针对政府用户的整体解决方案

■ **文档编号**	请输入文档编号	■ **密级**	请输入文档密级
■ **版本编号**		■ **日期**	2015/4/13

■ **版权声明**

■ **版本变更记录**

时间	**版本**	**说明**	**修改人:孙展**
2015/4/13			

■ **适用性声明**

本模板用于撰写**般固(北京)科技股份有限公司**内外各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

目录

一. 行业背景

以 Internet 为代表的全球性信息化浪潮日益深刻，信息网络技术的应用正日益普及和广泛，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展，典型的如行政部门业务系统、金融业务系统、企业商务系统等。伴随网络的普及，安全日益成为影响网络效能的重要问题，而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求。如何使信息网络系统不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化健康发展所要考虑的重要事情之一。

当前，我国已将电子政务建设作为今后一个时期国家信息化的重点，到“十五”期末，我国将初步完成发展电子政务的基础性工作。在政府大力推进电子政务的同时，信息安全问题也日益突出。一般来说，政府的电子政务体系包含三个部分：一是各级政府机关内部局域网，机关内部通过在内部网实现办公自动化。二是各级政府部门通过政府专网互联实现信息共享及实时通信。三是政府职能部门通过互联网向公众发布信息并在互联网上提供公众服务，实现政府上网。

政府机构从事的行业性质是跟国家紧密联系的，所涉及信息可以说都带有机密性，所以其信息安全问题，如敏感信息的泄露、黑客的侵扰、网络资源的非法使用以及计算机病毒等。都将对政府机构信息安全构成威胁。为保证政府网络系统的安全，有必要对其网络进行专门安全设计。

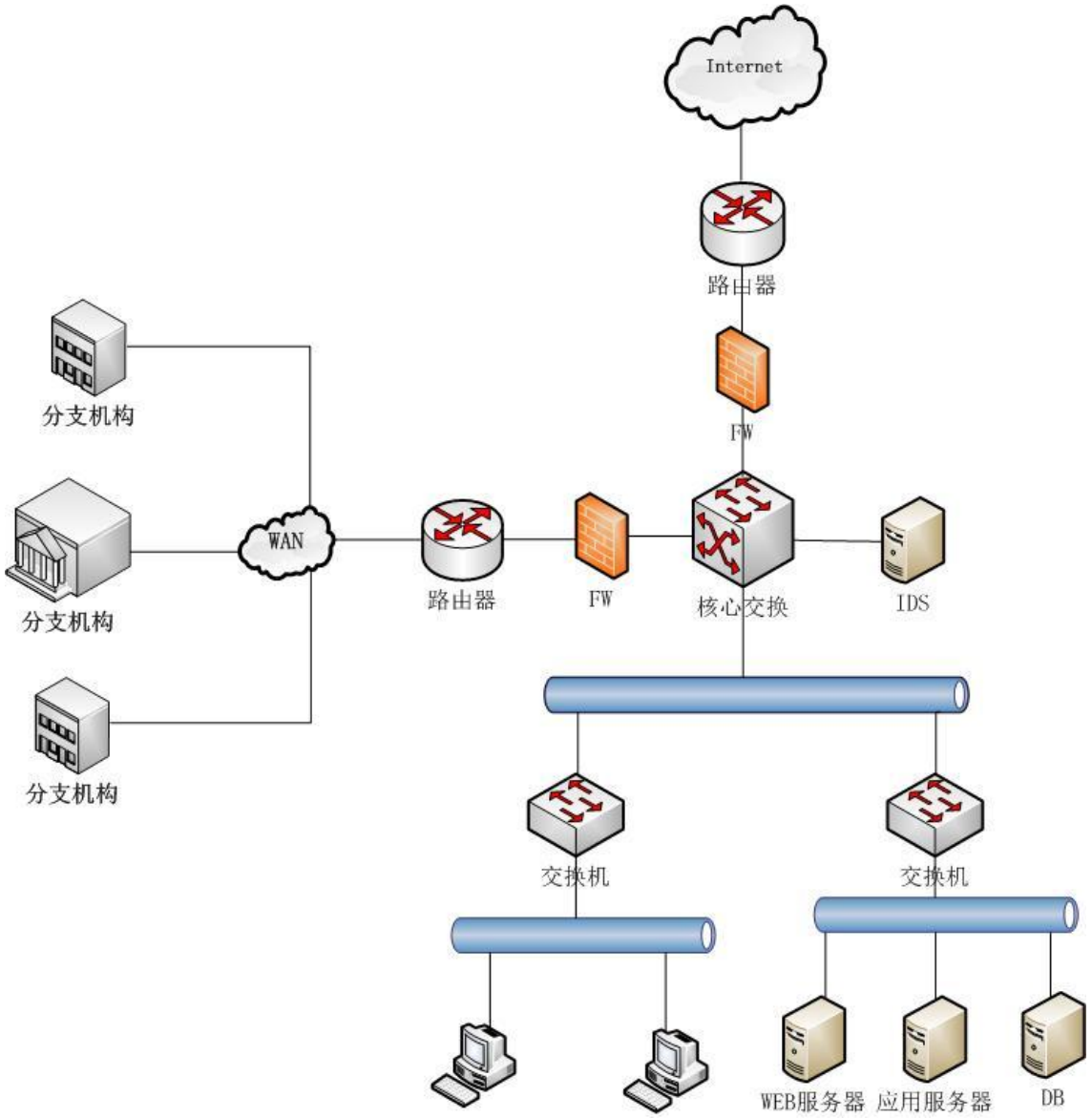
由于政府机关信息有较高的保密性，要求有效阻止木马、蠕虫类病毒的传播，及时修补系统漏洞， 并能够有效阻止来自 Internet 的各种恶意攻击，如 DDoS 等，杜绝安全隐患。在管理上，一般采用集中进行信息安全管理，以保障整个网络的安全。

