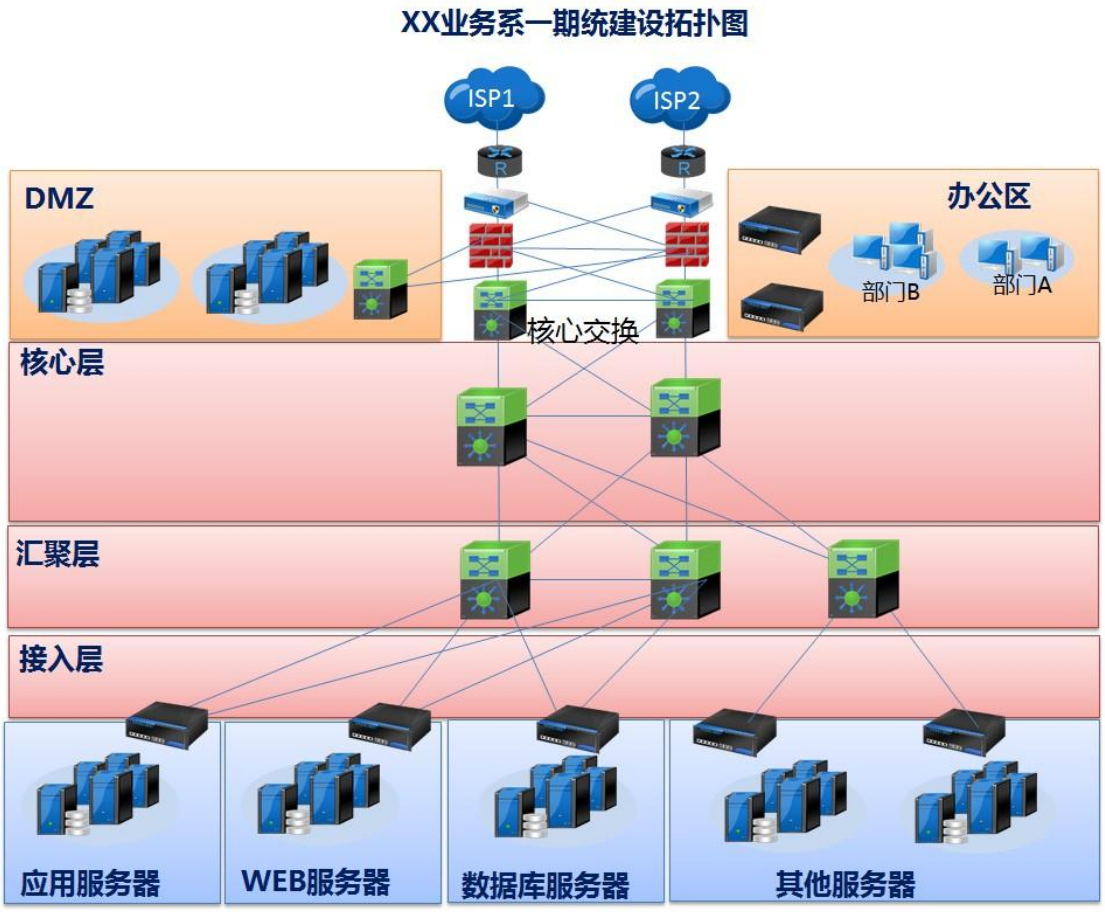
业务系统应用安全加固解决方案

一、应用背景

网络的飞速发展促进了各行业的信息化建设，近几年来 XX 单位走过了不断发展、完善的信息化历程，现已拥有技术先进、种类繁多的网络设备和应用系统，构成了一个配置多样的综合性网络平台。随着互联网的飞速发展，外部网络安全日趋严重，面对业务系统的信息安全攻击逐渐从网络层向应用层和系统层迁移。各类新型的黑客技术手段、计算机病毒、系统漏洞、应用程序漏洞以及网络中的不规范操作对单位业务系统均有可能造成严重的威胁。在给内、外网用户提供优质服务的同时，也面临着各类的应用安全风险，为了加强业务系统的防护能力，提高业务系统安全性，并且满足等保三级的要求，单位将启动二期业务系统应用安全加固的安全建设。

