可以提交正常数据的 URL 或者表单输入框中提交一段精心构造的数据库查询代码，使后台应用执行攻击着的 SQL 代码，攻击者根据程序返回的结果，获得某些他想得知的敏感数据，如管理员密码，保密商业资料等。

跨站脚本攻击：由于网页可以包含由服务器生成的、并且由客户机浏览器解释的文本和 HTML 标记。如果不可信的内容被引入到动态页面中，则无论是网站还是客户机都没有足够的信息识别这种情况并采取保护措施。攻击者如果知道某一网站上的应用程序接收跨站点脚本的提交，他就可以在网上上提交可以完成攻击的脚本，如 JavaScript、VBScript、ActiveX、HTML 或 Flash 等内容，普通用户一旦点击了网页上这些攻击者提交的脚本，那么就会在用户客户机上执行，完成从截获帐户、更改用户设置、窃取和篡改 cookie 到虚假广告在内的种种攻击行为。

随着攻击向应用层发展，传统网络安全设备不能有效的解决目前的安全威胁，网络中的应用部署面临的安全问题必须通过一种全新设计的高性能防护应用层攻击的安全防火墙——应用防火墙来解决。应用防火墙通过执行应用会话内部

的请求来处理应用层。应用防火墙专门保护 Web 应用通信流和所有相关的应用资源免受利用 Web 协议发动的攻击。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。

产品概述

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。

AppRock 应用防火墙采用全新的体系结构和最佳的攻击检测方法实现，主要特征有：

- ü 主动安全
- ü 动态策略学习
- ü 用户行为检测
- ü 应用攻击防护
- ü 简单配置管理
- ü 应用日志分析

功能介绍

AppRock ™应用防火墙作为一款优秀的应用安全产品，可保护用户的应用系统，免受黑客及其它的恶意攻击。通过主动安全模式，仅允许有效应用流量通过，并阻止其它一切请求。另外，AppRock ™应用防火墙提供简单的网络及应用管理、完全日志记录、审计及报告等特性。

主动安全

安全防护从一开始就朝着两个方向努力着：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，拿正常的数据来匹配。实现的产品有IDS，IPS，防毒墙，杀毒软件等等。这些都是从已知的特征库进行模式匹配。这种做法的致命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

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

对于目前未知的攻击，AppRock™应用防火墙具有同样的防护作用。

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：

应用日志分析

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

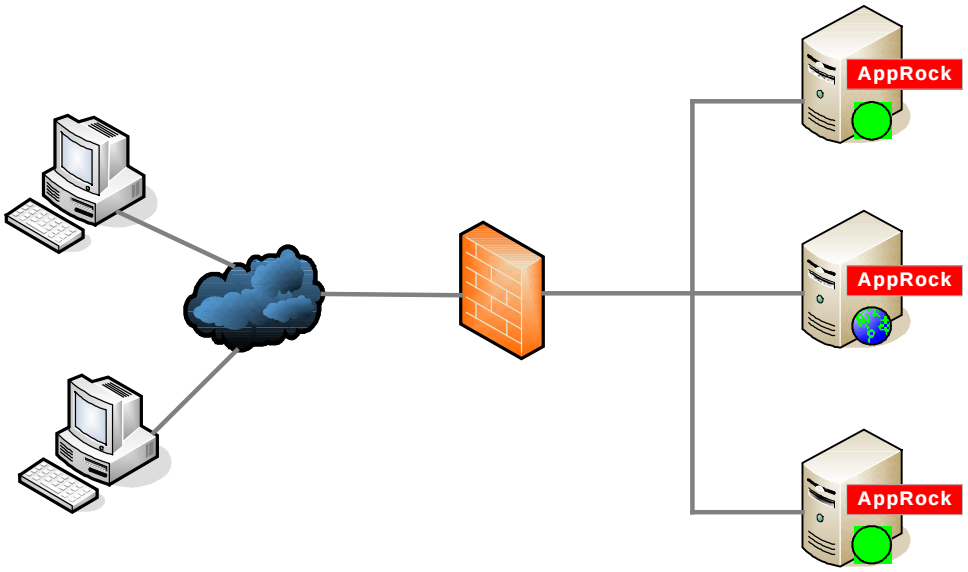
攻击日志——对阻断的攻击进行全面的日志记录

错误日志——对所有的出错信息进行记录

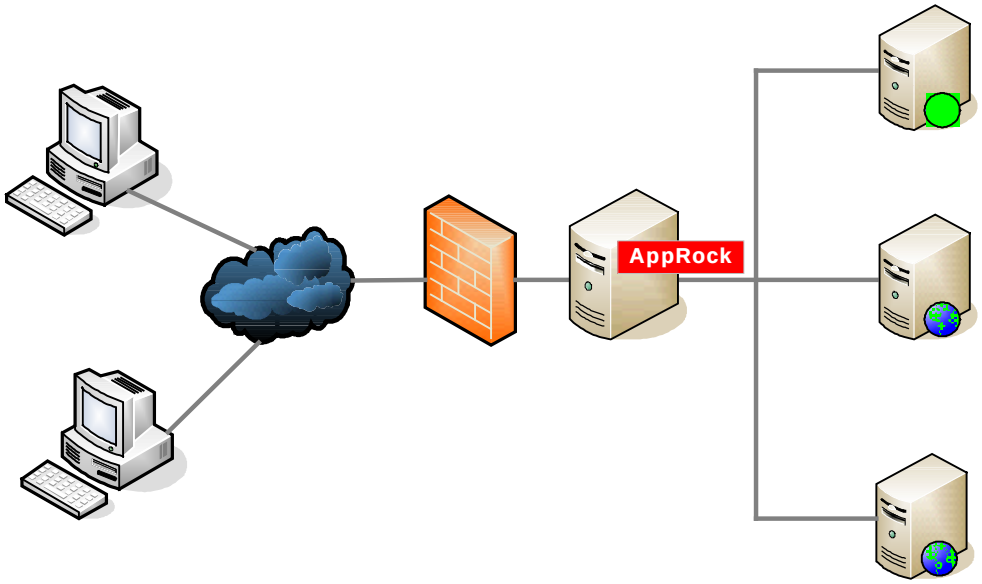
所有的日志信息以标准的 xml 格式保存，方便第三方的日志分析系统进行高层的分析处理。

部署方法

AppRock 应用防火墙可以直接安装在 WEB 服务器上，保护服务器的安全。



AppRock 应用防火墙也可以安装在单独的服务器上，保护后面的多台 WEB 应用服务器。


AppRock