xxxxxxxxxxxxx 限公司

网站服务器基础架构及安全解决方案

目录

1. 前言

1.1 简述

随着网络事业的爆炸式增长，交易需求也随之提高，为满足需求，网络交易平台成为一种应运而生的旨在通过电子手段建立一种新的秩序，它不仅涉及电子技术及商务本身，而且涉及到诸如金融，税务，教育，法律等社会其他层面。它是充分利用高清技术而引发革命性的商务实践，也必将对传统的交易模式带来广泛而深刻的影响。

1.2 文档目的

互联网正使得信息访问变得随处可及，如何才能实现企业级信息的随需访问，如何才能够使得企业级信息的访问、安全、服务易如反掌？旧有的、孤岛式的数据中心的信息基础架构已经难以满足企业的需求，必须进行变革，完善企业的信息基础架构。

盗用账号、缓冲区溢出以及执行任意命令是 Web 服务器比较常见的安全漏洞。黑客攻击、蠕虫病毒以及木马是因特网比较常见的安全漏洞。口令攻击、拒绝服务攻击以及 IP 欺骗是黑客攻击比较常见的类型。随着网络技术的不断发展，Web 服务器面临着许多安全威胁，直接影响到 Web 服务器的安全。因此，加强 Web 服务器的安全防护是一项迫切需要的解决的时代课题。特此编写了本文档供用户领导及相关技术人员参考。

1.3 目标读者

本文的主要读者为信息技术部门领导及下属技术人员、代表与工程技术人员，以及合作伙伴及项目集成商等相关人员。

2. 现有状况分析

2.1 环境分析：

XXXXX 公司目前需要构建一套网上交易平台，包括 web 服务、中间件服务器、数据库服务器、跳板服务器以及网络安全、接入设备。所有设备会托管于 IDC 机房。

2.2 主要需求分析：

2.2.1 基础架构建设

- 主要应用和数据库服务器架设，要求具有可扩展性。需要 7 台服务器承载包括 web 服务、中间件服务、数据库服务、跳板服务，配置均为单 4 核芯片，16GB 内存，3x300GB 硬盘，Raid5。
- 存储设备需求，双光纤控制器存储，容量 1TB，磁盘转速 10krpm，要求具有扩展性。
- 网络接入、交换设备，要求具有可扩展性、高可用性。

2.2.2 信息安全、网络安全需求

- 防火墙需求，需要 IDS、IPS、VPN 等功能保护主机安全。
- Web Application Firewall，用于保护 HTTP\HTTPS。
- SSL 认证，验证身份，确保网站安全性、真实性。

2.2.3 高可用、容灾需求：

- 所有设备需要冗余，可采用主\备或主\主的形式。
- 由于 WEB 服务器可能扩展至多台，因此需要多点负载均衡。

3. 针对现状和需求提出建议及解决方案

3.1 总体建议方案简述：

3.1.1 一期方案

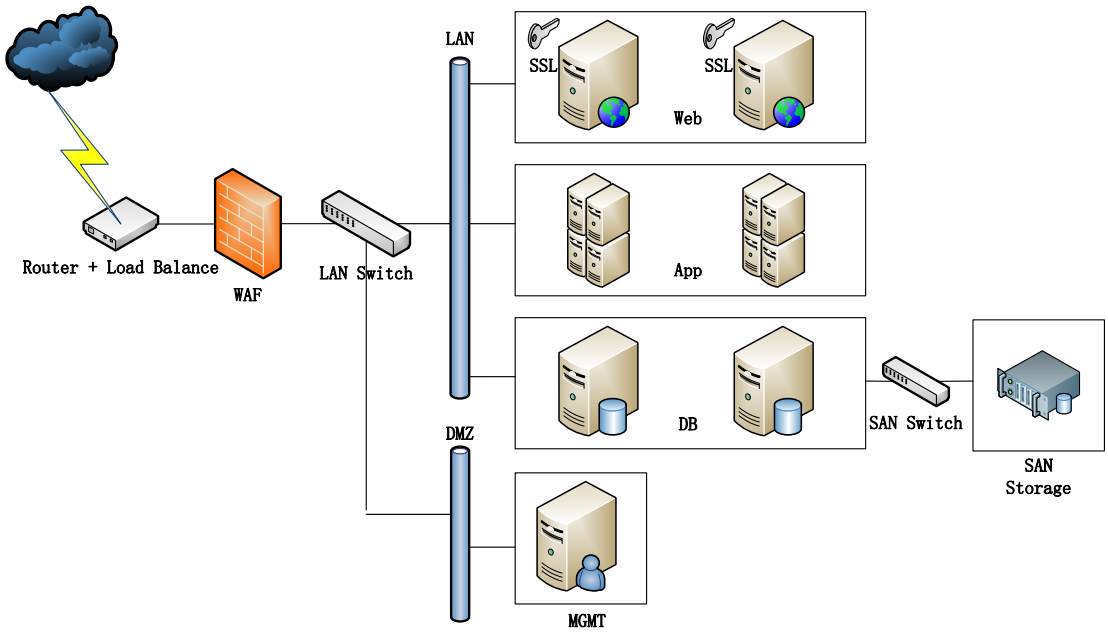
- 新服务器、存储架设
- WAN+LAN 网络负载均衡
- 防火墙+WAF
- Verisign 安装