二、需求分析



XX 业务系统是整个业务的支撑，应对业务系统进行重点防护，如果业务系统的访问行为控制不利，非授权用户可能窃取机密数据、删除和修改业务数据、甚至植入病毒，引起系

统中断服务或瘫痪。同时，如果不对日益猖獗的病毒问题进行防御，有可能从外部或内部其他区域引入病毒，影响业务系统的正常运行。同时，垃圾邮件的泛滥将阻碍业务的正常开展，同时可能引入注入病毒、木马、钓鱼攻击等众多的安全风险。最后，操作系统漏洞、业务系统漏洞、应用软件漏洞不断被发现，如果不重视业务系统日常的安全运维，业务系统将可能由于安全漏洞的发现、由于缺乏及时的响应，而引入风险、造成破坏。

目前 XX 单位正在着手进行二期 XX 业务系统网络建设，本次规划内容主要涉及针对业务系统的应用安全加固的内容。通过对该业务系统目前的安全状况以及二期建设目标分析，XX 业务系统目前还存在以下几个方面的问题：

1、业务系统与内外网对接没有实现有效的边界访问控制，无法界定用户访问是否为合法请求；

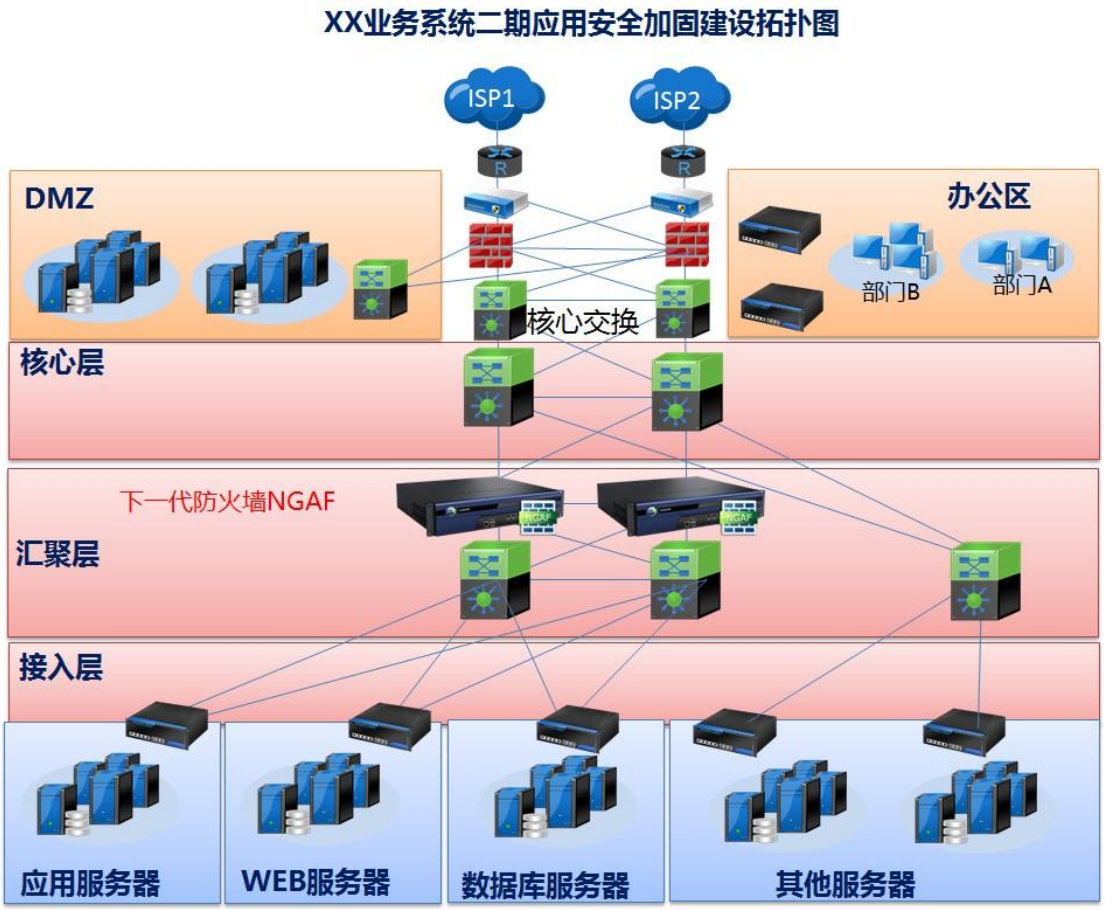
2、对于流经业务系统的数据没有有效的流量清洗的能力，无法识别流量是正常的访问请求还是 DOS/DDOS 拒绝服务类的攻击；

