



# 应用交付网络的安全性

## 概述

互联网已变得日益复杂，众多企业面临着恶意攻击的威胁。各个企业面临防御其基础设施免受网络安全攻击，以及针对特定应用层攻击的挑战。每年，企业的安全成本耗资达几百万美元，其中包括：企业收入锐减、生产效率下降，以及信誉受损。

企业应对这些威胁的传统方式，是采用防火墙来增强网络的安全性。然而经证实，这种覆盖面相对较窄的方式不足以应对需求。尽管传统的防火墙可以保护企业免受网络攻击，但是，它们不足以防御新型应用级攻击。企业正在寻求更多可靠、可扩展的解决方案，来扩展其安全覆盖范围、提高保护的级别。借助应用交付网络解决方案，企业能够获得全面的安全性（无论是网络级安全，还是应用级安全）。

本白皮书旨在探讨 **BIG-IP** 系统如何提供全面集成的方法，保护系统免受网络级和应用级的威胁和攻击，从而增强用户应用的整体安全性。

## 挑战

应用已成为当今企业经营过程的一项核心内容。应用对企业的收入有着直接的影响，因此，保护关键业务信息免受恶意攻击至关重要，这些攻击通常包括针对应用漏洞的攻击，以及低级网络攻击。企业在实现真正的网络和应用安全时，面临着诸多挑战，因为：

**应用漏洞越来越多**——当今的安全系统和防火墙并非智能型系统，不能检测新型的应用层攻击，也不能单独防御此类攻击。这些设备无法确认应用的类型，它们仅是锁定/解锁某个地址、端口或资源。这些传统设备不能对数据包进行深度检查，不能通过维持会话状态信息来检测攻击，也不能防止应用攻击的发生。应用攻击通常包括：注入和执行受到限制的命令，**cookie** 篡改、获得非法访问敏感文档和用户信息的权限。这些攻击会导致损失大量的收入，以及生产效率降低，上述结果反过来还会影响企业的信誉。

**网络漏洞越来越多**——网络攻击变得越来越复杂和广泛。恶意用户正在寻找新的突破网站防线、窃取有价值信息、甚至使整个站点停机的方法。诸如拒绝服务攻击、分布式拒绝服务攻击、无序包泛滥、**TCP** 窗口大小篡改等复杂攻击，正给安全系统抵御大量攻击带来巨大的压力。在发起攻击之前，黑客和恶意用户还启用了站点扫描技术（一种被称之为 **profiling**（特性描述）的技术），从似乎无害的源码（如服务器错误代码、源代码注释）当中检索任意系统或应用信息。

**内部安全危害与信息泄露**——当今企业所面临的其中一个最大的威胁是来自企业内部的攻击。这些攻击难以检测和预防，因为企业内部的员工是可信域中的一部分。当今的安全系统不能

灵活地部署安全策略，不能在对企业内部某些关键业务流量进行加密的同时，允许其它未加密的非关键流量通过。企业正借助其现有解决方案努力部署高效统一的安全策略，使企业的组织机构符合诸如萨班斯 奥克斯利法案、HIPAA 以及 FIPS 等安全监管标准。

## 解决方案

**BIG-IP** 系统可提供范围广泛的各种安全服务，在为企业安全提供支持方面发挥着至关重要的作用。**BIG-IP** 系统可在关键网关位置进行部署，它既能添加功能强大的网络级安全策略，又能过滤最复杂的应用攻击，从而可保护您最宝贵的资源——支持您的业务正常运行的应用与网络。作为一款集成 SSL 加密和新兴应用安全技术领域的领先产品，**BIG-IP** 系统能够使您的站点固若金汤，免受各类攻击。

### 功能强大的应用安全性

**BIG-IP** 解决方案能够对整个应用的有效负载进行深度数据包检查，从而为企业提供了功能强大的应用级安全性。凭借 **BIG-IP** 灵活的特性集及其无可比拟的强大功能，管理员能够轻松管理和控制其应用流量。凭借 **BIG-IP** 系统全方位的认证、授权、审计，以及有效负载解析特性，在允许进行会话之前，企业就能在网络边缘执行安全策略。这些特性包括：

