

应用防火墙

概述

随着企业在 Web 应用的日益增多，客户机密数据也更容易泄漏给网络黑客或遭受身份窃贼的攻击。现在，许多身份盗窃事件的发生源于 web 应用的各种漏洞，因而这些应用受到恶意用户的攻击。基于浏览器的应用系统隧道穿透了一个企业的安全防线，使用户得以访问企业内部系统。对于大多数企业来说，Web 应用本身已经成为了安全边缘，那么唯一可确保这些应用系统安全的方法就是使用“应用防火墙”。

但是，只有将应用防火墙按应用需求量量身定制时，才可有效的发挥作用，否则将不可避免的会发生阻隔了合法用户或客户，却放进了黑客的情况。F5 的 BIG-IP Application Security Manager 是一款新型应用防火墙，可保护应用系统免受黑客及其它的恶意攻击。该设备精细的安全策略可以保护 web 应用系统及用户机密，使其免受针对应用安全的随机及目标攻击。借助突破性的技术，BIG-IP Application Security Manager 能够完全满足这些安全策略，从而适用于每一应用所需的安全状况。

挑战

今天，商业交易的各个部分都正在向 Web 中转移，但每增加一个新的基于 web 的应用系统，都会导致之前处于保护状态下的后端系统直接连接到互联网上了。随之而来的结果是，将公司的关键数据置于外界攻击之下。

同时，黑客们也正寻找新的方法来突破传统的防线。据最近的美国计算机安全协会（CSI）/美国联邦调查局（FBI）的研究表明（资料来源：计算机安全协会），在接受调查的公司中有 52% 的公司的系统遭受过外部入侵，但事实上他们中有 98% 的公司都装有防火墙。而这些攻击为 269 家受访公司带来的经济损失——包括系统入侵、滥用 web 应用系统、网页置换、盗取私人信息及拒绝服务共计超过 1.41 亿美元。

虽然传统的防火墙过去曾为阻挡非法访问公司网络做出过杰出的贡献，但现在这些功能已不能满足用户的需求。早在 2002 年，国际数据中心（IDC）就曾在报告中：“防火墙对应用层已几乎无法提供保护，因为为了确保通讯，防火墙内的端口都必需处于开放状态。”

近来，传统的防火墙提供商不断的鼓吹“应用层安全性”，声称已将入侵探测系统（IDS）与入侵防范系统（IPS）功能集成到他们的产品之中。但，事实已经证明这些解决方案效率不高，主要有以下两个基本原因：

☆ 仅依据攻击特征或其它异常用户行为来判断

这就使得系统又处于新型攻击（零日攻击）或伪装成正常流量的攻击的威胁之下。但更重要的是，对于应用系统中某一漏洞的目标攻击，他们没有任何防御能力，因为这些攻击没有明显的特征可供判断。

☆ 仅作用于网络层，而非应用层

因此，现在的网上交易要求应用系统本身要具有高度的安全性。防火墙与 IPS 系统只是查看网络上的数据包，而非对整个请求进行检查，由于缺少特定应用的相关信息，它们无法区分请求的合法性。实际上，很多设备连简单的 SSL 加密信息都无法查看。

因此，现在的网上交易要求应用系统本身要具有高度的安全性。目前流行的一些类似于应用扫描器的工具可帮助找出明显的漏洞，但每次对系统进行扫描然后再为漏洞打补丁，真是费时费力。但问题是扫描程序永远不可能查到所有的应用系统漏洞，因为太多的参数需要检查，有太多的侵入点可以攻击。开发商可以为成千上万的漏洞打补丁，但黑客只需要找到一个致命漏洞，就可以造成巨大的损失。

因此，理想的解决方案就是卸载应用系统的安全功能，交给网络设备来完成。网络设备根据提供的特定应用的相关信息可以滤出对系统的恶意访问。此类设备能够正确识别应用的流量，并阻挡其它非法流量。为了满足这种需求，一种新型安全解决方案——应用防火墙诞生了。

解决方案

F5 BIG-IP Application Security Manager 是一款独具特色的应用防火墙，能够为 web 服务器和 web 应用提供全面的保护——既可防范已知的对 web 应用系统及基础设施漏洞的攻击，也可抵御更多的恶意及目标攻击。