般固（北京）科技股份有限公司针对日益突出的服务器压力过大问题推出了一系列负载均衡产品。旨在推动我国应用交付事业的发展，为我国的信息网络保驾护航。为广大的网络用户提供一个安全、稳定的网络应用平台。本方案就是针对我国政府上网工程提供的一套整体解决方案。

二. 政府用户网络应用现状

2.1 政府网络应用现状简述

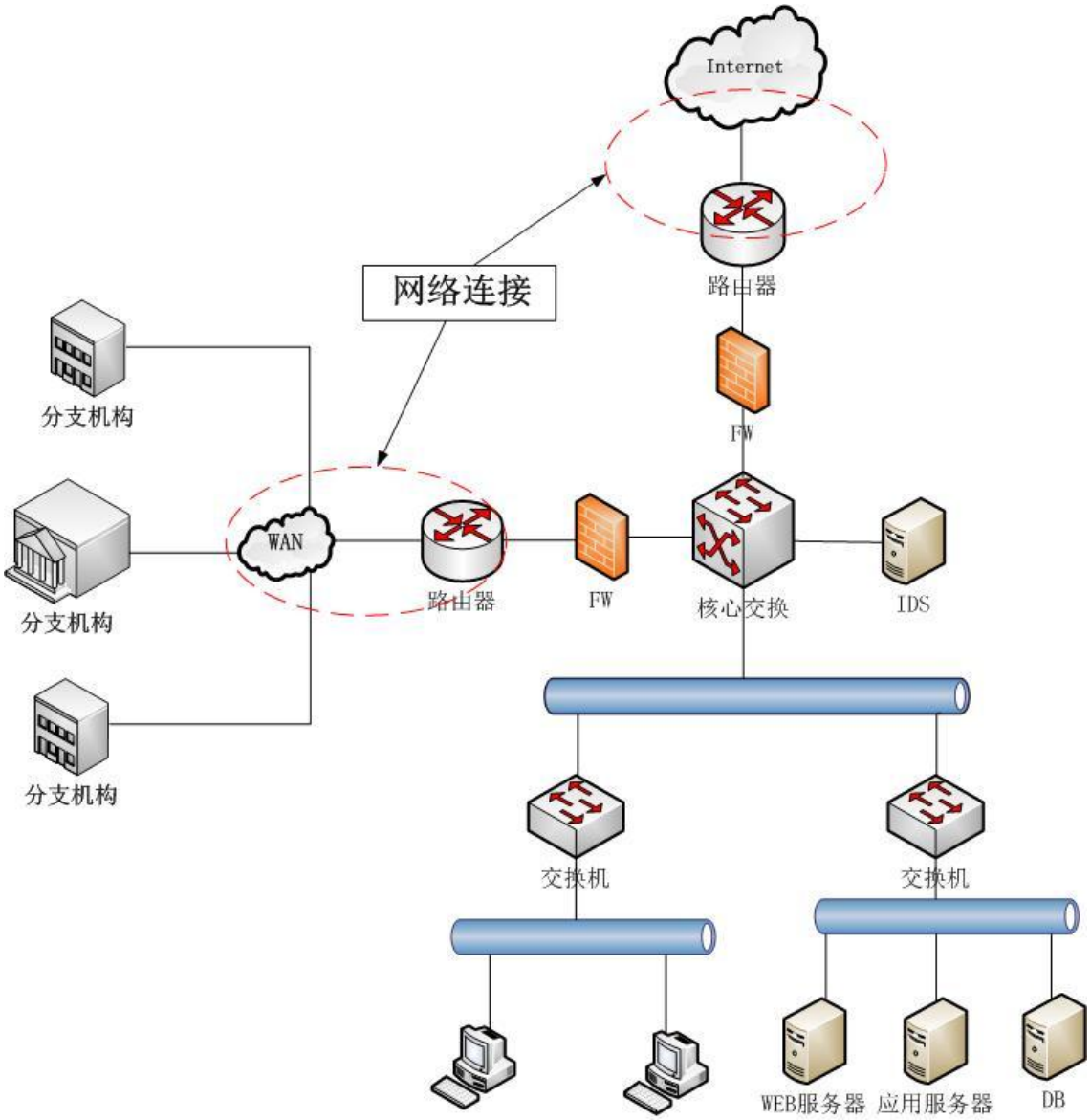
一个典型的政府的网络拓扑结构图如下图所示：



可以看出上述典型的政府网络大致由 3 部分组成：

