



华为电子政务专网解决方案

版权所有 © 华为技术有限公司 2012。保留一切权利。

非经华为技术有限公司书面同意，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播。

商标声明

、HUAWEI、华为、 是华为技术有限公司的商标或者注册商标。

在本手册中以及本手册描述的产品中，出现的其他商标、产品名称、服务名称以及公司名称，由其各自的所有人拥有。

免责声明

本手册可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本手册信息仅供参考，不构成任何要约或承诺。华为可能不经通知修改上述信息，恕不另行通知。

华为技术有限公司

深圳市龙岗区坂田华为基地

电话: (0755) 28780808

邮编: 518129

业务咨询热线: 400-822-9999

版本号: M3-035553-20120903-C-1.0

enterprise.huawei.com

华为企业业务 悉您所需 为您所用



前言

爆炸的信息时代让政府服务的资源调用量增大、社会对政府服务的需求提高，政府机构需要加速变革增加公众参与度；而政府机构职能转变也需要信息技术的支撑来实现“思维方式、工作方式”的转变。

在运用信息技术的基础上建立以公众为中心的服务平台，基于多元化的信息手段完善各职能环节服务，建立信息时代的透明、公开、互动的服务型政府已经成为世界各国政务发展的共识。

为了更好应对未来电子政务的发展，华为针对性的推出了“电子政务专网”解决方案，从基础网络的现状出发，深层次挖掘可改进部分，运用信息化手段帮助客户实现开放的、融合的、高效的、透明的、绿色的、安全的政府。



需求与挑战



创建服务型政府已逐渐成为各国政府的发展趋势，从政府行政程序、职能、机制上的全面转变，区域性或国家性的业务架构与设备支撑已很难满足日益增长的业务需求，政府信息化的过程中我们不得不面临诸多的问题：

- 政务建设缺乏统筹发展规划，电子政务的“数字鸿沟”、“信息孤岛”林立；
- 电子政务信息涉及国计民生，安全问题不容忽视；
- 便捷性和可参与性仍需提升，公众满意度差；
- 多样且复杂的业务带来爆炸式增长的数据，需要保证电子政务的便利性、完整性、交互性。



图1：政府信息化发展的四个阶段

Source: IBM

如图1所示，政府的信息化正按照政府“单向发布→在线互动→按需服务”的服务模式演进，业务的需求对网络提出了全IP、高带宽、更高开放灵活性的要求，同时保证高安全性。政府渴望搭建一个高效、低成本、政务匹配的多层级网络，同时具备专业的业务保障能力、多层的安全防护系统。

华为电子政务专网解决方案



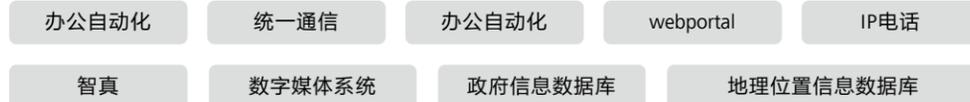
华为电子政务专网解决方案提供端到端的网络部署方案，在整个电子政务信息化建设架构中，以网络为基础架构支撑底层的数据接入传输、上层的业务互通、及业务平台数据处理，能够同时满足全IP、高带宽的业务体验保障需求，并拥有完善的网络安全方案降低运营风险，增强系统可靠性。

提高市民生活品质，提高政府运作效率

电子政务的业务场景



电子政务的应用支撑平台



电子政务的专用网络连接



交互终端类型



图2：电子政务总体架构图

华为电子政务专网解决方案 — 基础网络解决方案



政府多层级架构的广域骨干网和城域网方案

应用场景

政府多层级架构广域骨干网和城域网方案主要应用在国家骨干网络建设，确保从中央政府到省（州）政府、以及地方政府城域网的接入可靠性、高安全性，并且满足语音、视频、数据多业务承载。

方案概述

作为国家或省(州)电子政务业务连通的数据承载平台，方案可实现业务跨越各区域。广域网方案采用RPR环网或者GE/POS环网拓扑结构，每个核心节点部署两台设备组成双平面(可以先建设单平面，后续扩容至双平面)；各个核心节点部署在核心城市内，同时兼顾地理位置的分布情况和传输资源的分布情况。

