KSIDC
Korea Server Hosting Inc

KS

Korea Server Hosting
韩国斯博 IDC

- 2011年引领IDC领域技术革新
- 2010年rankey.com IDC领域名列第一
- 2009年被韩国互联网振兴院授予客户满意度第一名

韩国斯博IDC将以突出的维护管理服务成为企业和个人的战略伙伴。
首尔市瑞草区瑞草洞1710 - 1 SK Broadband IDC中心
联系电话 : 02 - 593 - 8320 传真 : 02 - 6264 - 8321

网络防火墙

KSIDC的网络防火墙服务是，
针对网络资源的安全漏洞
检测并排除攻击的服务。

网络防火墙是什么？

网络防火墙服务是指，不同于网络安全设备（firewall，IDS，IPS）服务的，为了从根本上解决，因降低网络资源安全漏洞而发生的黑客等安全事故，所需要的能够修正，使网络资源安全得到强化的工作。
但是，考虑到在中小型企业，修正网络安全资源的工作相当艰难，所以KSIDC提供了网络防火墙服务。
网络防火墙服务，是以应用基层（Layer 7）分析技术和正规化技术为基础，监视 HTTP/HTTPS 项目的通信量，检测非法攻击，并在该攻击到达客户网络服务器之前，将攻击阻断的服务。

OWASP TOP10 网络应用安全漏洞

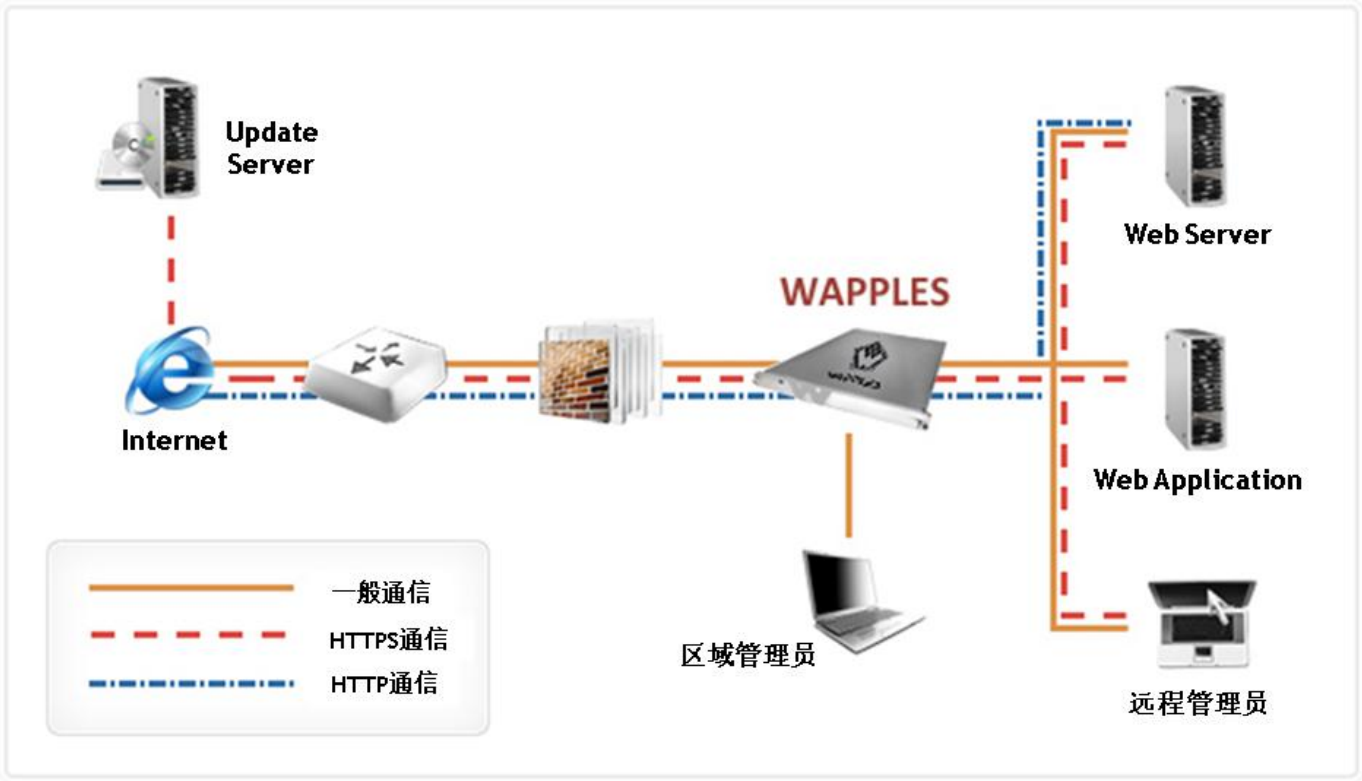
1. 支持多种 Linux 平台安装（Cent OS，Fedora 最新版本）
2. 注入漏洞（Injection Flaws）
3. 恶意文件执行（Malicious File Execution）
4. 不安全的直接个体引用（Insecure Direct Reference）
5. 跨站请求伪造（CSRF: Cross Site Request Forgery）
6. 信息泄露和错误处理不当（information leakage and Improper Error Handing）
7. 缺陷认证和会话管理（broken Authentication and Session Management）
8. 不安全的密码存储（Insecure Cryptographic Storage）
9. 不安全的通讯（insecure Communications）
10. URL 限制连接失败（failure to Restrict URL Access）