- 网络连接部分
- 网络安全部分
- 网络应用部分

三. 广域网链路现状



网络连接部分还可以分为 Internet 连接部分和专网连接部分：

Internet 连接部分

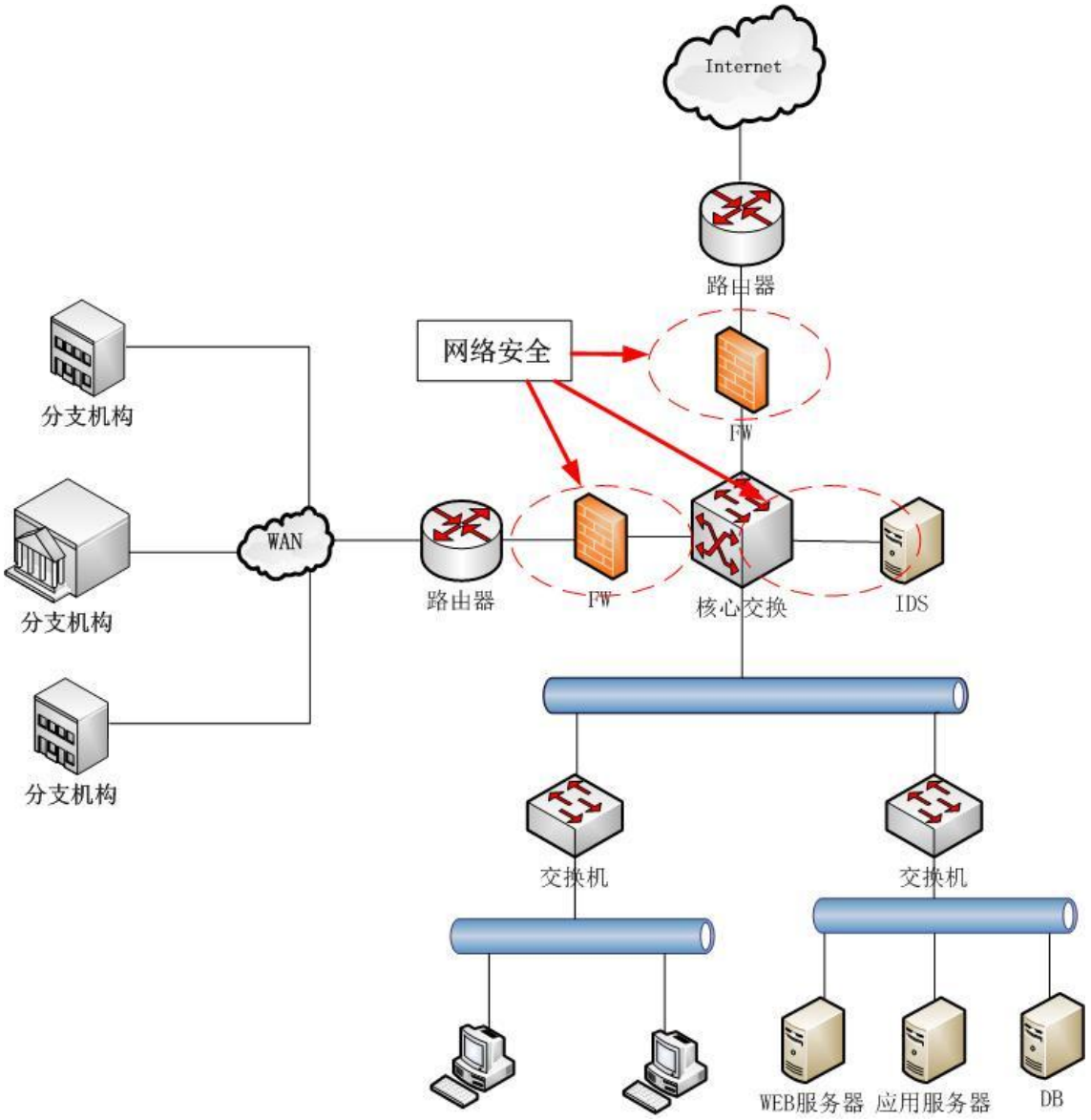
Internet 连接部分是指政府网络数据中心通过 ISP 运营商的链路连接到 Internet，用于政府对外的网上公共信息发布、为 Internet 用户提供政府网上应用，同时政府内部用户也可以访问 Internet 上的资源。