城域网拓扑结构与广域网类似，可根据不同规模及可靠性要求采取对应的组网结构，较大规模的采用双平面组网，对规模较小的城域网采用星型组网；同时，在城域网内选择两个核心节点双归到广域网，各汇聚设备双归到这两个核心节点，形成冗余备份。

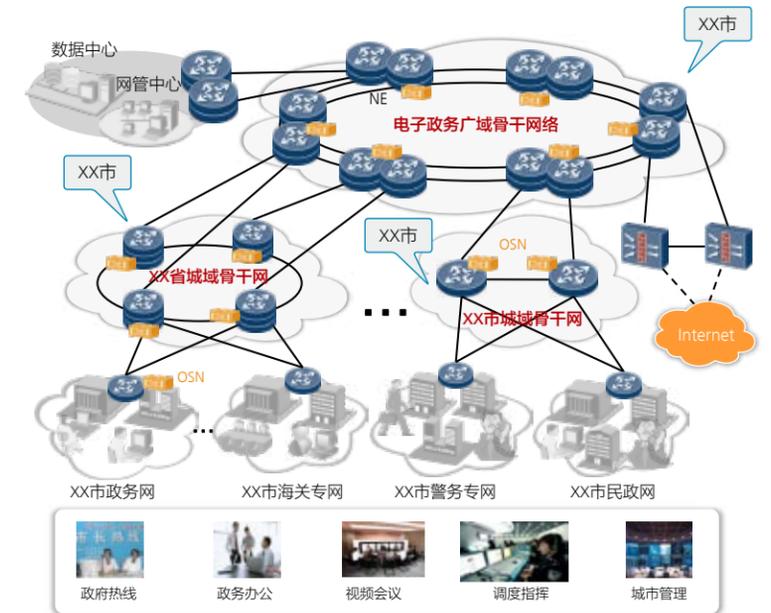


图3：政府多层级架构的广域骨干网和城域网方案

方案特点

- 多层级架构的组网方案，可以使多种业务共享带宽，支持快速倒换，确保业务不中断，消除来自于组网方案的不合理对政府服务造成的影响；
- 方案配置业界领先的网络设备，使设备级可靠性大于99.999%，保障网络故障10ms-500ms内恢复，拥有业界最全BFD(双向转发检测)，全业务保护倒换；
- 可扩展40G/100G高速端口，兼容IPv6；可以快速平滑升级光网络。

政府园区网络解决方案

应用场景

政府园区网络解决方案应用在政府办公园区内或园区与园区之间，通过MPLS VPN技术实现一张物理网和多张逻辑网，一网多用可以有效的解决业务应用多、平台分散、效率低、政务数据易泄露等问题。