3.1.2 二期方案

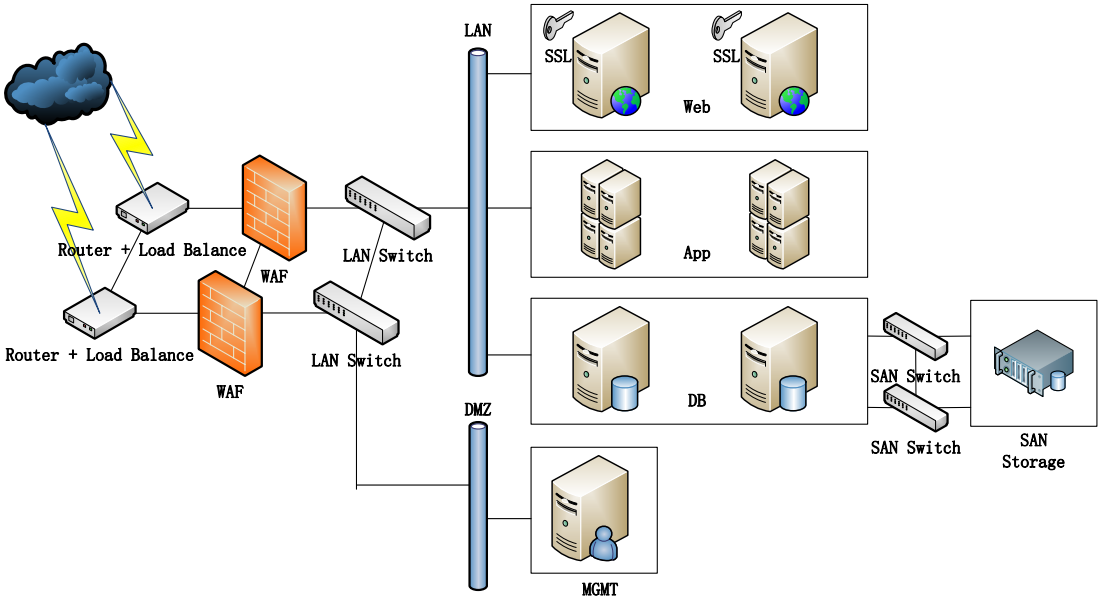
- 双线接入（电信+联通）
- 交换机防火墙负载均衡等设备冗余

3.2 方案拓扑图

3.2.1 一期



3.2.2 二期



3.3 软件部署方案：

3.3.1 Symantec Secure Site Pro with EV

全球最值得信任的网络基础架构供应商——威瑞信（VeriSign）公司提供的 Web 服务器证书（SSL 证书）可以确保您的网站与您的客户之间安全的信息传输，为超过 93%的财富 500 强企业，97%的世界 100 大银行，以及全球 50 家最大电子商务网站中的 47 家提供了数字认证服务。Symantec 提供的 SSL 证书（Symantec Secure Site Pro）产品可以最大限度上提升客户交易信心。截至目前，全球范围有超过百万台服务器部署了 Symantec SSL 证书，并且这一数字还在不断刷新。

- **SGC128 位强制加密技术**

能自动激活浏览器显示“锁”型安全标志，地址栏“https”开头的页面意味着在客户端浏览器和 Web 服务器之间已建立起一条 SSL 安全加密通道（secure sockets layer），此时用户在线输入的信用卡号、交易密码等机密信息在网络传输过程中将不会被查看、窃取和修改。

SGC128 位强制加密技术，能够保障浏览器与 Web 服务器之间建立至少 128 位，最高 256 位的传输加密通道，确保加密传输的数据不可被破解。

- **SSL 证书包含企业身份信息**

  VeriSign 从成立之初一直坚持严格遵循业内最为严格的身份鉴证机制，不提供单一域名鉴证产品，确保每张签发证书身份真实有效，在数字证书领域拥有良好声誉，可以最大程度上提升网站的可靠和信任度。当客户访问网站时，可通过点击金色安全锁或站点签章标志，便可检验网站真实身份。