### 通用检查引擎和 iRule

借助 **BIG-IP** 系统，企业可设置并执行通用应用级安全策略。借助 **BIG-IP** 全新的增强性通用检查引擎 (UIE) 和 TCL 规则 (iRule) 能力，企业能够过滤并阻止应用级攻击与威胁。借助全新的 UIE 组件，**BIG-IP** 系统可检查整个应用的有效负载，同时也可根据连续流灵活地做出转变、坚持执行、或拒绝执行之决定。通过使用诸如 TCL 等标准编程接口创建 iRule，以及创建与本企业安全方针一致的策略，企业能够充分利用 **BIG-IP** 灵活而功能强大的特性。一旦创建上述策略，即可将其分配给各文件，从而借助其全新的 GUI 特性就能实现轻松重复部署。通过整合这两项特性，企业就具有了无可比拟的对其应用流量进行控制和保护的能力。

### 认证和授权

通过在网络边缘提供认证功能，以及针对网络中的资源又增添一道安全防线，**BIG-IP** 系统能够增强应用的安全性。高级客户认证 (ACA) 模块可视为站点的“哨所”，它能够为各种类型的 IP 流量提供认证代理。高级客户认证模块可与可插拔模块 (PAM) 引擎协同工作，借助 RAM，用户能够从认证机制库中进行选择，ACA 可从服务器卸载关键认证流程，并降低一些负载和管理任务（通常它们消耗大量的服务器资源）。ACA 模块能够与诸如 LDAP、RADIUS 以及 TACAS+ 等各种授权机制共同工作。

在客户端对证书进行处理时，在接收证书并转发数据包至目标服务器之前，**BIG-IP** 系统可通过证书撤销列表 (CRL) 或在线证书状态协议 (OCSP)，了解该证书的撤销状态。在网络层强化进行认证能够降低应用和服务器的负载，使企业无须花费大量的人力物力对成百上千个应用认证系统单独进行维护。

### 应用和内容过滤

借助 **BIG-IP** 系统功能强大的通用检查引擎、以及其基于策略的 iRule 定制引擎，企业就能有效部署其安全策略。**BIG-IP** 解决方案具备应用和内容过滤功能，通过对流经服务器的流量进行定义，企业能部署一套积极的安全模型系统。由于具备独特的对应用中的有效负载进行数据包检查或会话流检查的能力，**BIG-IP** 系统可阻止对记录/目录、限制性命令的非法访问，并能阻止访问应用服务器上的敏感文档，同时，还能保护企业的关键资产。**BIG-IP** 系统还能过滤受到限制或黑名单中的网站中的内容，这有助于企业执行其安全策略。

## Cookie 加密和认证

借助这一功能强大的特性，企业能够对应用流量中使用的 cookie 进行加密和认证，这就能阻止黑客利用 cookie 来发起应用攻击。由于支持 cookie 加密和认证特性，因此，黑客将无法读取 cookie，从而无法访问诸如 JSessionID 和用户 ID 等信息；无法利用这些信息，黑客也将不能对 cookie 进行修改并创建非法会话。通过阻止会话劫持、Cookie 篡改等攻击（通过改写 cookie 内容并利用关键应用漏洞来实现），BIG-IP 系统能够为企业运行的状态应用提供先进的保护功能。

## SSL 加速与加密

繁重的 SSL 流量会带来处理瓶颈，累垮最为强大的设备，严重影响服务或应用的总体安全性能。同时，不能为 SSL 协议使用的专用密钥提供保护会使用户和服务存在安全风险。

BIG-IP 系统的集成 SSL 加速能力能够强化 SSL 计算资源、使关键任务的管理更加集中。BIG-IP 设备可提供市场上最快、最安全的加密算法。通过为企业配备 AES（高级加密标准，一种对称加密技术，可选择 128、192 或 256 位块加密），BIG-IP 系统可提供更高级的保护，它是企业真正安全技术标准。结合使用 AES 和 SSL 处理，无须任何额外成本，BIG-IP 系统就能提供市场上最安全的 SSL 加密算法。