与从不同之处在于，BIG-IP Application Security Manager 可阻止市场中其它解决方案无法抵御的攻击。例如，两种普通的黑客技术就可直接通过目前的安全解决方案侵入系统——虽然这些解决方案宣称是实现了“应用安全”或“内容识别”阻隔：

☆ 黑客以用户的身份进入，然后修改他们的 ID 或篡改权限，以通过认证。

市场中几乎每种解决方案都无法检测到这种最为复杂的形式（动态参数篡改）。

☆ 黑客更改 Web 应用的 URL 或将其设置为书签，以便进入受到限制的访问区域。

通常，仅需将 URL 从 ../webapp/user 更改为 ../webapp/admin 即可。更常见的情况是，错综复杂的路径、或者路径被应用系统隐藏起来。但是，对应用了如指掌的用户一般能够猜出或检测到去向。

只有 BIG-IP Application Security Manager 能够保护系统免受针对这些漏洞的攻击，因为它是第一款对用户与防火墙的交互具有全面了解的交互安全解决方案。这意味着，它不仅对合法的活动实施精细地控制，并且对于任意特定时刻的用户环境（或状态）也具有深入的了解。不仅如此，BIG-IP Application Security Manager 的精确安全策略基于其专用的模型（称为应用流程模型），这种模型可将 Web 页面内容的自动分析与基于真实流量分析的反复调整完美结合。

应用流量模型

实施安全策略的最佳方式是，为用户与应用系统间的交互设定一个详细模型（或策略）。一旦您已定义合法活动，那么，其它活动就会被视为非法活动而被禁止访问。这样，用户活动的精确模型对于安全策略的实施便至关重要。否则，安全策略容易放入攻击或阻止用户的合法访问。

F5 的应用流程模型是对合法用户与 web 应用间交互的逻辑表述。在呈现在用户面前的每一个 web 页面中，该模型描述了由客户端网页源代码发出的 HTTP 请求及合法的跳转页面之间的结构。构建模型或策略可通过仅采用几种关键因素（以便降低复杂性），或利用非常详尽的描述（以便提高精确度），或根据所需的应用安全状态在二者之间加以选择。策略可包括以下所有或一些属性：

△ RFC 标准和请求长度限制

△ 已知对象类型

△ 已知对象名称

△ 已知参数名称

△ 已知参数值限制

△ 对象请求的流程（或顺序）

应用流量模型是应用模型技术上的一个突破，因为之前只是在扫描用户流量的基础上创建用户请求的模型。F5 公司的应用流量模型可自动“搜寻”整个应用系统，映射用户与网站间的互动流程或全部模式。除跟踪流量模式以外，可映射应用系统的能力远比之前为用户互动制定模型的方法更为精确。这种模型具有以下三点优势：

△ 脱机策略审核与分析

由于安全策略为应用的脱机模型或规划，因此可采用模板或“假设（what if）”分析对其进行审核、导出，从而逐步提高安全性。这种策略为应用的可读规划，而非仅仅为一套规则或常规表达式。

△ 灵活性

借助提供的工具，客户能够立即开始保护其应用，随着他们在已创建的策略中赢得自信，安全粒度也将逐步得以增强。

△ 精细控制

仅 BIG-IP Application Security Manager 能够在每个页面（还包括每个对象，每个对象的每个参数，每个对象参数中的每个合法值）转换时创建一个完整的逻辑结构。

采用这种模型构建的安全策略支持 BIG-IP Application Security Manager 根据 web 应用设计来验证用户与 web 应用间的互动，并支持其阻挡所有有别于这种设计的流量。

换言之，应用流程模型将问题由应用安全转变为协议执行，而此功能过去一直都是由防火墙来完成的。

应用流程模型是如何生成的

要生成一个精确的模型及限制流量的安全策略，BIG-IP Application Security Manager 可利用一切可用信息，包括页面源代码及与其相关的流量，对应用系统的表示层自动进行非常详细的审计。这要求对大量的信息进行精确的记录并设定模型。

BIG-IP Application Security Manager 之所以能利用一项创新的方法实现这一目的，主要通过以下两个步骤：

☆ 自动分析应用网页内容

BIG-IP Application Security Manager 利用脱机工具构建将要保护的应用的初始配置文件。这些工具包括，直接访问应用服务器元数据的接口以及可映射指定用户活动的完善的搜索工具。Web 页面内容，包括如 JavaScript 等动态程序代码进行分析，也使得 BIG-IP Application Security Manager “学会”应用逻辑，包括用户与 web 应用之间的所有详细互动。