- **扩展验证功能帮助挫败欺诈钓鱼网站**

  扩展验证（EV）SSL 证书经过最彻底的身份验证，确保证书持有组织的真实性。绿色地址栏将循环显示组织名称和作为 CA 的 VeriSign 名称，从而最大限度上确保网站的安全性，树立网站可信形象，不给欺诈钓鱼网站以可乘之机。

- **绿色地址栏，增加顾客信赖度**

  对线上购物者来说，绿色地址栏是验证网站身份及安全性的最简便可靠的方式。在 IE7.0、FireFox3.0、Opera 9.5 等新一代高安全浏览器下，使用扩展验证（EV）SSL 证书的网站的浏览器地址栏会自动呈现绿色，从而清晰地告诉用户正在访问的网站是经过严格认证的。此外绿色地址栏临近的区域还会显示网站所有者的名称和颁发证书 CA 机构名称，例如 Symantec。所有的一切，均向客户传递同一信息，该网站身份可信，信息传递安全可靠，而非钓鱼网站。拥有 Symantec 扩展验证（EV）SSL 证书的客户的转换率大幅增加，销售额平均增幅达到 17.8%（根据 11 个国家或地区的 32 个案例研究来计算）。

- **EV Upgrader 技术支持，帮助更多客户轻松获得安全绿色地址栏**

  Symantec 提供 EV Upgrader 升级技术，该技术可帮助非 VISTA 的 IE7 的用户自动升级根证书。

- **无法仿冒的 Symantec 信任签章**

在拥有扩展验证（EV）SSL 证书的同时，您还可拥有 Symantec 信任签章（Symantec Trust Seal）。该标志拥有庞大的用户群，Symantec 信任签章在 160 个国家或地区中超过 90,000 个网站上，一天显示次数多达 2 亿 5 千万次。任何网站都可以通过显示 Symantec 信任签章（Norton Trust Seal）建立网上信任度、可靠性及忠实度。配合 Symantec 搜索结果签章的应用，它可以将 Symantec 信任签章（Norton Trust Seal）展示在搜索结果旁边，从而让您的网站在其他竞争对手中脱颖而出，向客户标明您的网站从搜索到浏览再到购物整个过程安全可靠。

创新的签章实现技术确保该标志不会被假冒或钓鱼网站非法使用。图中签章只是一个样本（实际签章是已经取消鼠标右击并保存功能），点击 Symantec 信任签章，会看到网站提供给 Symantec 且经过验证后完全可靠的信息，包括网站所有者的名称、城市、州/省、国家或地区，以及最近恶意软件扫描的情况。

- **全球最广泛的浏览器支持**

今天，越来越多的用户希望随时随地能够通过电脑、 PDA 和智能手机浏览互联网。而 Symantec Secure Site Pro 由于其根证书预埋在主流浏览器中，支持全球超过 99%的浏览器。因此可以无缝支持主流浏览器,确保固定网络和移动网络 Web 站点的安全。

PC 端浏览器	IE	Firefox	Opera	Chrome	Safari	Mozilla	Netscape
版本支持	4.0+	0.1+	7.0+	All	1.2+	0.6+	4.7+
移动终端	IOS	Android	BlackBerry	Symbian	WebOS	JRE	Windows Mobile
版本支持	All	1.9+	4.1+	S40+	All	1.4.2+	2003+

- **30 天无条件退款保证**

消费保障计划，支持 30 天内无条件全额退款。只要在证书签发后 30 天内撤销证书，将不会收取任何证书费用。您可以放心申请试用，不必担心项目上线之前的测试阶段有证书需求而又无法确认合适的产品了。

3.4 硬件部署方案

3.4.1 负载均衡

深信服 AD-1600

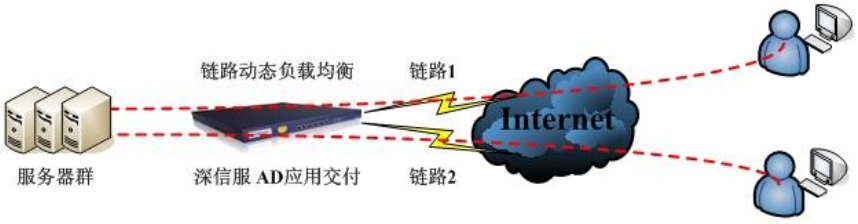
3.4.1.1 链路负载均衡

- **出站流量**

AD 接收到流量以后，可以智能的将访问 ISP1 的资源的出站流量分配到 ISP1 的接口，并做源地址的 NAT，（可以指定某一合法 IP 地址进行源地址的 NAT，也可以用 AD 的接口地址自动映射），保证数据包返回时能够正确接收，其他的流量走 ISP2 的线路。

