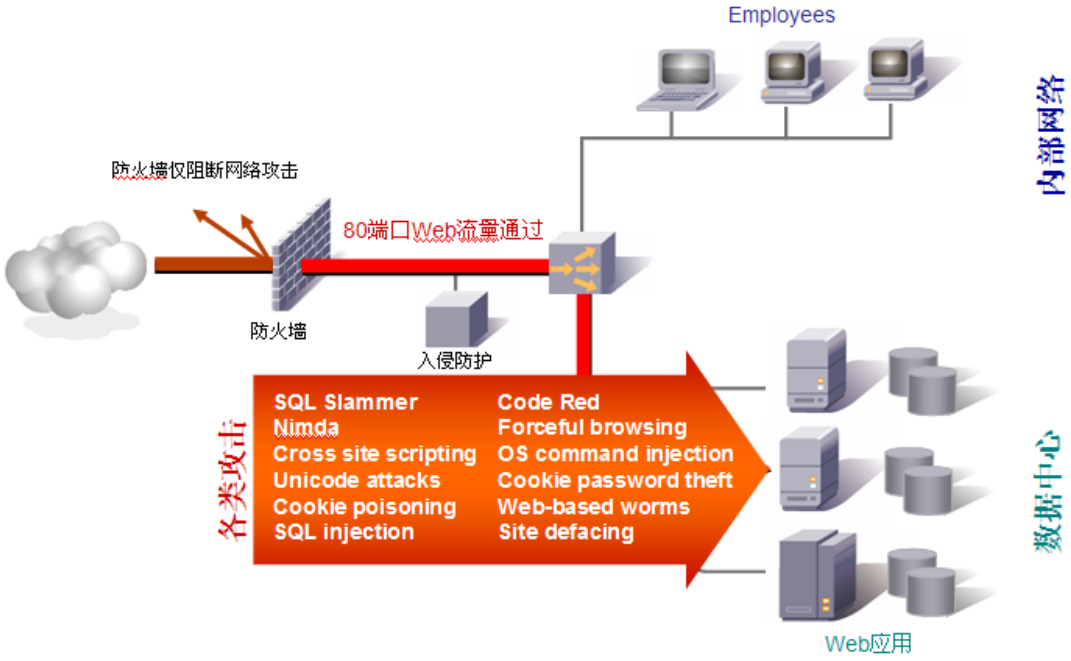
# 梭子鱼 Web 应用防火墙白皮书

随着网络应用的发展，企业 Web 应用日益增多，同时也面临着 Web 滥用、病毒泛滥和黑客攻击等安全问题，导致企业 Web 被篡改、数据被窃取或丢失。根据 Gartner 的统计当前网络上 75%的攻击是针对 Web 应用的。攻击者通过应用层协议进入企业内部，如 Web、Web 邮件、聊天工具和 P2P 等攻击企业网络。利用网上随处可见的攻击软件，攻击者不需要对网络协议的深厚理解基础，即可完成诸如更换 web 网站主页，盗取管理员密码，破坏整个网站数据等等攻击。而这些攻击过程中产生的网络层数据，和正常数据没有什么区别。

因此，传统的防火墙是无法进行 Web 应用防护的。防火墙工作在网络层，通过地址转换、访问控制及状态检测等功能，对企业网络进行保护。但对于应用最广泛的 Web 服务器，防火墙完全对外部网络开放 http 应用端口，这种方式对于 Web 应用没有任何的防护。防火墙无法防护上述应用层的攻击。

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，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。

入侵检测系统作为防火墙的有利补充，加强了网络的安全防御能力。但是，入侵检测技术的作用存在一定的局限性。由于需要预先构造攻击特征库来匹配网络数据，对于未知攻击和或伪装成正常流量的攻击，入侵检测系统不能检测和防御。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。另外就是其技术实现的矛盾，如果需要防御更多的攻击，那么就需要很多的规则，但是随着规则的增多，系统出现的虚假报告（对于入侵防御系统来说，会产生中断正常连接的问题）率会上升，同时，系统的效率会降低。

