

高校网站群系统的建设思路

庄恩泽

(福建工程学院信息化建设与管理中心 福州 350108)

摘要 当前,网站群的建设已经成为数字化校园建设的重要组成部分。本文以福建工程学院网站群系统为例,从系统整体部署结构、反向代理、负载均衡、SSL卸载及相关控制策略等角度,介绍了高校网站群的关键技术和相关规范,同时对下一代融媒体网站群的应用前景进行了展望,以为高校网站群建设工作提供参考和借鉴。

关键词 数字化校园;网站群系统;安全等级保护

中图分类号 TP393.092 DOI:10.16707/j.cnki.fjpc.2021.04.006

Research on the Construction of Website Group System in Colleges and Universities

ZHUANG Enze

(Center for Information Development and Management, Fujian University of Technology, Fuzhou, China, 350108)

Abstract The construction of website group has become an important part of the current digital campus construction. Taking the website group system of Fujian Institute of Technology as an example, this paper discusses the key technologies and related specifications of the university website group from the perspective of the overall deployment structure, reverse proxy, load balancing, SSL unloading and related control strategies of the system. In addition, this paper also looks forward to the application prospect of the next generation of financial media website group. this paper can provide reference for the construction of university website group.

Keywords Digital Campus; Website Group; Safety Level Protection

1 引言

随着高校的职责划分日益明确,二级学院/机关部处的不断增设,网站的重要性在高校信息化建设的进程中与日俱增。与此同时,如何对高校的所有网站资源进行统一、有效的管理,实现各门户网站间的信息共享,以及对所有网站的统一运维和统一安全防护显得至关重要。建设网站群系统是当前各高校解决上述问题的主流方案^[1]。所谓网站群系统,是将原先分散部署、由学院/部处各自管理和维护的门户网站统一部署到同一个平台上,并通过同一套CMS(Content Management System,内容管理系统)进行网页模板的制作和管理、用户账号及权限管

理、文章内容的分级审核和发布。本文以福建工程学院网站群系统为例,对高校网站群系统建设过程中的关键技术和相关规范进行简要介绍。

2 网站群总体架构

福建工程学院于2011年完成了网站群系统的建设和整体部署。该网站群的总体架构如图1所示。采用发布/制作相分离的方式,由一台制作服务器、一台数据库/文件备份服务器和多台静态发布服务器组成。其中,制作服务器用于建设、管理、维护网站和信息管理,部署网站群的CMS系统;发布服务器用于静态网页的发布。网站管理员在制作服务器上发布的文章、附件等内容通过数据镜像备份

本文得到2020年福建省中青年教育科研项目(科技类)《基于云计算的高校网络信息运维服务平台研究》(No.JAT200356)资助。庄恩泽,男,1991年生,硕士,助理实验师,主要研究领域为数字化校园、教育信息化。E-mail: zhuangenze@fjut.edu.cn。

工具 rsync 实时同步至发布服务器上,生成静态网页以供用户访问。文件备份服务器定时对网站群的站点目录和 MySQL 数据库进行备份,可将备份文件同步至其它服务器上,实现主从备份,提高系统的高可用性。

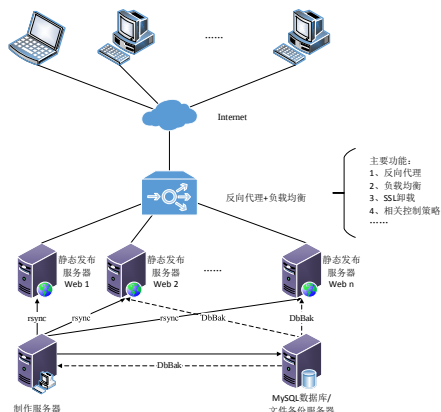


图1 福建工程学院网站群总体架构

该网站群系统达成了以下建设目标:

(1) 实现信息资源的有效共享和管理。通过网站群系统创建的所有站点的信息在保持相对独立的同时,又可以实现站点间的信息共享,避免了“信息孤岛”的产生,从而降低了维护难度,保证了权威信息的一致性。