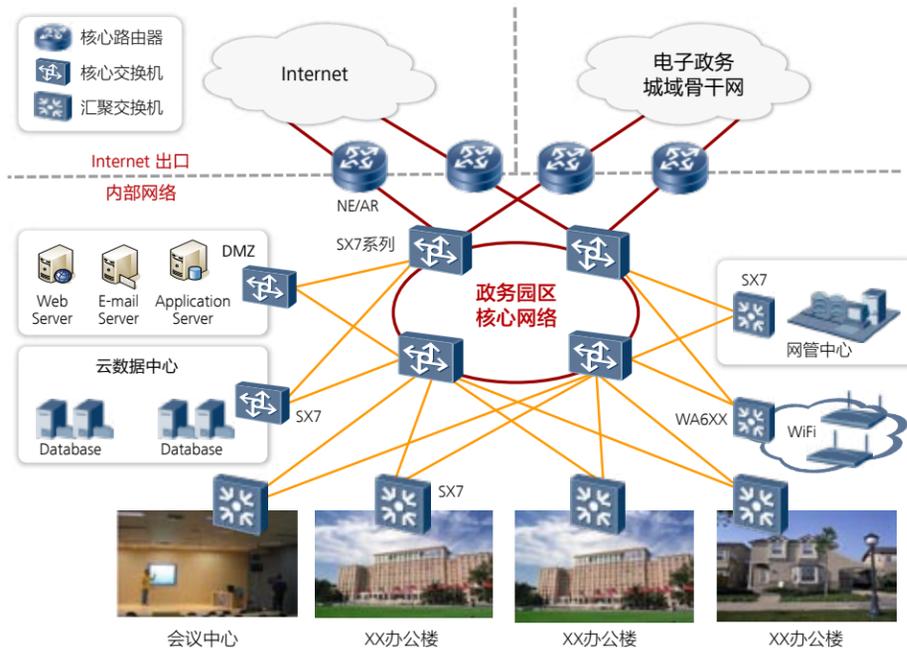


图4：政府园区网络整体解决方案

子方案一：一网多用政务园区网方案

方案概述

在政务或行政中心，利用一套基础网络设备支撑不同办公大楼中的多个部门的业务使用，可以根据需要进行业务隔离，也提供部门间互通通道，全面提升同一系统内上下级办公专网的互连互通能力。

方案特点

- 采用有线、无线一体化接入方案满足政府办公区多种方式业务接入需求；
- 不同的部门可以采用多种VPN一站式接入方案，达到有效、安全、隔离的效果；
- 方案完备的安全特性来自于：设备级/网络级关键组件/设备冗余，采用多种数据认证加密授权机制，高性能防火墙可以阻止非法入侵等行为；
- 高带宽、丰富的接口易于业务平台的扩展。

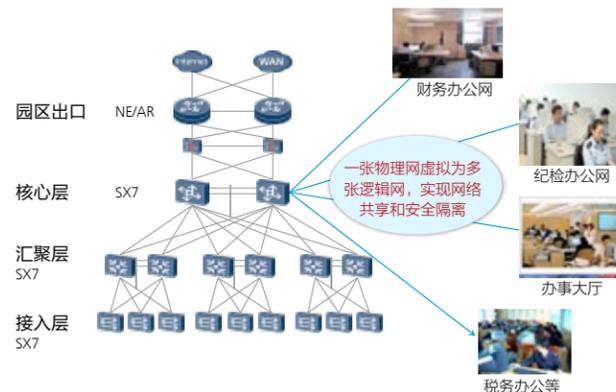


图5：一网多用政务园区网方案

子方案二：政务园区办公桌面云方案

方案概述

在政府园区中使用办公桌面云可以增强园区办公的移动性，工作人员用账号密码在园区内任何瘦终端都可登陆个人桌面办公，有效的应对普通PC固定办公模式带来的诸多不便和问题，提升紧急事务的应急处理。

方案特点

- 办公桌面云方案，可以解决以往政府园区内办公灵活性差的问题，方便办公人员随时随地的访问使用；
- 后台数据信息统一构建和部署，容灾备份保障信息安全，使系统稳定的运营，有效的降低宕机事件的发生，同时保障业务连续性；
- 最大化降低能耗和噪音影响，能耗为同性能产品35%，噪音为20%，为政府园区创造更加绿色的办公环境。



图6：办公桌面云方案

子方案三：园区无线网络方案

方案概述

在政府园区中，接入端通过AP广泛集中、分布式部署无线网络接入方案，工作人员可以利用各种终端随时随地的接入办公系统，资源获取简单、便捷，保障园区的安全移动接入性。

方案特点

- 政府园区无线网络方案可以让园区内所有人都能够随时随地互通信息，覆盖范围广；
- 通过WLAN可以保证形式多种的业务快速接入，支持多种无线无线QoS协议；
- 易部署，AP支持即插即用，“零接触”自动配置及升级；
- 大带宽，保证业务质量；高安全、易部署。



图7：园区无线网络方案

客户价值

- 政府园区网络解决方案，多种途径的接入网络方案为客户业务运行提供同一物理网络承载，不同部门业务安全隔离和共享；
- 保障业务顺畅，信息数据的安全，绿色办公环境；
- 有线无线一体化，增强了业务快速部署能力，提升市民满意度。