专网连接部分

专网连接部分用于政府网络连接各地分支机构。

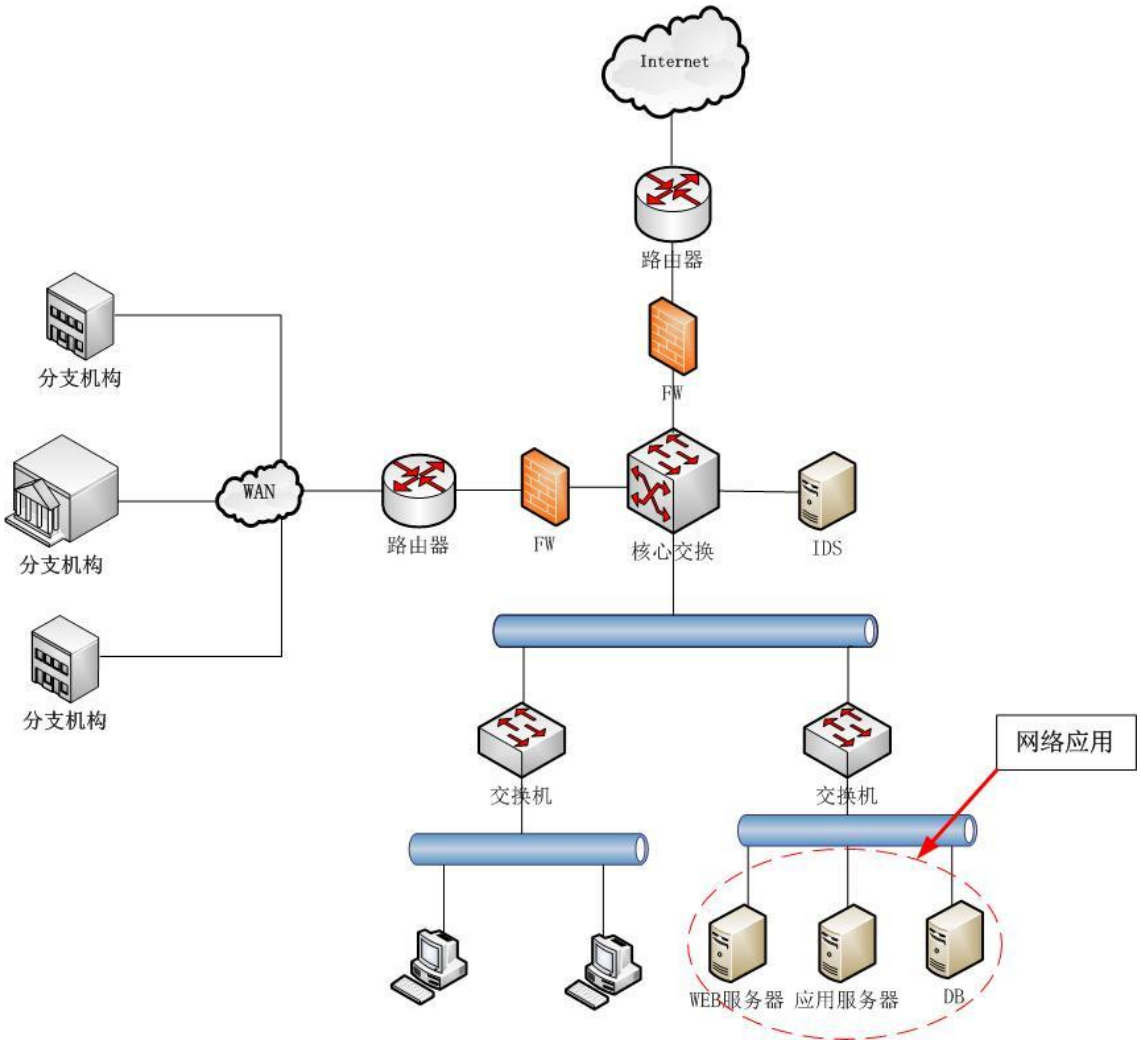
分支机构的内部用户通过专网连接访问数据中心的应用服务器，例如：WEB 服务器，E-Mail 服务器等，同时也可以通过数据中心的 Internet 链路访问 Internet 上的资源。