(2) 各站点间采用垂直管理模式,形成与高校的管理体系相一致的树状体系结构。通过建设网站群系统,使得上级站点可以拥有、管理、分配下级站点的所有资源,同时各子站点内的用户职责得以明确,从而实现了各网站的集中、统一管理。

(3) 提供统一的网页模板^[2],便于后期网站调整,并能实现页面的自适应和个性化定制。网站群系统为用户提供了一系列支持响应式布局的网页模板,用户可以用拖拽方式自由配置,实现了模板栏目的自由组合。如需更改网页样式,仅需通过编辑HTML和CSS文件即可实现,无需编写前后端交互代码,使非专业人员也极易上手。

同时,福建工程学院依照等级保护第三级的要求,对网站群系统实施SSL/TLS证书的统一签发部署,完成了三级等保的备案和测评,建立起完善的整体安全防护体系。

3 系统安全风险与应对策略

现阶段高校网站群系统面临的主要安全风险包括DDoS攻击、xss注入、SQL注入、中间人攻

击等Web攻击行为,导致网页存在被篡改、挂马的可能性,敏感信息也有可能被窃取和泄露;同时高校网站日均访问量大、增长速度快,因此存在服务器无法承担大量用户并发访问,而导致网站群整体性能降低的风险。与上述风险对应的安全策略包括负载均衡、反向代理、SSL加密等^[3-5]。

3.1 负载均衡

负载均衡即由若干台功能相同的服务器组成一个集群,并通过某种方式,将Internet上的用户请求均衡地分配给集群中的某台服务器,由该服务器单独作出响应的技术。负载均衡能够实现流量的均匀分配、优化资源使用、避免过载访问。当其中一台服务器发生故障时,可由其余服务器继续承担全部负载,提升了集群的灾备能力。

常见的Web负载均衡方法包括:(1)DNS负载均衡,即通过在DNS服务器上对同一域名配置多条IP地址记录,当用户访问该域名时,DNS服务器将解析请求按照IP地址记录的顺序返回不同的解析结果,从而将客户端的请求引导到不同的服务器上,实现负载均衡。(2)硬件负载均衡,即通过单独的设备实现负载均衡。此类设备通常称为负载均衡器,常见的包括四/七层负载均衡交换机等。

(3)软件负载均衡,即通过软件方式实现负载均衡,如具有四层负载均衡功能的LVS(Linux Virtual Server),以及基于HTTP、同时具有反向代理和七层负载均衡功能的Nginx、L7SW、HAProxy等。

3.2 反向代理

反向代理(Reverse Proxy)服务器部署在客户端与Web服务器之间,当客户端发起连接请求时,由代理服务器接受请求,并转发至内网服务器,再由内网服务器将得到的结果通过反向代理服务器返回给请求连接的客户端。外部网络客户端仅能获取反向代理服务器的虚拟IP地址,而不能获取集群内部服务器的真实IP地址。使用反向代理技术的优势主要包括以下几点:

(1)代理服务器未像发布服务器和制作服务器一样保存网站的真实数据,因此当反向代理服务器遭受外部网络攻击时,静态页面和动态资源等并不会遭到破坏,从而增强了Web服务器的安全性。

(2)由于网站群系统部署了反向代理服务器,校园内部的二级站点共享同一个在Internet中注册的IP地址或域名,使有限的IP地址资源得以节约。

(3)反向代理服务器的缓存网页功能使用户

可直接从中获取页面内容，极大地提高了用户的访问速度，减轻了内部服务器负荷。

3.3 SSL/TLS加密

浏览器和 Web 服务器之间的通信通常遵循 HTTP 协议,即请求(request)报文和响应(response)报文之间的交互。HTTP 协议的缺陷主要包括:(1)使用明文进行浏览器和服务端间的通信,未对信息进行加密,内容有可能被第三方窃听。(2)无法证明双方接收的信息是否遭到第三方篡改。(3)未对通信双方的身份进行验证,中间人可能伪装成其中任意一方与另一方进行通信,同时无法阻止分布式拒绝服务攻击(DDoS)。