边远区域远端接入方案

场景分析

一直以来，边远区域在政令信息通畅的上传下达渠道存在着很大的困难，边远城镇或村基础设施较差，专线部署成本高且实施难度大，只有少数区域可以通过有线接入。华为边远区域远端接入方案，提出用微波、卫星、SHDSL、ISP等接入方式，帮助边远区域的镇(村)政府接入到市县网络中，搭建畅通的通信渠道，最大化的规避基础设施差的问题。



方案概述

较大乡镇，采用E1等专线方式接入；较小的偏僻乡镇，采用布设微波站、卫星通信或者租用SHDSL专线接入；对于家庭办公，利用当地ISP拨号接入。

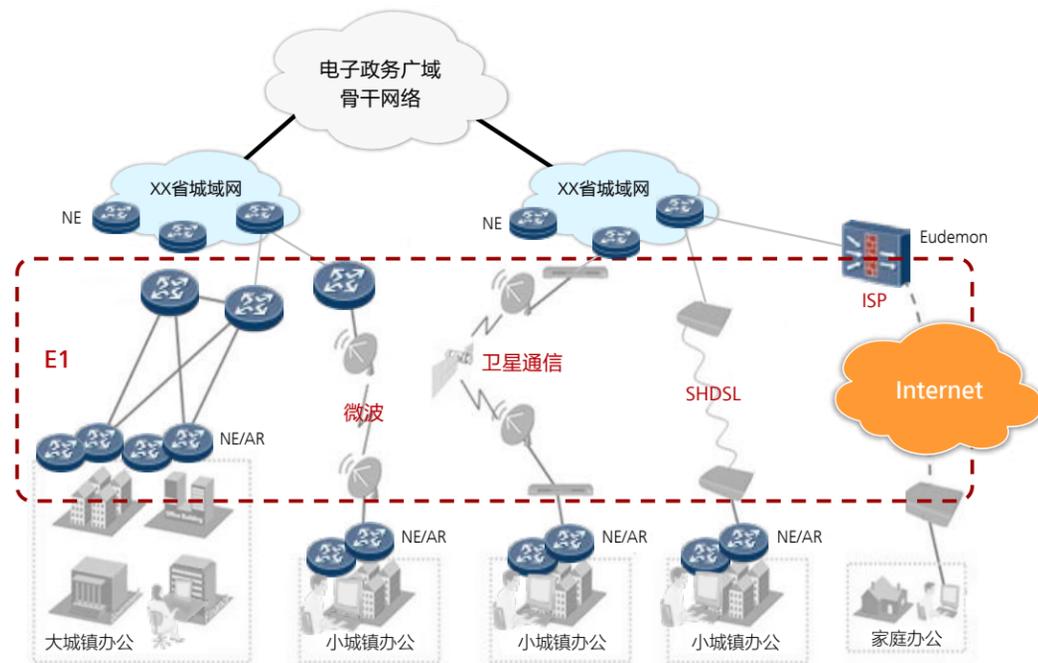


图8：边远区域远端接入方案

方案特点

- 全面的远端接入方式，适合边远各种规模的乡镇政府部门以及家庭办公；
- 边远地区政务多手段接入，确保政令通达，同时满足经济性。

数据中心网络解决方案

方案概述

华为数据中心网络解决方案，采用成熟的三层网络架构，主要包括广域互联方案、内部互联方案和容灾备份方案三个部分，可以满足公务员办公、园区网接入、公众和企业接入的政务办公需求，利用IP异步的异地灾备、光纤同步的同城备份方案能保护政府业务服务在任何情况下不宕机正常运行。