- **入站流量**

AD 分别绑定多个 ISP 服务商的公网地址，解析来自多个 ISP 服务商的 DNS 解析请求。ISP1 的用户访问通过 ISP1 的线路访问内部，其他的用户访问通过 ISP2 的线路来访问内部。AD 不仅可以根据服务器的健康状况和响应速度回应 LDNS 相应的 IP 地址，还可以通过多条链路分别与 LDNS 建立连接，根据 RTT 时间判断链路的好坏，并且综合以上多个参数回应 LDNS 相应的 IP 地址。



- **DNS 透明代理技术、链路拥塞控制技术**

实现对带宽资源的合理利用，避免过多用户被分配到同一链路之上，造成访问速度变慢。

通过单边加速技术不需要在客户安装任何软件和插件就可以实

现用户访问速度的提升，大大提升用户的访问体验。

3.4.1.2 Web 服务器负载均衡

- **轮询**

  将所有网络链路放在一个队列当中，按顺序依次返回给用户队列中下一个网络链路的 IP 地址。

- **加权轮询**

  由于各条互联网链路的吞吐量可能不一，因此可以为各条链路分配不同的加权值。根据这个比例，把数据流量轮询分配到每条链路。

- **加权最少连接**

  是一种动态调度算法，它通过链路当前所活跃的连接数来估计链路数的负载情况。AD 需要记录各个链路已建立的连接书，当一个请求被调度到某链路，其连接数加 1；当连接中止或超时，其连接数减 1；

  加权最小连接算法通过以各条链路上的实际连接数为权值，在调度新连接时尽可能的使各条链路上已建立连接数为 1：1，AD 将把新的连接请求分配到当前比例最小的链路上

- **静态就近性**

  SANGFOR AD 搜集了各运营商所有的 IP 地址库并提供实时更新，目标 IP 属于哪个运营上选择那个运营商链路；同时，用户可在上为某个目标定义静态的最佳链路。例如目标 IP 地址属于 ISP1 的，应选择 ISP1 链路；目标 IP 地址属于 ISP2 的，应选择 ISP2 链路。

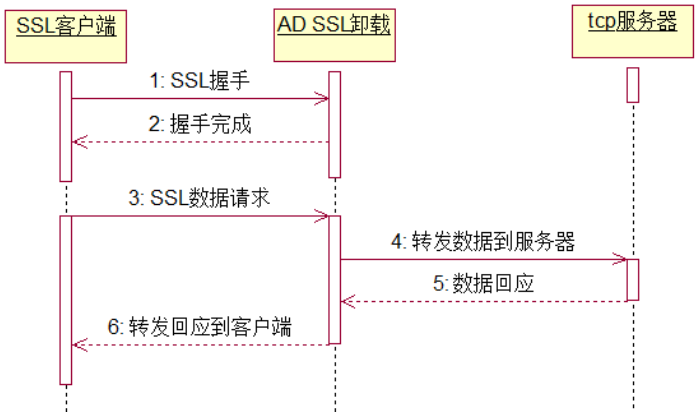
- **动态就近性**

  在选择最佳链路时，SANGFOR AD 通过综合考虑与目标网络之间的路由节点数量、数据传输的延迟和链路的实时负载，准确计算出最佳路径。因此用户能充分地享受到优化的服务和快速地响应。

3.4.1.3 SSL 卸载技术

通过将 SSL 的加密过程专家的深信服 AD 设备之上，由于深信服设备拥有超强的加解密能力能够满足高并发访问网站的需求，减少服务器的性能压力，提升访问速度，甚至可以根据用户情况减