## 提高网络和基础设施的安全性

通过提供功能强大的网络层安全特性，BIG-IP 系统能够保护企业资源免受大量攻击，这将进一步提升企业的安全性。借助 BIG-IP 设备、其独特的通用检查引擎，以及可编程 iRule 语言，用户能够对网络有效负载的状况了然于胸，企业因此能够智能地管理并部署其安全策略。上述组合能够阻止一些通用网络攻击、Dos（拒绝服务）攻击、DDos（分布式拒绝服务）攻击，以及协议篡改攻击，如果再结合使用 BIG-IP 系统的数据包过滤能力，企业的安全性将获得前所未有的提升，从而生产效率 and 收入将提高、拥有成本将下降。BIG-IP 系统能够提高网络和基础设施的安全性，它具备如下特性：

### 缺省拒绝 (Deny-by-default)

BIG-IP 系统是一种缺省设置为拒绝的设备。缺省条件下，管理员未明确允许可通过 BIG-IP 系统的流量类型，均会拒绝通过。这样，只有您指定的流量才能通过 BIG-IP 系统，从而可提供极高的安全保证。

### 自动防护

BIG-IP 软件内置众多流程，能够保护您的网络免受通用攻击类型的攻击。它将忽略以子网为目的的广播地址，并且不会对广播 ICMP echo 进行应答（这些广播用于发起 Smurf 和 Fraggle 攻击）。由于 BIG-IP 设备连接表与现有连接完全一致，因此，诸如局域网攻击等欺骗连接将无法传递至服务器。BIG-IP 系统可不断进行检查，实现适当的帧定位，从而可防止诸如 Teardrop、Boink、Bonk、Nestea 等通用碎片攻击。诸如 WinNuke、Sub7 以及 Back Orifice 远程控制工具等威胁，都将无法通过缺省的封锁端口。由于 BiG-IP 能够重组重叠的 TCP 报文段和 IP 碎片，因此，企业能够避免近来日益猖獗的一些新型未知攻击。

## SYN CHECK

人们熟知的一种拒绝服务攻击类型为 SYN flood，发起该攻击旨在耗尽系统资源、使其无法建立合法连接。通过发送 cookie 代表服务器对客户发出请求，以及不再纪录尚未完成初始 TCP 握手连接的状态信息，BIG-IP 系统的 SYN CHECK 模块能够降低 SYN flood 带来的危害。这一独特特性确保了服务器只处理合法的连接，BIG-IP SYN 队列资源将不会被耗尽，因此，正常的 TCP 通讯就能继续进行。SYN CHECK 模块是 BIG-IP 系统 Dynamic Reaping 模块的完美补充；同时，

Dynamic Reaping 能够处理已建立连接的 flooding，SYN CHECK 能够查找处于早期阶段的 flooding 连接，从而可防止 SYN 队列被耗尽。由于 SYN CHECK 能够与高性能 syn-cache 协同使用，因此企业能够在不损耗 TCP 报文的情况下，使用 syncookies。

### 拒绝服务攻击 (DoS) 和 Dynamic Reaping

BIG-IP 软件含两项全局设置，具有自适应进行 reap 连接的能力。为了防止拒绝服务 (DOS) 攻击，企业可分别标出一个低水印阈值和高水印阈值进行 reaping 连接。低水印阈值能够测定在这一点之上，reaping 连接（与已定义的时隙接近）中的自适应 reaping 会变得更加活跃。高水印阈值能够测定何时不再允许通过 BIG-IP 系统建立非连接 (non-established connection)。变量的值代表内存利用率百分比。一旦内存利用率达到此值，连接将不被允许，直到可用内存已降低至低水印阈值范围。