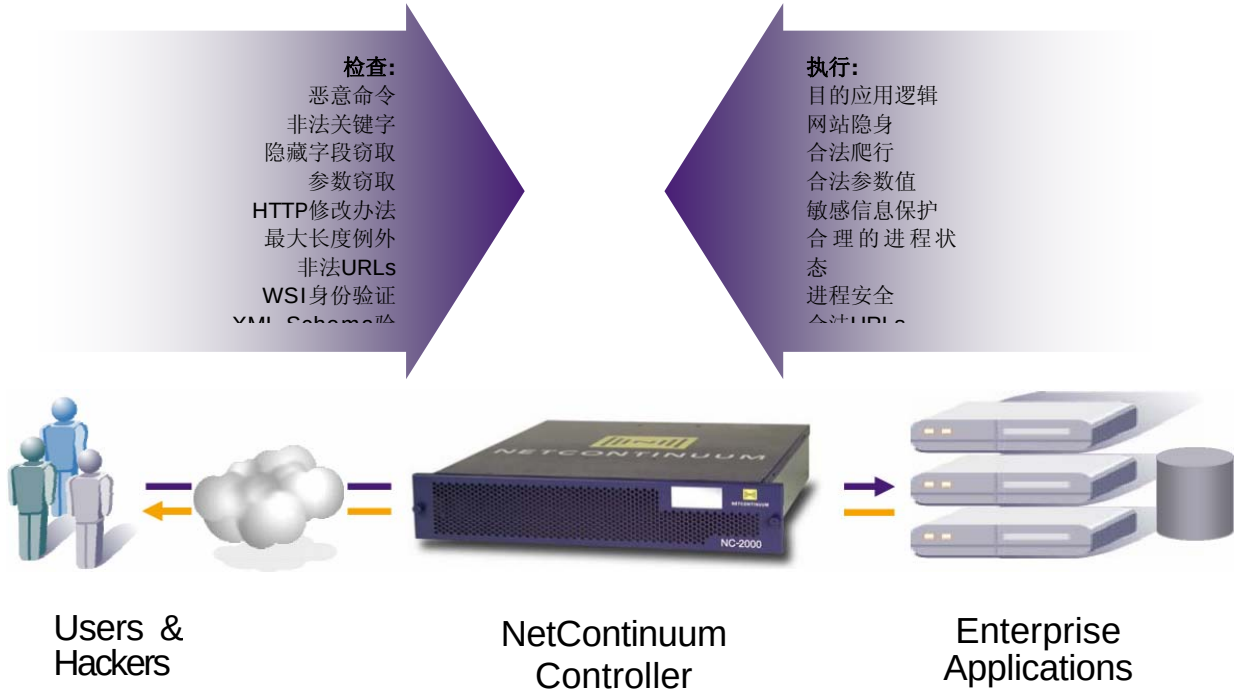



图一 Web 攻击对防火墙及 IDS 是不可见的

梭子鱼提供了世界上最强大的 Netcontinuum 应用防火墙产品线，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。梭子鱼应用防火墙基于 NetContinuum 专利的 NCOS 系统，对 Web 应用具备终止、防护和加速。集中化 GUI 控制界面可以让系统的配置和管理变得十分简单。 特别是，梭子鱼应用控制防火墙完全符合 WAFEC & OWASP 提出的标准。并且是世界上唯一被 ICSA 在网络层和应用层上通过认证的产品。

**梭子鱼应用防火墙的原理：**

梭子鱼应用防火墙通过代理(Proxy)帮助企业建起防线！基于会话的双向代理不仅能应用在网络层，同时还能应用在 HTTP 应用层上，确保内部服务器操作系统和 TCP 堆栈不直接暴露在 Internet，保障 web 应用的安全。