为解决上述问题,通常使用 SSL(Secure Socket Layer, 安全套接层)或 TLS(Transport Layer Security, 传输层安全)协议,在传输层和应用层间加入 SSL/TLS 层^[5],由 SSL+HTTP 构建数据加密通道,实现浏览器和服务端间的安全通信。SSL/TLS 协议的层次结构如图 2 所示:

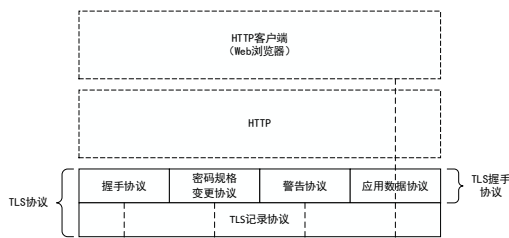


图 2 SSL/TLS 协议的层次结构

SSL/TLS 协议使用对称密码对消息进行加密通信，基于证书对 Web 服务器进行认证，并负责将应用层承载的应用数据传达给通信对象。HTTPS 通信的具体流程如图 3 所示。

4 网站群安全部署实践

4.1 Nginx的部署与配置

Web 服务器又被称为 WWW 服务器或 HTTP 服务器，是运行及发布 Web 应用的容器。其主要功能是部署 Web 应用，并提供用户的网页浏览服务。目前主流的 Web 服务器包括 Apache、Lighttpd、Tomcat、Microsoft IIS 和 Nginx 等。

其中, Nginx 作为一款高性能的 Web 服务器^[6], 将负载均衡方案和反向代理集成在一起, 还可通过配置 SSL/TLS 证书实现网页的 https 访问, 相较于 Apache 具有部署简单、配置灵活、执行效率极高的优点。同时由于网站群系统包含大量图片、文件等

静态资源，而 NginX 易于实现动态请求和静态请求的分离，可将所有静态资源放到 NginX 上以加快解析速度，因此更适用于网站群系统的部署需求。

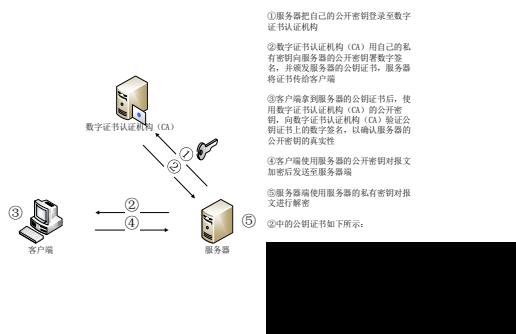


图 3 HTTPS 通信的具体流程

网站群系统的 nginx.conf 配置文件如下所示:

```
upstream webplus {
    server ***.**.***.**:80;
    server ***.**.***.**:80;
    .....
    server ***.**.***.**:80;
    ip_hash;
}
```

```
log_format webplus '$remote_addr - $remote_user [$St
ime_local] "$ssl_protocol/$ssl_cipher" "$request"'
"$status" $body_bytes_sent "$http_referer"
"$http_user_agent" "$http_x_forwarded_for" $upstre
am_addr $upstream_response_time';
```

• • • • •

```
server {
    listen 443 ssl http2;
    server_name *.fjut.edu.cn;
```

```
access_log /var/log/nginx/fjut.edu.cn.log webplus;
```

```
ssl_certificate      /usr/local/openresty/nginx/
conf/ssl-cert/fjut.edu.cn.crt;
ssl_certificate_key  /usr/local/openresty/nginx
x/conf/ssl-cert/fjut.edu.cn.key;
```

```
location / {
    proxy_pass http://webplus;
    proxy_set_header Host $http_host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add
    _x_forwarded_for;
}

error_page 500 502 503 504 /50x.html;
```

```
location = /50x.html {
    root html;
}
}
```

其中，upstream 节点中添加的是网站群的各发布服务器 IP 地址，这样即实现了负载均衡且各服务器的权重是相同的。ssl_certificate 中指定的 crt 文件为 CA 证书，ssl_certificate_key 中指定的 key 文件为密钥文件。listen 指令中指定了需要监听的端口号，并实现了从 http 到 https 的强制跳转。