### 虚拟服务器上的连接限制

借助 BIG-IP 系统，管理员能够限制并发连接至一台虚拟服务器的最大数量。这就设置了另一道针对拒绝服务攻击等类型攻击的防护屏障。

### 协议无害处理

借助本特性，企业能够保护自身免受黑客采用 IP 协议篡改发起的攻击，这种攻击能够耗尽服务器的资源并使站点停机。通过在第一道屏障内保护系统资源并终止所有客户端与服务器间的 TCP 连接，BIG-IP 系统能够阻止诸如无序包泛滥、MSS tiny packet floods、TCP 窗口篡改等攻击。BIG-IP 设备能够对客户端-服务器间的通讯进行清除处理，查找具有攻击特征的流量和异常情况，并清除服务器和应用所用流量。

### 数据包过滤

BIG-IP 系统的增强数据包过滤引擎提供深层数据包检查功能，管理员可根据高级数据包过滤规则接收、丢弃或拒收（使用诸如“administratively prohibited”等代码发回）流量。数据包过滤规则具有对第四层进行过滤的能力，允许可信流量通过，并能根据安全策略处理其它特定流量类型。企业现在能够在 IPV4 或 IPV6 条件下使用数据包过滤功能来提供基本的防火墙保护能力，并能添加另一道安全屏障。这种过滤基于数据包的源或目标 IP 地址，源或目标端口号（支持该端口的协议），以及诸如 UDP、TCP 或 ICMP 等数据包类型。数据包过滤能够保护系统免遭 IP 欺骗和 bogus TCP flag（伪装 TCP 标记）的攻击。

### 审计和日志记录

由于出现异常或参数无效（如 Land 攻击，Smurf 攻击、校验和出差、IP 协议号或版本未经处理，等等），一些数据包可能会被丢弃，BIG-IP 系统功能强大的日志记录功能能够将与此有关的事件记录下来。通过对尝试发起攻击的源 IP 地址，所用端口、以及尝试攻击的频率进行监控，BIG-IP 设备的安全报告功能能够标识出任何收到的对服务和端口的访问企图。在找出安全网络中的漏洞方面，这一信息能够起到非常重要的作用，能够帮助确定攻击的来源。除了添加了一些新的用于通用内容交换的规则和变量以外，规则的语法也得到了进一步的扩充，其中包括两个新的规则声明：log 和 accumulate。借助上述功能，企业就能利用 iRule 来调用日志记录或系统日志信息，并向管理员实时发出威胁告警。

### 带宽调整

借助这一全新功能，企业能够有效而灵活地保护系统免受带宽滥用攻击。结合使用带宽类型与带宽过滤模块，企业现在就能实现对自身的保护，避免处于流量峰值状态，并免受定期滥用品

户型攻击或可拖垮网络资源的网络攻击。企业能够设定流量和应用的限定条件，控制这些资源以哪一个速率达到峰值状态，这样就能识别并阻止试图累垮网络资源的通用安全攻击。

## 避免信息泄露

采用 **BIG-IP** 系统，那些可利用安全漏洞获取的企业宝贵信息将得到保护。黑客以扫描或分析 Web 站点以获得 IT 基础设施线索而臭名昭著。此类用户通过分析流量特征、检查错误代码来查找漏洞，通过充分利用这些漏洞，他们就能发起攻击。违反安全规则的内部用户访问的行为也日益成为一个常见问题，因为该网络内部的恶意用户尝试非法获取某些敏感数据。**BIG-IP** 系统为企业提供了一款不可或缺的工具，借助这一工具，就能阻止对敏感和关键信息的访问，还能在需要时有所选择地实施加密。**BIG-IP** 设备能够使信息免于泄露，它具有如下特性：

## 资源隐藏

借助 **BIG-IP** 系统，企业能够保护其自身系统免受黑客进行站点扫描或其它类似应用，或进行有关查找漏洞线索的行为。通过对资源进行隐藏，**BIG-IP** 设备能够删除敏感信息（这些信息通常与服务器有关，包括如下内容：网页中的错误代码、源代码注释，包含相关服务器和应用重要信息的服务器标头等）。结合使用功能强大的通用检查引擎以及灵活的 **iRules**，**BIG-IP** 系统就能阻止/过滤任何与站点有关的敏感信息，并能保护企业免受恶意用户的攻击。