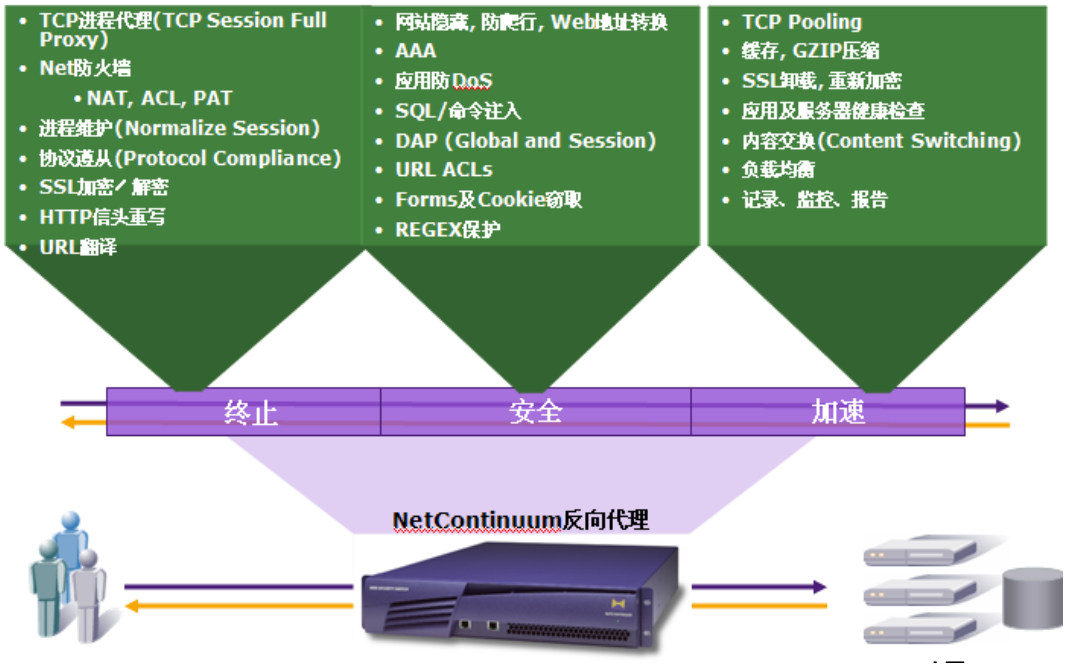

图二 Web 应用防火墙的原理

## NetContinuum 应用防火墙功能：

**终止：** NetContinuum 产品有一个基本原则：用户浏览器和应用程序服务器的连接会话都在此终止。 Netcontinuum 将对应用流量（向内和向外）进行全面的检查，并管理每一个会话。通过 TCP 握手切断任何基于 TCP 的 DOS 攻击。在终止会话的同时，应用防火墙可以提供网络层的 NAT、PAT 、ACL 策略和 SSL 密码系统。系统对于 HTTP 内容有着完全的访问权和控制权，检查所有的 HTTP 内容，解释和建立规则。

**安全：**一旦某个会话被 NetContinuum 应用防火墙终止并被控制，将会对向内或向外的流量进行多种检查，以阻止内嵌的攻击、数据窃取和身份窃取。 可以指定各种策略对 URL、 参数和格式等进行检查。

**加速：**除了 WEB 应用的安全性，数据中心还负责应用的可用性和响应时间。将加速功能(TCP 池，缓存，GZIP 压缩)和可用性功能（负载均衡，内容交换，健康检查）在一个单一的节点处结合起来会显著地简化数据中心的体系结构，以此来降低成本。




## 梭子鱼 NetContinuum 应用防火墙的安装

梭子鱼应用防火墙部署简便灵活，共有 4 种部署方式。

- 单臂模式

单臂模式是目前为止用于残品测试的最透明和最简单的方式，不会影响网络中的其他流量。在单臂模式下，只有 HTTP 和 HTTPS 流量会被指到控制器，控制器处于 DMZ 区。控制器检查这些流量，转发给服务器，记录所有违背安全策略的行为。单臂模式是一种让用户“进入”第 7 层安全应用的方便的方法。

- 桥模式

桥模式是指在两台运行的设备中间插入控制器，但是对流量并不产生任何影响。在桥模式下，控制器阻断第 7 层的应用攻击，但是让其他的流量通过。桥模式是部署最为简便的方式。桥模式是透明的，所以不会干预任何网络中的设备。然而，某些功能在桥模式下是无法启用的，比如负载均衡，内容交换和网络防火墙。

- 代理模式

代理模式为您的应用结构提供了最高程度的保护。然而，这种模式要求应用的 IP 地址在控制器的控制之下。这种模式通常在数据中心与系统相兼容并且已准备好作为代理设备的情况下使用。