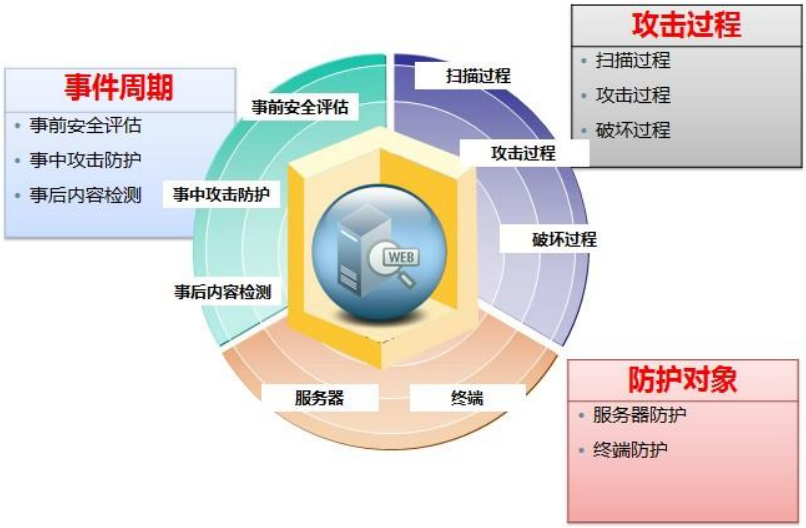
少服务器的硬件投资。SSL 卸载技术细节说明请参见下图：



3.4.2 防火墙

深信服 NGAF

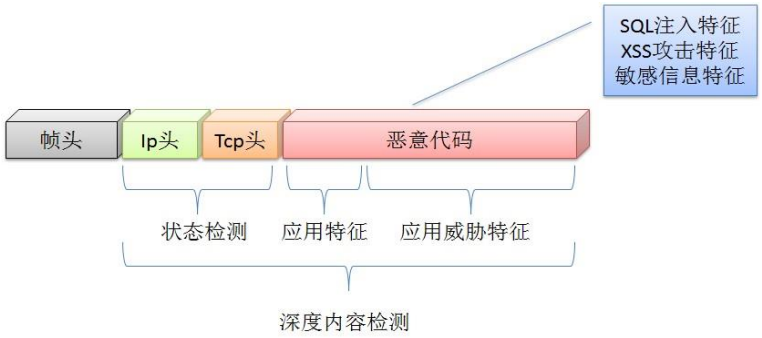
深信服 NGAF 提供对 Web 业务系统的三维立体防护解决方案，深入分析黑客攻击的时机和动机。从事件周期、攻击过程、防护对象三个维度出发，提供全面的安全防护手段，保护 web 业务系统不受来自各方的侵害。



- **多种拦截方式支持**

NGAF 可实现对 HTTP/HTTPS 协议的深入解析，精确识别出协议中的各种要素，如 cookie、Get 参数、Post 表单等，并对这些数据进行快速的解析，以还原其原始通信的信息，根据这些解析后的原始信息，可以精确的检测其是否包含威胁内容。而传统的 IPS 基于 DPI 深度数据包解析技术，只能实现在网络层数据包层面进行重组还原及特征匹配，无法

解析基于 HTTP 协议的内容分析，很难有效检测针对 web 应用的攻击。而具备简单 web 攻击防护的 IPS，仅仅是基于简单的特征检测技术，存在大量的漏报误报的信息。



- **安全风险评估与策略联动**

NGAF 基于时间周期的安全防护设计提供事前风险评估及策略联动的功能。通过端口、服务、应用扫描帮助用户及时发现端口、服务及漏洞风险，并通过模块间的智能策略联动及时更新对应的安全风险的安全防护策略。帮助用户快速诊断电子商务平台中各个节点的安全漏洞问题，并做出有针对性的防护策略。

- **典型的 Web 攻击防护**

深信服下一代防火墙 NGAF 有效结合了 web 攻击的静态规则及基于黑客攻击过程的动态防御机制，实现双向的内容检测，提供 OWASP 定义的十大安全威胁的攻击防护能力，有效防止常见的 web 攻击。（如，SQL 注入、XSS 跨站脚本、CSRF 跨站请求伪造）从而保护网站免受网站篡改、网页挂马、隐私侵犯、身份窃取、经济损失、名誉损失等问题。

- **网页木马**

网页木马实际上是一个经过黑客精心设计的 HTML 网页。当用户访问该页面时，嵌入该网页中的脚本利用浏览器漏洞，让浏览器自动下载黑客放置在网络上的木马并运行这个木马。NGAF 设备可以检测到此类攻击行为。

- **网站扫描**

网站扫描是对 WEB 站点扫描，对 WEB 站点的结构、漏洞进行扫描。

NGAF 设备可以检测到如爬虫、扫描软件，如 appscan、等多种扫描攻击行为并进行阻断。

- **系统命令注入**

攻击者利用服务器操作系统的漏洞，把 OS 命令利用 WEB 访问的形式传至服务器，获取其网络资源或者改变数据。NGAF 设备可以检测到此类攻击行为。

- 文件包含攻击

文件包含漏洞攻击是针对 PHP 站点特有的一种恶意攻击。当 PHP 中变量过滤不严，没有判断参数是本地的还是远程主机上的时，就可以指定远程主机上的文件作为参数来提交给变量指向，而如果提交的这个文件中存在恶意代码甚至干脆就是一个 PHP 木马的话，文件中的代码或者是 PHP 木马就会以 WEB 权限被成功执行。NGAF 设备可以检测到此类攻击行为。

- **目录遍历攻击**

目录遍历漏洞就是通过浏览器向 WEB 服务器任意目录附件“.../”，或者是在有特殊意义的目录附加“.../”，或者是附件“.../”的一些变形，编码访问 WEB 服务器的根目录之外的目录。NGAF 设备可以检测到此类攻击行为。