网络防火墙

KSIDC
Korea Server Hosting Inc

❖硬件网络防火墙服务（Wapple）

✓ 隐形代理（Transparent Proxy）方式



- 以网络服务器和防火墙之间的 In-line 方式设置 、运营
- 可以在不改变网络设置的情况下部署
  - 无须变更网络服务器 IP 及 DNS

- 将网络客户端的 IP 完整的传送到网络服务器
- Bypass 功能支援

网络防火墙

KSIDC
Korea Server Hosting Inc

产品功能

✓ 对 **Inbound** 通信量分3阶段实施检查

- **预处理器**
  - 通过对 SSL 解密及 Normalization，HTTP 是否遵守规章，来清除异常流量
- **Positive Security Model 模块**
  - 通过执行特别的 URI 访问控制，拒绝连接未授权的 URI
- **Negative Security Model 模块**
  - 在连接许可的请求中，也要检查是否包括攻击

✓ 对**Outbound** 通信量的检查

- **Content Filter 模块**
  - 是否包含个人信息，是否伪造网页的确认，通过对错误分析而造成的信息泄露
- **Encryption 模块**
  - 对可能伪造的 cookie 及隐藏字段等，计算无结果的检测价格
- **检测分析攻击技巧**
  - 普通网络攻击检测的局限性
    - 检测已知的多种攻击模式，在攻击模式更新之前发生的 zero-day attack 下薄弱
    - 在没有固定形式的 SQL/Command Injection 的攻击下薄弱
    - 对于在学习时间内发生的攻击，存在学习的可能性
    - 因一定存在例外的情况，所以需要管理员的调整
    - 当网站重组或修改是需要额外的学习

网络防火墙

KSIDC
Korea Server Hosting Inc

- 不是单纯的模式匹配，而是提供应用攻击逻辑分析功能
  - 即使是遇到不知道的新的漏洞，也要通过检测相关的攻击方法的规则来防止
  - 输入信息内容攻击可能性的逻辑结构，如果被确定为攻击，则立即切断该检测
  - 测试 HTTP 处理能力 → 检测伪装成浏览器的 Worm 及漏洞扫描器

- 在网络攻击检测的最优化结构
  - 可以检测到用单纯模式匹配无法检测的多种变形攻击
  - 管理员的介入最小化

- **未知攻击检测**

- **Input Content Filtering（用户自定义规则）**
  - 检测用户输入的字符串
  - 支持对制定字符串的变更

- **Invalid HTTP**
  - HTTP 规格以外的请求或响应，不存在的网站请求的阻断
  - 包括利用位置漏洞的蠕虫攻击工具，产生的非正常的流量的阻断

- **Invalid URI**
  - RFC 定义的格式以外的 URI 请求阻断
  - 防止对侵害 RFC 标准的新漏洞的攻击

- **Suspicious Access 检测规则**
  - 对不是正常网络浏览器的客户端的连接对象，被确定为异常状态或限制该连接
  - 对新漏洞的扫描，自动攻击工具拒绝访问