- 主动/被动 安全性增强

此外，以上每一种模式可以运行在主动或者被动模式。在被动模式下，控制器不会执行策略。

仅仅让流量通过，始终学习、报告和记录事务日志。对于理解应用的行为和提供有价值的信息来将控制器移入应用数据流是非常有用的。只有在主动模式下，控制器才会执行安全策略。

- 备机

NetContinuum 控制器拥有 stateful failover 功能。在主控制器失败的情况下（由于软件出错，网络连接出错等），备用控制器能够安全、有效地进行接替。没有流量丢失。

- 穿透功能

NetContinuum 控制器包含可选的网络层 fail open 功能。 若控制器的硬件、PSU 或软件出错，控制器会把自己从网络中移除，使所有流量都能到达后面的设备。任何控制器的问题都不会导致应用的失效。

## *管理简便*

在部署完毕后，NetContinuum 控制器提供一个信息和控制的中心点来操作您的应用。数据中心能够观察到完整的应用健康程度。能够方便迅速地调整策略，不需停止任何服务。NetContinuum 研发了一个管理模型和特别设计的 GUI，用来促进当前技术人员运用 NetContinuum 的水平并拓展对于应用控制的能力。最重要的是，系统设计了向导功能和预设置功能，这将能够对新的应用的安全性和新的策略进行迅速的定义。

- 运行情况报告 – 应用和系统健康

运行情况报告发布实时完整的应用运行的健康数据。处理率、比特率、健康攻击都被实时监控并显示在运行情况报告面板里。诸如内存和 CPU 的利用情况、应用防火墙、网络防火墙和系统的日志等控制器信息都实时显示。

- 虚拟功能 – 多个应用

NetContinuum 的虚拟功能是一个为数据中心所提供的强大的工具，这个数据中心处理着应用方面的管理。虚拟功能允许您定义多个独立的应用。每个被定义的应用都被当作一个单独的实体进行处理。系统让管理员独立、清晰地管理多个应用服务。

- 当前策略调整

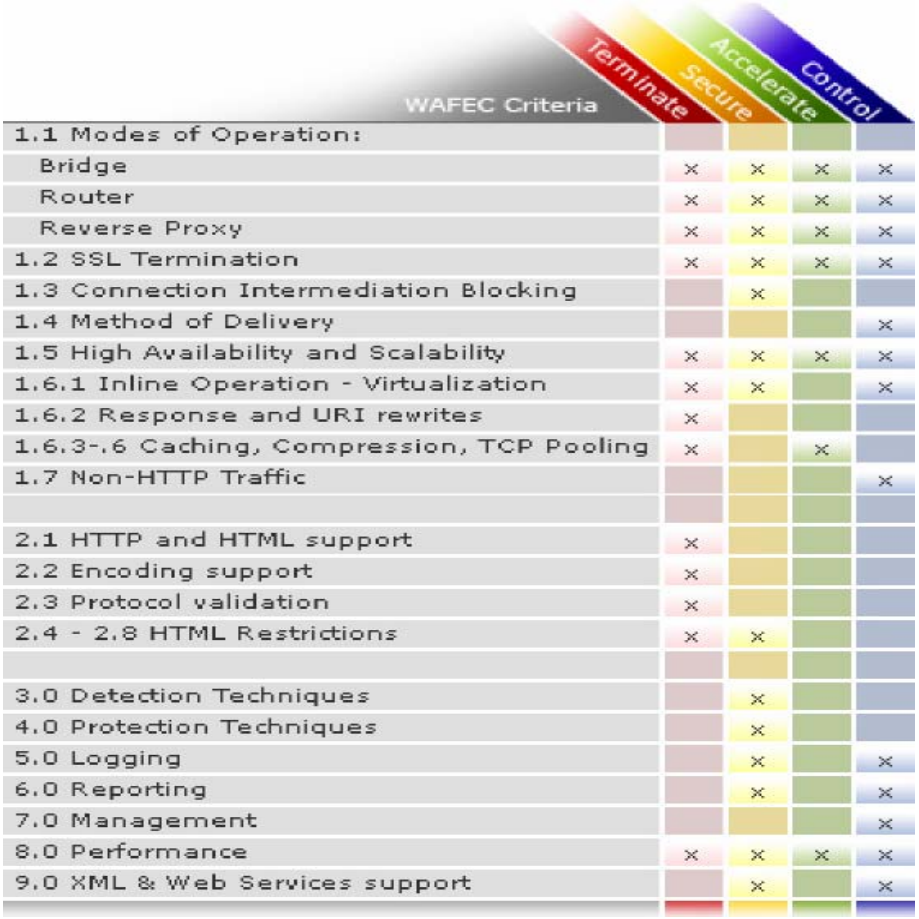
应用服务经常改变并被部署。因此，控制器必须能够方便地调整策略。NetContinuum 控制器有两种方法来帮助管理员管理这种情况。NetContinuum 动态应用调试和执行 (DAP) 能够实时地自动学习和执行策略。此功能使得管理员在不对控制器产生任何影响的前提下部署应用的升级。一些安全人员更加喜欢一种操控性更强、手动进行的应用升级。实时策略向导能够协助您自定义策略，同时让您对于当前的策略拥有完全的掌控。此系统能够记录所有违背 ACL 的行为。根据这个日志，当然，您也可以随时重新创建策略。