- **信息泄露攻击**

信息泄露漏洞是由于 WEB 服务器配置或者本身存在安全漏洞，导致一些系统文件或者配置文件直接暴露在互联网中，泄露 WEB 服务器的一些敏感信息，如用户名、密码、源代码、服务器信息、配置信息等。NGAF 设备可以检测到此类攻击行为。

- **口令暴力破解防护**

弱口令被视为众多认证类 web 应用程序的普遍风险问题，NGAF 通过对弱口令的检查，制定弱口令检查规则控制弱口令广泛存在于 web 应用程序中。同时通过时间锁定的设置防止黑客对 web 系统口令的暴力破解。

- **文件上传过滤**

由于 web 应用系统在开发时并没有完善的安全控制，对上传至 web 服务器的信息进行检查，从而导致 web 服务器被植入病毒、木马成为黑客利用的工具。NGAF 通过严格控制上传文件类型，检查文件头的特征码防止有安全隐患的文件上传至服务器。同时还能够结合病毒防护、插件过滤等功能检查上传文件的安全性，以达到保护 web 服务器安全的目的。

- **URL 防护**

Web 应用系统中通常会包含有系统管理员管理界面以便于管理员远程维护 web 应用系统，但是这种便利很可能会被黑客利用从而入侵应用系统。通过 NGAF 提供的 URL 防护功能，帮助用户选择特定 URL 的开放对象，防止由于过多的信息暴露于公网产生的威胁。

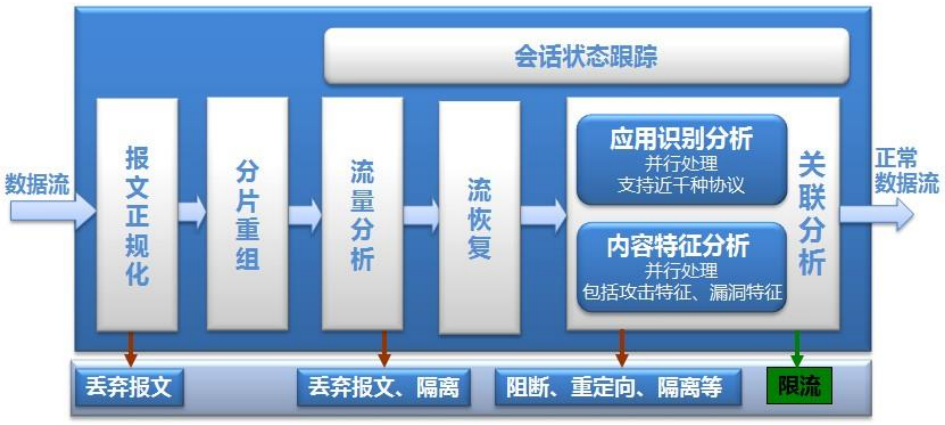
- **网关型网页防篡改**

此功能是深信服下一代防火墙 NGAF-服务器防护中的一个子模块，其设计目的在于提供的一种事后补偿防护手段，即使黑客绕过安全防御体系修改了网站内容，其修改的内容也不会发布到最终用户处，从而避免因网站内容被篡改给组织单位造成的形象破坏、经济损失等问题。

- **基于应用的深度入侵防御**

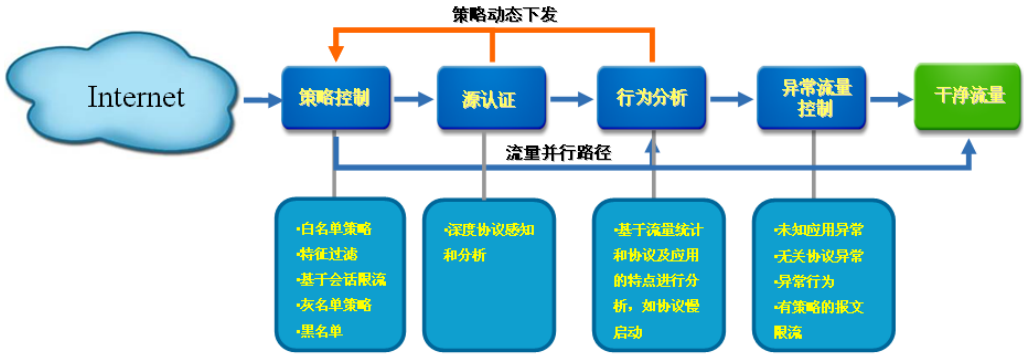
NGAF 基于应用的深度入侵防御采用六大威胁检测机制：攻击特征检测、特殊攻击检测、威胁关联分析、异常流量检测、协议异常检测、深度内容分析能够有效的防止各类已知未知攻击，实时阻断黑客攻击。如，缓冲区溢出攻击、利用漏洞的攻击、协议异常、蠕虫、木马、后门、DoS/DDoS 攻击探测、扫描、间谍软件、以及各类 IPS 逃逸攻击等。