四. 网络安全防护现状



网络安全部分通常由防火墙、入侵检测系统（IDS）和防病毒网关等设备构成，用于制定内部信息资源的不同访问策略，保护数据中心的应用免受来自 Internet 的网络攻击。

五. 网络应用现



网络应用由政府对外 WWW 信息发布系统，业务应用系统和后台数据库系统组成

政府网络中存在的缺陷

从上图中可以看出，在政府网络中存在很多网络设计上的缺陷，总结起来可以分为以下三个部分的问题：

- 网络连接部分存在的问题
- 网络安全部分存在的问题
- 网络应用部分存在的问题

下面我们就这三部分存在的问题做详细描述：

5.1 广域网链路存在的缺陷

政府网络连接部分存在的问题可以分为以下两部分：

- 政府中央机构 Internet 链路存在的问题：
- 各分支机构到中央机构之间广域网链路存在的问题：

5.1.1 政府中央机构 Internet 链路存在的问题：

链路的单点失效性：

采用单一 Internet 连接链路存在单点失效性，一旦该链路出现故障将造成整个网络的瘫痪。

链路性能的瓶颈：

单一 Internet 连接链路的带宽资源是有限的，无法满足政府内部全体用户对网络访问 Internet 时带宽不断增长的需求，同时也无法大量的 Internet 上的用户对政府的访问。

访问速度快慢不一

内部用户访问 internet 资源时，或外部用户访问政府发布的内部资源时，会受到 ISP 提供商的不同， 而产生访问快慢不一的现像。例如：如果政府采用的 ISP 是通过网通接入的，在访问处于电信的资源时，会由于不同 ISP 之间互连互通的问题造成访问变慢，而访问网通资源时，就不会存在问题。

网络安全防护能力弱：

目前 Internet 上的各种各样的网络攻击层出不穷，路由器自身对网络攻击的防护能力非常有限，DOS/DDOS 网络攻击会对广域网络由器产生严重的影响。

5.1.2 各分支机构到中央机构之间广域网链路存在的问题：

链路的单点失效性：

各省级机关到中央机构之间采用单一广域网链路，存在单点失效性，一旦该链路出现故障将造成该省级机关无法访问中央机构和 Internet。

链路性能的瓶颈：

各省级机关到中央机构之间采用低速的广域网链路（Frame Relay，DDN），而各分支机的用户访问中心的应用服务器的网络流量，以及各分支机的用户访问 Internet 的网络流量都要经过这条单一的广域网链路，因此无法满足用户对网络带宽不断增长的需求。

网络安全防护能力弱：

各省级机关中收病毒感染的机器会向中央机构发送攻击数据包，造成各省级机关到中央机构之间的链路拥塞，从而影响网络中的关键应用的正常运行

5.2 网络安全防护存在的缺陷

网络安全设备的单点失效性：

单一的网络安全设备存在单点失效性，例如：图中的防火墙和防病毒设备一旦出现问题，将造成整个网络的瘫痪。

网络安全设备性能的瓶颈：

网络安全设备由于要对进出网络的数据包进行安全性检查，与网络路由器和网络交换机相比，性能通常会降低很多，例如防病毒设备的网络吞吐量通常只有 3－10Mbps。因此网络中的安全设备通常都是制约网络传输速度的瓶颈点。