## 符合标准

由于当今 Web 攻击日益严重，加上与它们相关的攻击与日俱增，因此研发一种测试产品安全性的标准来全面保护应用显得至关重要。

两个站在定义应用安全前线的组织机构是：

- 开放Web应用安全项目 (OWASP),这是一个致力于寻找和攻克危险软件的组织。OWASP 所规定的前十项要求提供了最低标准的应用安全。NetContinuum产品能够轻松解决前十项最普遍的WEB安全漏洞问题。请浏览OWASP官方网站： www.owasp.org.
- Web应用安全联盟 (WASC)是一个包含专家、行业人员、和生产开源应用安全标准的组织代表的国际组织。联盟新的 “Web应用防火墙评测标准” (WAFEC)是一个为提供独立的、与厂家无关的WEB应用防火墙产品的评测标准。符合了这些标准意味着能够确保进入的数据都是安全的。自从标准出台以来，NetContinuum就着手开始满足WASC-WAFEC 评测标准的工作。下表表明了NetContinuum如何满足这些标准，包括终止，安全，加速和会话控制等功能。要获得更多详细信息，请浏览www.webappsec.org 和 NetContinuum的官方网站。



| WAFEC Criteria | Terminate | Secure | Accelerate | Control |
|---|---|---|---|---|
| 1.1 Modes of Operation: | | | | |
| Bridge | × | × | × | × |
| Router | × | × | × | × |
| Reverse Proxy | × | × | × | × |
| 1.2 SSL Termination | × | × | × | × |
| 1.3 Connection Intermediation Blocking | | × | | |
| 1.4 Method of Delivery | | | | × |
| 1.5 High Availability and Scalability | × | × | × | × |
| 1.6.1 Inline Operation - Virtualization | × | × | | × |
| 1.6.2 Response and URI rewrites | × | | | |
| 1.6.3-.6 Caching, Compression, TCP Pooling | × | | × | |
| 1.7 Non-HTTP Traffic | | | | × |
| | | | | |
| 2.1 HTTP and HTML support | × | | | |
| 2.2 Encoding support | × | | | |
| 2.3 Protocol validation | × | | | |
| 2.4 - 2.8 HTML Restrictions | × | × | | |
| | | | | |
| 3.0 Detection Techniques | | × | | |
| 4.0 Protection Techniques | | × | | |
| 5.0 Logging | | × | | × |
| 6.0 Reporting | | × | | × |
| 7.0 Management | | | | × |
| 8.0 Performance | × | × | × | × |
| 9.0 XML & Web Services support | | × | | × |

## 总结

要完全控制企业的 Web 应用需要强大的功能来确保执行所有安全策略的可用性和响应时间。负载均衡、内容交换、full-stack 协议检查（网络和应用）的响应时间加速、内容检查、告诉密码系统、认证、访问控制和完整登陆等策略都要严格地应用，从此安心地在互联网中进行商业事务的操作。

应用控制器正在迅速成为一个企业应用DMZ的“最优方法”。NetContinuum通过行业中使用最简单、运行最高效的应用控制器家族来不断证明自己对保护Web应用、降低终端用户响应时间和提供应用可用性的能力。