深信服 NGAF 融合多种应用威胁检测方式，提升威胁检测的精度。检测方式主要包含 6 种检测方式：攻击特征检测、特殊攻击检测、威胁关联分析、异常流量检测、协议异常检测、深度内容分析。



- **智能的 DOS 攻击防护**

NGAF 采用自主研发的 DOS 攻击算法，可防护基于数据包的 DOS 攻击、IP 协议报文的 DOS 攻击、TCP 协议报文的 DOS 攻击、基于 HTTP 协议的 DOS 攻击等，实现对网络层、应用层的各类资源耗尽的拒绝服务攻击的防护，实现 L2-L7 层的异常流量清洗。



- **智能的用户身份识别**

NGAF 用户识别功能可以与 8 种认证系统（AD、LDAP、Radius 等）、应用系统（POP3、SMTP 等）无缝对接，通过单点登录的方式自动识别出网络当中 IP 地址对应的用户信息，并建立组织的用户分组结构。

3.4.3 服务器

DELL PowerEdge R720

- **高性能计算**

借助下一代英特尔®至强®E5-2600 系列处理能力和多达 24 个 DIMM，显著提升应用程序性能。英特尔®至强®E5-2600 处理器采用 32 纳米处理技术构建，可实现计算密集型任务的超快处理。

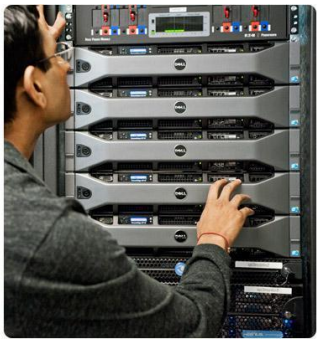
- **高级的 I/O 功能**

利用包含集成式第三代 PCIe 扩展插槽的 PowerEdge R720 均衡且可扩展的 I/O 功能，增强您的数据中心的性能。

- **灵活且可扩展的网络**

借助使您能够充分利用额外的 I/O 性能的功能，调整您的网络吞吐量以满足您的应用程序需求。

- **不打折扣的工作效率**



借助 PowerEdge R720 机架式服务器，在大中型企业的要求苛刻的虚拟化、数据库和企业资源规划(ERP)工作负载中实现最高效率。

- **强大的系统管理功能**

借助硬件驱动的智能化系统管理、全面的电源管理和其他创新型管理工具，体验轻松的生命周期管理性。

- **增强运营效率**

借助 R720 基础架构所具有的下一代可靠性、可用性和可维护性(RAS)功能，维持较高的数据中心工作效率、安全性和维护水平。

- **多种存储容量和性能**

借助 PowerEdge R720 机架式服务器的灵活 I/O 和存储选项，与时俱进，并对数据的呈指数级增长实行高效管理。

3.4.4 外接存储设备

新存储推荐 **Dell PowerVault MD3600f**，非常适用于需要高可用性、高性能和业务连续性的入门级存储整合，而且丝毫不会影响易用性和可靠性。此设计支持多种硬盘类型、RAID 级别和多用途的软件选项。其介绍、特性与优势如下：

- **与高性能、高容量的存储相整合。**

  MD3 光纤通道阵列系列可选配标准 2U 阵列或 4U 高密度阵列，非常适用于需要高可用性、高性能和业务连续性的入门级存储整合。

- **借助 PowerVault MD3600f，可实现高密度，且占用空间更小。**

  借助高性能、高密度的 PowerVault MD3600f 2U 阵列，您可以大幅提存储容量，而不会增加数据中心的占用空间。

- **利用可选的 PowerVault 软件，保护您的数据。**

  所有 PowerVault MD3 阵列系列均可提供高级功能选项，包括数据保护、快照、数据复制、加密和安全的数据删除。

- **扩展能力**
  - 利用 MD1200，MD3600 最多可扩展至 192 个硬盘
  - 最多可配置十二个 3.5 英寸 SAS、近线 SAS 和固态硬盘
  - 最多可支持 64 台主机
  - 可通过最多八个 MD1200 或 MD1220 扩展盘柜来扩展容量
  - 单控制器或双控制器选项
- **RAID 级别**
  - 支持的 RAID 级别有：0、1、10、5、6
  - 在 RAID 0、1、10 中，每组最多包含 192 个物理磁盘
  - 在 RAID 5、6 中，每组最多包含 30 个物理磁盘
  - 最多包含 512 个虚拟磁盘