安全体系架构存在漏洞：

防火墙可以基于网络中的 TCP、UDP 端口对网络流量进行访问控制，并且可以对基于状态的协议进行协议状态检查，因此防火墙通常是在网络第四层上对用户的网络进行保护。但是防火墙无法对基于网络七层中的网络攻击进行防护例如：

- 蠕虫入侵
- 病毒入侵
- 后门攻击

IDS 可以对网络中的数据包进行深入的分析，可以检查到资料包中第 7 层的信息，它具备随时对可疑流量进行检查和识别的能力。但是 IDS 最大的问题是 IDS 并不能阻止攻击的入侵，仅仅能发出告警，而此时网络攻击已经进入到网络内部。

目前我们面临着手段各异形式多样的混合式攻击威胁，这些攻击中应用级层的攻击占了绝大多数，为了抑制这些攻击，Gartner 建议“在作出安全方面的决策时除了考虑简单的静态协议过滤外， 还要考虑对应用内容（网络七层中的攻击特征）进行深入的数据包检查，并阻挡该攻击”。因此，政府在面临多种多样的攻击威胁时，急需找到更严密的安全防护手段。

5.4 网络应用存在的缺陷

应用服务器由于服务器硬件的稳定性、流量压力超载、网络攻击等情况经常会出现意外宕机的情况，从而无法保证网络应用的 7x24 小时的持续性服务。

网络应用的性能瓶颈：

在网络应用系统中，通常会采用多台服务器同时提供服务的方式。但是由于网络中的流量并不均衡，因此经常会出现某台服务器由于访问量过大而宕机，造成网络应用性能的不稳定，从而影响到整个网络应用系统的性能。

网络应用的安全性较差：

- 现有的安全性防护机制通常是针对来自外网的攻击。
- 缺乏针对来自内网的攻击防护机制。
- 现有的安全性防护机制通常是针对整体网络层面的攻击防护，即针对网络 IP 层、TCP/UDP 层的网络 4 层以下的攻击防护。
- 缺乏针对具体的、特定的政府网络应用的特点而专门制定的符合政府网络应用的基于网络 7 层防护的安全性防护机制。

六. 政府网络应用需求分析

6.1 广域网链路需求分析

6.1.1 网络连接方面的需求－多链路负载均衡技术

政府在网络连接方面的需求可以分为以下两部分：

- 中央机构 Internet 网络连接方面的需求
- 各省级机关到中央机构之间网络连接方面的需求

6.1.2 中央机构 Internet 网络连接方面的需求

目前在国内由于多家 ISP 的竞争，Internet 接入链路的成本大幅降低，多链路 Internet 的接入已成为许多用户在的选择网络连接方面的需求。因此在中央机构 Internet 网络连接方面,政府网络将存在如下要求：

提高 Internet 网络链路的可用性：

建议政府采用接入多个 ISP 的方式提高可用性，而当政府网络中心具有多条 Internet 链路后，应提高 Internet 网络链路可用性的智慧检查能力，防止出现由于某一条 Internet 链路的失效造成整体网络的不可访问。

提高 Internet 链路的网络吞吐量：

提高网络中心的 Internet 网络链路的吞吐量，申请多条 Internet 链路

提高 Internet 网络链路的抗网络攻击的能力：

Internet 上的各种各样的网络攻击首先影响的将会是 Internet 网络链路，因此应加强在 Internet 链路上的攻击防护。

6.2 各省级机关到中央机构之间网络连接方面的需求分析

目前各省级机关到中央机构之间通常采用 DDN 等昂贵的专线广域网链路，而目前国内运营商可以提供相对高速同时价格便宜的 Internet 接入链路，例如：ADSL 因此政府网络存在入下要求：

6.2.1 提高省级机关到中央机构的广域网链路的可用性：

如果各地省级机关与中央机构之间存在多条链路，应注意提高省级机关到中央机构的广域网链路可用性的智慧检查，防止出现由于某一条链路的失效造成整个省级机关无法访问到中央机构。增加省级机关到中央机构的链路，增加带宽，同时降低省级机关与中央机构之间广域网链路的成本，利用运营商提供的低价、高速链路，在各地省级机关与中央机构之间增加链路带宽，设法降低减轻各地省级机关与中央机构之间专线的流量压力，降低广域网链路的成本。

6.2.2 提高各个省级机关的网络安全防护能力：

在各个省级机关的广域网出口和 Internet 出口的位置增加网络安全防护的能力，以保证各省级机关的网络安全，同时可以保证一旦某个省级机关内部的用户受到网络攻击的侵袭，那么该网络攻击不会扩散到中央机构，以及其它省级机关。