## 安全网络地址转换 (NAT) 和端口映射

**BIG-IP** 系统能够对设备所用的地址和端口进行转换，并解析为可广而告之给外部用户的地址和端口。通过转换这些地址，管理员就永远不会担心其 **BIG-IP** 设备资源的泄露，这就降低了黑客获得访问服务器权限的机会。**BIG-IP** 系统包含一个称为智能安全网络地址转换（智能 **SNAT**）的特性，该特性与 **NAT** 类似，能够使服务器同时具有一个不公开的 **IP** 址和一个公开的 **IP** 地址，这就能安全地与外部互联网进行连接。然而，智能 **SNAT** 与 **NAT** 不同，它允许管理员分配或映射一个单独的 **IP** 地址至一组节点，或整个子网，或 **VLAN**。智能 **SNAT** 还能根据 **IP** 数据包数据中的任何一个部分，映射至一个 **IP** 地址。通过 **BIG-IP** 的通用检查引擎，企业现在就能根据 **IP** 数据包数据中的任何一个部分，智能映射 **IP** 地址。缺省条件下，**SNAT** 地址只能用来启动出站连接。在缺省条件下，定向至 **SNAT** 地址的进站初始连接，将被 **BIG-IP** 系统阻止，这就提供了另一道安全屏障。

## 可选内容加密

借助 **BIG-IP** 解决方案，企业能够灵活地根据其应用安全策略和标准需求，对所选的数据进行加密，企业现在能够对其敏感应用数据进行保护，能够构建一套通用的安全策略，能够在一处中心位置在不同需求间谋求一套折衷策略。企业现在能够在清晰可见的通道下传递非关键流量，并有所选择地对敏感流量（如账号和密码）加密，这就使其能够符合诸如萨班斯 奥克斯利法案、**HIPAA** 以及 **FIPS** 等安全监管标准。

## 扩充现有安全解决方案

防火墙、入侵检测系统 (**IDS**) 以及 **VPN** 设备是企业内部以及外部保护系统免受安全威胁的第一道防线。这些设备在网络安全中的重要作用决定了其必须符合如下特性：在所有时间均可用、功能合理、并能快速做出响应。通过将 **BIG-IP** 设备添加至安全基础设施，企业就能扩展其现有解决方案，极大地提升其可扩展性及可用性。上述目标可通过采用一些 **BIG-IP** 系统的高级特性来实现，这些高级特性能够满足企业安全基础设施方面的需求，可实现可靠和无缝的集成。这些特性包括：

高级负载平衡算法——**BIG-IP** 软件提供范围广泛的各种负载平衡算法供管理员选择，其中一些算

法对诸如防火墙、VPN 或 IDS 系统等设备尤其具有重要价值。**BIG-IP** 系统有几种高级算法，如 Predictive、Observed、Dynamic Ratio，用户在选用时需考虑一项或多项动态因素（如：当前连接数）。为了在处理速度、内存及连接类型有显著差异的设备间实现负载均衡，这些算法提供了一种更加出色、一致的利用资源的办法，能够实现最大的投资回报、提升安全设备的性能，并提高用户防护其网络的能力。

### 高级透明状态检查能力

凭借 **BIG-IP** 系统透明状态检查能力，通过透明节点就能对拥有别名的目标地址进行检查。在透明模式下，监控人员可透过节点检查关联（通常为防火墙）至目标节点的地址为哪一个地址。换言之，如果在负载均衡池中有两个防火墙，最初的服务器或内部 **BIG-IP** 对儿将用作通过专用防火墙的目标节点。如果目标节点未响应，防火墙（而非最初的服务器）将标为停机，业务将转发至运行状态良好的资源节点。