☆ 循环策略调整

BIG-IP Application Security Manager 获得了 Web 页面内容的“快照”，并持续在实际流量中检查用户如何与 web 应用进行互动。对这个过程加以划分，以便自动调整至“可信赖”或预先记录的流量，或基于正常生产流量进行调整。BIG-IP Application Security Manager 前瞻性地建议根据这些流量调整当前策略。

BIG-IP Application Security Manager 的“循环分析和调整”机制的优势之一是能够最大程度地减少阻挡合法用户流量的可能性。从应用的现有安全状况开始，BIG-IP Application Security Manager 可在安全管理员确保限制因素不会影响正常的用户活动时，逐渐引入限制因素。管理员可在 BIG-IP Application Security Manager 处于“学习”模式时，对其警报进行监控，并在完全确定无误报情况时，才将其切换到“阻隔”模式。

一个普遍存在的问题是，BIG-IP Application Security Manager 如何处理 web 应用的更新。BIG-IP Application Security Manager 策略生成器：

☆ 持续监控 web 站点内容，以便自动检测变化

☆ 分析变化情况，并将其转化为一系列策略更新建议

☆ 应用推荐的自动应用更新，或支持管理员对其手动管理

请注意，BIG-IP Application Security Manager 可前瞻性地建议进行策略修改。管理员无需手动配置所有参数及策略流程。

此外，BIG-IP Application Security Manager 的创新型多层检查机制使其仅阻止不符合应用系统安全策略的请求。目前应用单层检测的解决方案都是屏蔽全部 IP 地址或泛泛的阻止对象访问。但是，BIG-IP Application Security Manager 可确保 web 安全和可用性，即便在这些资源面临攻击时也十分奏效。

全面抵御外部攻击

为了向企业 web 基础设施提供完善的保护，BIG-IP Application Security Manager 将强大的应用层过滤与一流的网络与加密技术融为一体，形成一套完善的 web 安全解决方案。

BIG-IP Application Security Manager 特性

防御随机攻击的消极安全攻击过滤器

☆ 初级黑客

☆ 已知的蠕虫和漏洞

☆ 对受限对象与文件类型的请求

☆ 其它已知的攻击方法

防御目标攻击的积极安全保护

☆ 无效输入处理

☆ 中断访问控制（强制浏览）

☆ 缓冲区溢出

☆ 跨网站指令码攻击

- ☆ SQL 代码/操作系统注入
- ☆ Cookie 中毒
- ☆ HTTP 请求走私

清除内容

- ☆ 防御 web 服务器上的身份盗用
- ☆ 确保清除 web 页面上的用户信息
- ☆ 配置清除一切可识别身份的信息，如：
 - ☆ 社会保险号码
 - ☆ 信用卡号码
 - ☆ 帐号
 - ☆ 病历数据
 - ☆ 电话号码

网络安全服务

- ☆ SSL 加速器
- ☆ IP/端口过滤
- ☆ 反向代理
- ☆ 密钥管理和故障切换处理
- ☆ SSL 终止和 Web 服务器重新加密

隐藏

- ☆ 防止操作系统和 Web 服务器的探测
- ☆ 隐藏用户的所有 HTTP 错误信息
- ☆ 从用户页面中清除应用错误信息
- ☆ 防止泄漏服务器代码

仅 BIG-IP Application Security Manager 能够将所有这些功能集成至一个易于管理的设备中，从而确保 web 应用完善的安全性。

部署方式

在企业或大型政府环境中部署 BIG-IP Application Security Manager 时，需将部署过程的安全性作为更广泛的风险业务中的一部分加以管理。某些应用系统需要即时严格的策略执行，而其它的系统需要的是更为快速的部署。

BIG-IP Application Security Manager 能够根据客户需求部署于各种安全级别下。BIG-IP Application Security Manager 的标准实施时间不超过一天，却能够抵御大多数普通的应用攻击。先进的策略定制支持用户全面满足其所需策略，提供市场上最周密的保护。BIG-IP Application Security Manager 还可在多种不同安全等级上进行配置，并具有为安全管理员提供灵活性的能力，以确保立即实现企业范围内的保护，却丝毫不会降低大多数敏感型应用的安全性。