6.3 网络安全防护需求分析

网络安全方面的需求－防火墙、IDS、防病毒设备负载均衡技术的需求

为了保证政府的网络在网络安全防护方面的高可用性、高性能和安全性，政府在网络安全方面的需求可以分为以下几部分：

提高网络安全设备的可用性：

网络中应具备安全设备的的可用性检查，避免单一的网络安全设备的单点失效性。

提高网络安全设备性能：

在网络中采用多台网络安全设备，避免网络安全设备带来的瓶颈，提高网络传输速度。

完善网络安全体系架构：

现今，各种各样的网络攻击层出不穷，导致防火墙的负荷在不断提高，再相对于网络物理带宽的大幅度提高，防火墙逐渐成为了网络的瓶颈，本案希望使用一组（2 个以上）防火墙采用负载均衡技术提供安全服务，以提升性能。

6.4 安全防护设备需求

当前的黑客攻击，具备层出不穷，隐蔽性强，攻量大，影响广等特点，对安全网关设备提出了更高的要求，因此需要政府的网络中的安全产品提出了新的需求，要求应用安全产品具备防范一系列攻击的智能和性能：

实时安全性：

发现攻击和入侵立即拦截。第二，能够深入检查数据包，防范各种应用层攻击，例如蠕虫、病毒、木马和 Dos 攻击。第三，能够即使拦截大流量，爆发性的 DoS/DDos 攻击，与此同时，要求网络访问正常进行， 网络的性能不能有太大降低。第四，要求安全产品具备数千兆位速度双向扫描的安全检测性能。第五，能够对链路的带宽使用进行有效管理，如对消耗带宽资源非常严重的 P2P 流量进行有效控制，保证关键应用的带宽使用。