### 高级应用状态检查能力

**BIG-IP** 系统的扩展应用验证 (EAV) 特性，可用于提高透明状态检查的精度。EAV 用于进行状态检查，通过远程运行应用，可验证节点中的某项应用。如果应用并非像预期那样在预定时间做出响应，那么，**BIG-IP** 系统会将该请求转发给运行状况良好的设备。

### 高级持续能力

当负载均衡客户端连接通过安全设备队列时，至关重要的一点是，具有相同会话标识的所有数据包将被发送到同样的设备上。借助 **BIG-IP** 解决方案，管理员将拥有众多维持持续性的手段，可确保所有连接针对相同节点具有相同的会话标识，但这一能力并非平衡负载。**BIG-IP** 通用的持续性为用户带来了灵活性，用户可持续保持其应用有效负载的任意部分。

### 任意 IP

借助任意 IP 业务特性，**BIG-IP** 系统能够负载均衡协议，而不仅仅是 TCP 和 UDP。例如，在定义与 VPN 设备池相关的虚拟服务器以支持 IPSEC 业务负载均衡时，管理员可使用该特性。

### 动态连接重新绑定

对于与集群中的其它设备共享会话表的安全设备而言，**BIG-IP** 设备可动态连接重新绑定该设备。如果集群中的某个成员连接失败，则动态连接重新绑定便会将所有连接从失效节点立即转移至同一个池中运行状态好的节点。因为其它节点共享会话表，因此，新选定的节点能够实现对现有连接的认证与许可，同时不会被用户中断或受到干扰。

### 上级节点域 (Last hop pool)

通过在负载均衡安全设备时采用上级节点域，可确保响应连接的路径（从资源节点到客户端）与源请求路径（从客户端到资源节点）相同。借助 **BIG-IP** 的这一特性，管理员可手工标注上级节点域成员，或允许系统利用自动上级节点域特性自动确定上级节点。

### VLAN 镜像

**BIG-IP** 系统改进的 VLAN 镜像特性能够将从 VLAN 收到的数据包复制，并将该副本发送至另一个 VLAN 或 VLAN 集中。无论数据包中的目标 MAC 地址为何处，VLAN 镜像配置条件下源 VLAN 收到的所有业务，均会按这种方式处理。从 **BIG-IP** 系统发送至指定 VLAN 的数据包，不会被镜像。在这种情况下，对于这些 VLAN 而言，**BIG-IP** 形如一台网络集线器。该特性适用于用来负载均衡入侵检测系统的带外配置。**BIG-IP** 系统经过改进的 VLAN 镜像功能，可提供更出色的

性能，使企业用户为其 IDS 设备增添加扩展性及冗余特性。

### 克隆池

BIG-IP 系统改进的克隆池特性可复制由池进行处理的所有业务，复制目标为装有 IDS 或探测设备的克隆池。对于标准负载均衡池而言，用户可对克隆池进行配置。当标准负载均衡池收到连接时，它会通过选定普通池来选择一个普通连接，然后从克隆池中也选择一个克隆节点。克隆节点会收到一份通过该普通池的所有业务的副本。BIG-IP 系统中改进的克隆池特性，可为采用 IDS 设备的企业提供更出色的性能和可扩展性。

### 客户端 SSL 代理

客户端 SSL 代理特性可终止 SSL 连接、对请求加密、以明文发送请求至最终目标。在终止 SSL 连接的过程中，代理可执行所有的认证验证功能，这些功能常由目标 Web 服务器来完成，此外，还包括加密与解密功能。当该特性与克隆池或 VLAN 镜像功能组合使用时，企业就能提高其 IDS 设备的工作效率，但这会造成无法处理加密数据。

### 集成控制

借助 F5 的 iControl API（应用编程接口），BIG-IP 系统正在整合所有防护相关应用。借助 iControl，通过创建、编辑或删除 iRule（通用检查引擎要求使用 iRule），其它设备技术可纳入到 BIG-IP 系统之中。借助 iControl，这些变化能够立即反映出来，从而更快地采用保护措施。这一功能可用于保护 Web 服务、移动应用，以及几乎任何基于 IP 的应用。