企业级系统架构

BIG-IP Application Security Manager 的多层系统架构是基于硬件安全防护设计的，用以满足企业对基础设施安全的所有需求，包括：

- ☆ 可忽略的延迟（少于 1 毫秒）及高吞吐率
- ☆ 可升级的架构——可添加额外的部件，用于处理更大的流量
- ☆ 高可用性——部件可配置为支持耦合服务器对（在线服务器与备用服务器）间的热状态故障切换这意味着，当偶然发生服务器故障时，所有的会话数据都将得到保留，并切换到用户不可见的备用设备上。
- ☆ 零故障配置，易于部署和维护——BIG-IP Application Security Manager 由可优化的预配置设备组成，可有效地满足配置、部署及维护事宜
- ☆ 集中与安全管理
- ☆ 易于与企业安全信息管理或管理框架系统集成

BIG-IP Application Security Manager 业务优势

将 web 攻击拒之门外

BIG-IP Application Security Manager 解决方案最主要的优势是可帮助公司网络应用系统抵御网络攻击。随着更多的系统向网络开放，越来越多的敏感的客户数据暴露在攻击面前，而目前的安全系统是无法抵御这种攻击的。一旦被黑客闯入，则将造成无可估量的损失，并滋生高额的保险费用与相应的法律责任。

身份盗窃及其它法规标准

目前，诸如 Basel Accords, HIPAA, California' s SB 1386 及其它的国家或跨国规定的出台，使得制定客户私人数据保护策略势在必行。现在，黑客主要通过网络应用系统窃取客户资料。企业每年因应用层攻击造成的损失高达数亿美元。F5 的 BIG-IP Application Security Manager 产品企业保护客户敏感信息的必备设备。

缩短上市时间

除防御攻击外，BIG-IP Application Security Manager 可切实提高对新应用系统的开发周期。现在，新应用的部署受到应用安全扫描

工具“扫描与修复 (scan-and-fix)”开发周期的影响。写出代码后，在众多产品中抽出一款对其进行扫描，然后，再返回给开发人员修正代码。这个过程不仅浪费时间与金钱，效率也不高，因为扫描器也只能找到几个有限的漏洞而已。借助如 BIG-IP Application Security Manager 等出色的产品，开发团队就可以迅速地开发出新的应用系统与功能，因为他们的程序代码有了强大的安全外围做后盾。

即插即保护

BIG-IP Application Security Manager 解决方案为用户设备提供即插即保护的承诺。BIG-IP Application Security Manager 是一款网络设备，安装在企业的 web 基础架构中非常简便。安装后，设备会自动学习机制并迅速、准确的为其保护的系统制定特定的安全策略。将策略管理与配置简化到最低点，BIG-IP Application Security Manager 可自动生成建议配置或策略，无需等待手动配置。

轻松地计算出投资回报率

可轻松的计算出使用 BIG-IP Application Security Manager 应用层安全解决方案的利润回报率。BIG-IP Application Security Manager 将大幅削减企业的安全执行、攻击损失与赔偿响应的开支。具体情况如下：

减少攻击事故

除攻击本身的损失（资金被盗、收入损失）外，企业还要响应赔付与攻击造成的相关费用，以及支付攻击修复费用。而且，此种响应不仅限于 IT 部门，还牵涉到公共关系、诉讼甚至是法规成本。

无需重写代码

如果没有对应用系统做出精确的保护，则程序开发者必需尽可多的消除程序中的安全漏洞，应用扫描器仅能探测出部分漏洞，因此，必须频繁进行严格的代码审查和改写。一旦应用了 BIG-IP Application Security Manager，程序开发者可全心投入到对新系统与功能的快速部署中去了。

无需反复修复

由于知道系统经常会遭到直接攻击，因此 IT 经理们不得不经常查询网站或公告，以立即安装最新补丁。如上所述，一个安全的应用防火墙可实现仅允许应用系统中的合法活动，以降低对打补丁的依赖性。

无误报

如果阻隔客户的合法访问，则很容易造成客户流失。没有精确的安全模型（如，应用流程模型）来定义合法活动，企业则不得不面对客户与黑客的双重压力，即：放松安全协议则易放入黑客，加强安全协议则易将合法用户阻隔在外。