福建工程学院通过部署、配置 Nginx 负载均衡与反向代理，实现了网站群高并发下的安全、稳定

运行，目前日平均访问者数为 20000+，最高日访问者数可达 170000+。

4.2 网站群部署中的 TLS1.3 协议

2018 年 3 月 4 日，互联网工程任务组（The Internet Engineering Task Force，IETF）发布了最新版本的 TLS 协议，即 TLS 1.3^[7-8]。相较于 TLS 1.2，TLS 1.3 对图 2 中握手层的消息结构进行了调整，同时移除了部分加密性能较弱或利用率不高的算法，引入了一些新的加密算法。TLS 1.3 协议的具体调整方案如表 1 所示。

表 1 TLS3.0 协议的具体调整方案

	移除	新增
握手层消息结构	“改变密码规范”消息；“密钥交换”消息。	Hello 扩展消息；“请求重新握手”消息。
算法	Diffie-Hellman 密钥交换算法；RSA 密钥交换算法；RC4 流密码算法；哈希算法（如 MD5、SHA-1、SHA-224）；部分椭圆曲线算法	AEAD 算法；CFRC 曲线和签名算法；SHA-2 哈希算法

除了部署 TLS1.3 协议，为解决 HTTPS 对 CPU/内存等资源的消耗问题，网站群系统使用了 SSL/TLS 卸载技术，由负载均衡设备实现原服务器上的证书加解密功能。SSL/TLS 证书部署配置如下：

```
# SSL Settings
##

ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLS v1.3; #
Dropping SSLv3, ref: POODLE
ssl_prefer_server_ciphers on;
ssl_session_cache shared:SSL:5m;
ssl_session_timeout 30m;
ssl_ciphers

.....
```

SSL/TLS 卸载的主要优势有如下几点：（1）避免消耗服务器的性能，降低了服务器的负载。（2）负载均衡设备使用专门的 SSL/TLS 卸载硬件芯片，提升了 SSL/TLS 的处理能力。（3）无需在多台服务器上管理和配置证书，方便管理员操作。（4）可在负载均衡设备上根据请求/响应内容灵活设置策略，提升了应用安全性。

5 总结和展望

下一步的工作将在继承网站群安全性、稳定性、易用性、扩展性等优秀特点的基础上，打造新一代融媒体平台^[9]，即通过建设“底层运行平台→中台服务加工→前台用户展现”的三层平台架构，

实现微博、微信等新媒体账号的统一授权管理，打通站群和新媒体间的壁垒，使得资讯和媒体资产能够互通，并采取网络爬虫等新技术进行实时数据的监控、采集、分析和预警，构建多媒体、多形式、多渠道、多终端的全媒体共享机制。

参 考 文 献

[1] 张咏梅,贾艳梅,蒲在毅.高校站群系统建设与应用.网络空间安全, 2018, 9(06): 86-89

[2] 路遥,任晓霞,侯静,李笑难,马皓.新形势下高校网站群建设与服务管理探究;以北京大学为例.实验技术与管理, 2020, 37(09): 32-34

[3] 杨紫淇,蔡葵,张皓晨,范艳芳.基于负载均衡的VEC服务器联合计算任务卸载方案.计算机科学, 2021, 48(01):81-88

[4] 何辉,樊小龙,常玮,吴倩,石全民,韩玮.基于开源方案的在线课程平台构建;以兰州工业学院“开物云课堂”为例.深圳大学学报(理工版), 2020, 37(S1):31-35

[5] 邓真,刘晓洁.HTTPS协议中间人攻击的防御方法.计算机工程与设计, 2019, 40(04):901-905

[6] 徐云涛,许武军,翟梦琳.基于B/S架构的高并发虹膜识别系统.计算机工程, 2019, 45(08):102-106,112

[7] 张兴隆,程庆丰,马建峰.TLS 1.3 协议研究进展.武汉大学学报(理学版), 2018, 64(06):471-484

[8] 沈若愚,卢盛祺,赵运磊.TLS1.3 协议更新发展及其攻击与防御研究.计算机应用与软件, 2017, 34(11):264-269,329

[9] 陈雄,杜义华,郭小龙.政务网站新媒体发布集成环境建设探讨.计算机系统应用, 2016, 25(08):86-90