3.4.5 网络交换设备

LAN 交换机选用 **Cisco 2960**，产品简介如下：

配备 LAN Base 软件的 Cisco® Catalyst® 2960 系列交换机，是一系列采用以太网供电 (Power Over Ethernet – PoE) 或非 PoE 配置，可提供桌面快速以太网和千兆以太网连接，并可为入门级企业、中间市场和分支机构网络实现高级局域网服务的固定配置独立式智能以太网设备（请参见图 1）。Cisco Catalyst 2960 LAN Base 系列可提供集成安全性，包括网络准入控制 (NAC)、高级服务质量 (QoS) 和为网络边缘提供智能服务的永续性。

- **Cisco Catalyst 2960 LAN Base 系列可实现**
  - 为多达 24 个端口提供完全 15.4 瓦功率的 PoE 配置

- 在网络边缘提供高级访问控制列表 (ACL) 和增强安全性等智能化特性
- 支持千兆以太网上行链路灵活性的两用上行链路，允许使用铜缆或光纤上行链路；其中每个两用上行端口分别拥有一个 10/100/1000 以太网端口和一个基于小形可插拔 (SFP) 的千兆以太网端口，每次有一个端口处于激活状态
- 采用高级 QoS、速率限制、ACL 和组播服务，提供网络控制和带宽优化
- 根据用户、端口和 MAC 地址，并通过多种不同的身份验证方法、数据加密技术和 NAC，提供网络安全性
- 采用 Cisco Network Assistant 软件，轻松进行网络配置、升级和故障排除
- 采用 Smartports 对专业应用进行自动配置

SAN 交换机选用 Cisco

4. 实施计划安排

5. 培训标准：

(1) 附赠产品相关资料

(2) 服务器配置

(3) 交换机配置

(4) 存储配置

(5) 软件配置

(6) 相关策略部署

(7) 相关应用测试

(8) 灾难恢复测试

6. 售后服务承诺（一年）：

6.1.1.1 专业售后服务：

(1) 用户通过电话、E-MAIL、传真等方式将问题或要求反应到客户经理。

(2) 客户服务经理安排相关的工程师为用户服务。

(3) 工程师通过电话支持、远程登陆、上门服务、季度巡检（每年 4 次）等方式响应客户的要求。

(4) 响应时间为 15 分钟内电话支持及半小时内远程在线支持，如不能解决则上门服务，外省市出行所需的差旅费，伙食费，住宿费全部由用户承担。

(5) 电话邮件支持服务响应时间为每个工作日上午 9:30-下午 17:30（节假日除外）。

(6) 工程师如果解决不了的特殊安全问题，会即时将问题反映到赛门铁克安全响应中心(SOC)。

(7) 工程师在完成服务后将服务记录提交给客户经理。

(8) 客户经理定期对用户进行电话回访。

6.1.1.2 紧急事件响应服务：主要包括重大安全漏洞的发现、大客户的重大安全事件，遇到此类事件应遵循以下流程：

(1) 建立紧急响应小组：小组成员由客户经理、工程师共同组成。

(2) 分析问题，制定紧急响应方案和工作流程。

(3) 客户服务经理安排工程师上门服务。

(4) 工程师记录响应服务全过程。

(5) 响应结束后整理所有相关文挡，形成响应事件报告。

6.1.1.3 以上的服务不包含以下内容:

(1) 由于贵方私自更改计算机硬件和软件的配置而导致的软件故障。

(2) 由于遭受病毒、外部攻击等所导致的非容灾部分应用故障。

(3) 其它因不可抗力而导致的软件故障。

6.1.1.4 以下为安全响应等级描述：

层	安全等级描述	性能	可用性	所需解决方法
5	正常操作	系统响应正常。	系统 100% 可用。所有中断均正确排定。	无
4	安全等级 4：问题微不足道，影响很小或无影响	性能比所要求的基准低 10%-30%。	系统、应用程序功能的 90%-95% 可用。	必须在五天内解决

3	安全等级 3： 问题很小，几乎没有影响	性能比所要求的基准低 30%-50%。	系统、用程序功能的 85%-90% 可用。	必须在三天内解决
2	安全等级 2： 问题需要关注，可感受到有影响	性能比所要求的基准低 50%-70%。	系统、应用程序功能的 80%-85% 可用。	必须在一天内解决
1	安全等级 1： 问题很严重，对业务有严重影响	性能比所要求的基准低 70% 或更低。	系统、应用程序功能的 75% 以下可用。	必须在三小时内解决

7. 软件、硬件配置列表