6.5 网络应用需求分析

网络应用方面的需求－应用服务器负载均衡技术的需求

为了保证政府的网络应用的高可用性、高性能和安全性，政府的网络应用存在下列需求：

提高网络应用的可靠性：

自动的网络应用可用性检查，保证网络应用的 7x24 小时的持续性服务。

提高网络应用的性能：

如果网络中仅有单台服务器提供网络应用的服务，很难保证网络应用的性能，可以考虑增加相应的服务器数量，配合负载均衡技术来提高网络网络应用的性能。

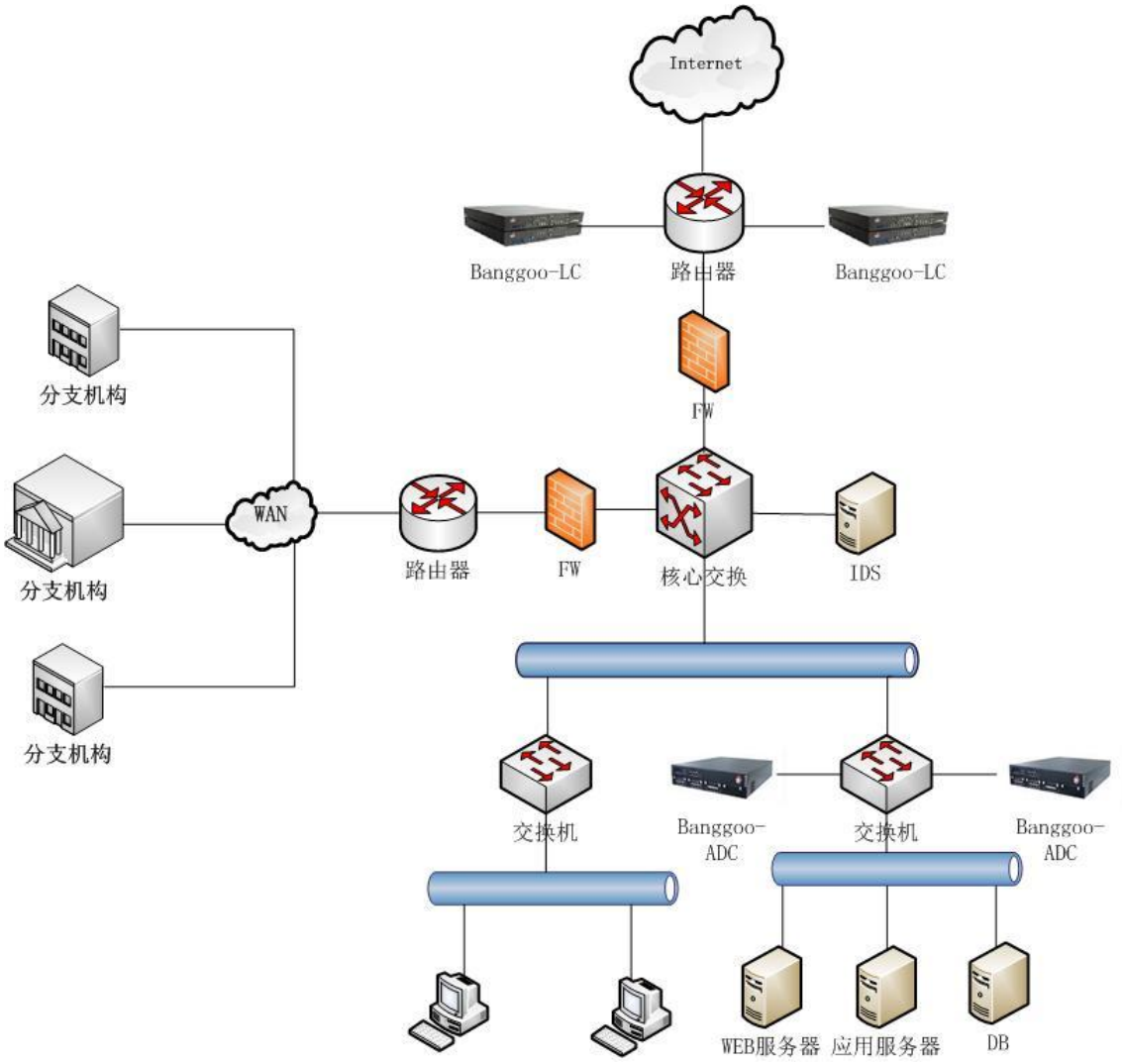
网络应用的安全性较差：

制定针对具体的、特定的网络应用的特点而专门制定的基于网络 7 层防护的安全性防护机制。

七. 般固-整体解决方案

7.1 解决方案拓扑图：

根据上述网络应用现状分析和用户的需求分析，结合般固产品的技术实现和特点，我们建议的政府方案设计包括两大部分，中央机构方案设计和省级机关方案设计，如下图所示：



7.2 般固解决方案简介

建议在中央机构网络各层面上共采用了如下般固的设备，其中包括:

Banggoo-LC 链路负载均衡设备

Banggoo-ADC 服务器负载均衡
该解决方案从功能上分为 2 个部分：

- 连接解决方案部分
- 应用的解决方案部分

般固连接解决方案部分简介：

banggoo-LC 实现多链路的负载均衡和防火墙的负载均衡：

如上图所示，我们建议在网络接入处，部署 banggoo-LC，实现对多条 internet 接入链路的负载均衡，可以同时实现 outbound 流量（内部办公用户访问 internet）和 inbound 流量（internet 用户访问内部服务器）双向的负载均衡。

banggoo-LC 可以配合 banggoo-LC 实现多台防火墙（最多 100 台）的负载均衡，防火墙可以是不同厂家，不同型号，不同性能，大大提供防火墙的扩展性和可用性。

省级机关的 banggoo-LC 实现多链路的负载均衡

在各省级机关的 internet 出口处部署一台 banggoo-LC(分支机构链路负载均衡器)，并在其上部署应用牵引模块。

如上图所示，我们建议在省级机关的网络接入处，部署 Banggoo LC，实现对 internet 接入和政府广域网接入这两条链路的负载均衡，根据省级机关办公用的访问的目的地址或者应用，智能的选择链路， 实现两条链路的冗余备份和透明容错，保证了省级机关访问中央机构关键应用的 100％的高可用性。

banggoo-LC 实现各安全网关的负载均衡

通过旁路部署各安全网关设备，banggoo-LC 可以实现多台 IDS（最多 100 台）、cache 服务器、防病毒网关，URL 过滤网关的负载均衡，这些安全网关设备可以是不同厂家，不同型号，不同性能，大大提供安全网关的扩展性和可用性。般固整体解决方案的优势

般固（北京）科技股份有限公司的智能应用网络解决方案，是以智能应用技术为基础，将先进的负载均衡、应用交换和包括业界领先的防 Dos 攻击技术在内的应用安全解决方案进行整合，是一个使网络能够尽快的满足动态的应用和业务需要而设计的集成的解决方案。该解决方案包括的所有产品系列都建立在相同的软硬体系结构上，彻底解决了大范围的网络可用性、网络性能和安全问题，使数据中心应用灵敏并具有自适应性。