3、对于夹杂在数据流中的病毒、木马、蠕虫没有良好的检测能力，很难避免在业务交互过程中由于数据中包含病毒、木马、蠕虫等威胁对业务系统造成的危害；

4、服务器系统底层漏洞攻击防护仅依靠时效性不强的手动补丁更新，缺乏有效的防护手段，尤其缺乏零日漏洞攻击的防护能力；

5、流经业务系统的数据没有应用层攻击（如 web 攻击）的检测能力，难以保证业务系统 Web 应用程序以及后台数据库不被攻击；

三、解决方案



深信服为 XX 单位提供针 XX 业务系统服务器集群完整的应用安全加固安全解决方案。

通过在服务器集群汇聚交换前双机部署两台深信服下一代应用防火墙 NGAF，可实现业务系统服务器的逻辑隔离，防止来自网络层面、系统层面、应用层面以及数据层面的安全威胁在业务系统数据中心各区域内扩散。

二期建设采用业务系统一站式应用安全加固部署方案，通过深信服下一代防火墙 NGAF 的部署可以从从攻击源头上帮助 XX 单位防护导致业务系统服务器区内业务各类网络、系统、应用、数据层面的安全威胁；同时深信服下一代防火墙 NGAF 提供的双向内容检测的技术帮助用户解决攻击被绕过后产生的网页篡改、敏感信息泄露的问题，实现防攻击、防篡改、防泄密的效果。

1、深信服下一代防火墙 AF-8020 双机部署于核心交换前可实现业务系统服务器区一站式整体安全防护；

2、通过防火墙子系统模块的访问控制策略 ACL 可实现网络安全域划分，阻断各个区域间的网络通信，防止威胁扩散，防止访问控制权限不当、系统误配置导致的敏感信息跨区域传播的问题；

3、通过 DDOS/DOS 子系统功能模块进行网络层面的安全加固，可以防止利用协议漏洞对服务器发起的拒绝服务攻击使得服务器无法提供正常服务，导致业务中断等问题；

4、通过防病毒子系统功能模块可实现各个安全域的流量清洗功能，清洗来自其他安全域的病毒、木马、蠕虫，防止各区域进行交叉感染；

5、利用入侵防御子系统功能模块可实现对服务器集群操作系统漏洞（如：winserver2003、linux、unix 等）、应用程序漏洞（IIS 服务器、Apache 服务器、中间件 weblogic、数据库 oracle、MSSQL、MySQL 等）的防护，防止黑客利用该类漏洞通过缓冲区溢出、恶意蠕虫、病毒等应用层攻击获取服务器权限、使服务器瘫痪导致服务器、存储等资源被攻击的问题；

6、通过 web 安全子系统功能模块的开启，可实现对各个区域（尤其是 DMZ 区）的 web 服务器、数据库服务器、FTP 服务器等服务器的安全防护。防止黑客利用业务代码开发安全保障不利，使得系统可轻易通过 web 攻击实现对 web 服务器、数据库的攻击造成数据库信息被窃取的问题；

7、通过信息泄漏防护子系统功能模块的开启，可自定义业务系统的敏感信息防止黑客绕过防御体系窃取业务系统的敏感信息；

8、通过防篡改子系统功能模块的开启，可防止黑客利用各层面安全漏洞非法篡改业务系统合法界面，防止被篡改界面发布于众；

9、通过风险评估子系统模块的启用对服务器集群进行安全体检，通过一键策略部署的功能开启入侵防御子系统模块、web 安全子系统模块的对应策略，可帮助管理员的实现针对性的策略配置。

10、通过智能联动模块的应用，可形成防火墙子系统功能模块、入侵防御子系统功能模块、web 安全子系统功能模块的智能联动，有效的防止工具型、自动化的黑客攻击，提高攻击成本，可抑制 APT 攻击的发生。