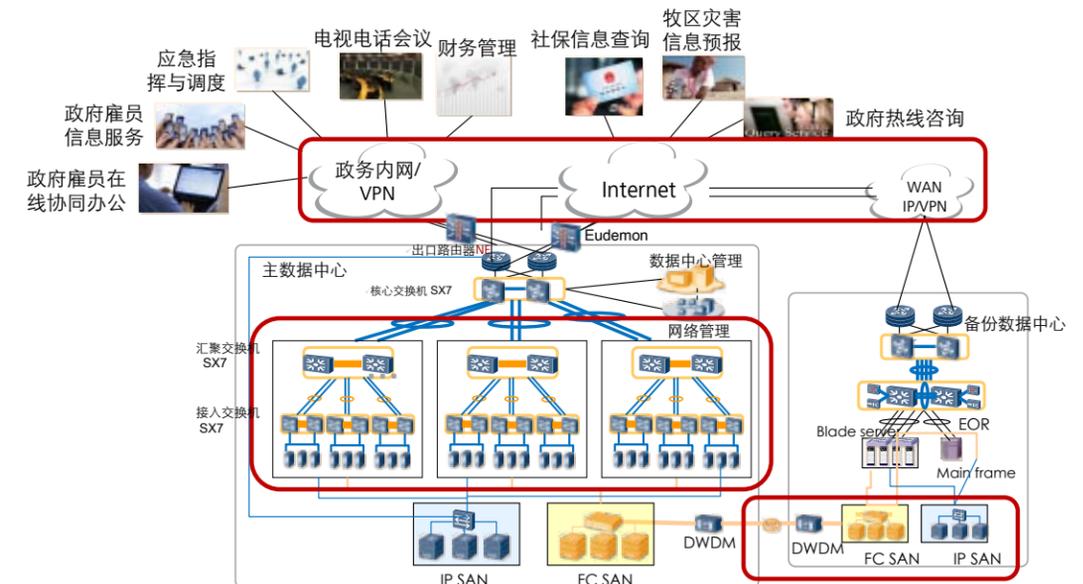


图9：数据中心网络解决方案

解决方案

容灾备份子方案

场景分析

“政务电子化”无限拉近了政府与公众的距离，在对政府部门IT建设提出更高要求的同时，也在考验着与之配套的灾难恢复体系。

解决方案

灾难恢复子方案，不是一个单纯的技术方案。她根据不同应用系统差异化的业务恢复要求，以及生产中心面临的主要风险，针对生产中心与灾备基础设施的实际情况，设计符合国家标准，不同灾难恢复等级的技术方案以节省投资，并协助客户在灾难恢复项目的实施过程中，建立强有力的应急体系，将危机处置意识植入企业文化的“血液”中。

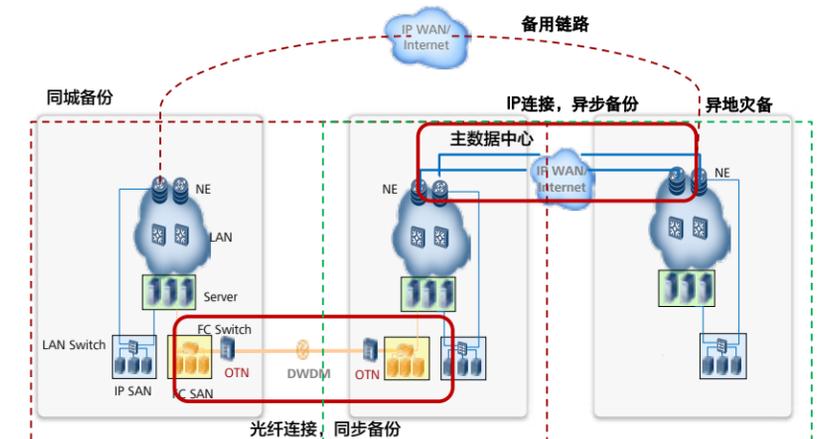


图10：“两地三中心”容灾备份解决方案

可视运维网管解决方案

场景分析

政务系统纷繁复杂、形态各异、维护难度大，运维机构需要一个简单便捷的网管系统，实现事前预防、故障定位和报警、应急响应，最大可能消除为此带来的负面影响。

方案概述

华为eSight可视运维网管解决方案网管分级建设，分担核心网管负荷，提升效率。提供端到端统一网管系统管理，对整网进行技术故障定位、可视化监控等。方案保障多层的网络高效、快捷、便利的运转，同时对传统的网络运维管理能力提出挑战，解决了整网故障定位难、第三方设备定制管理能力等问题。

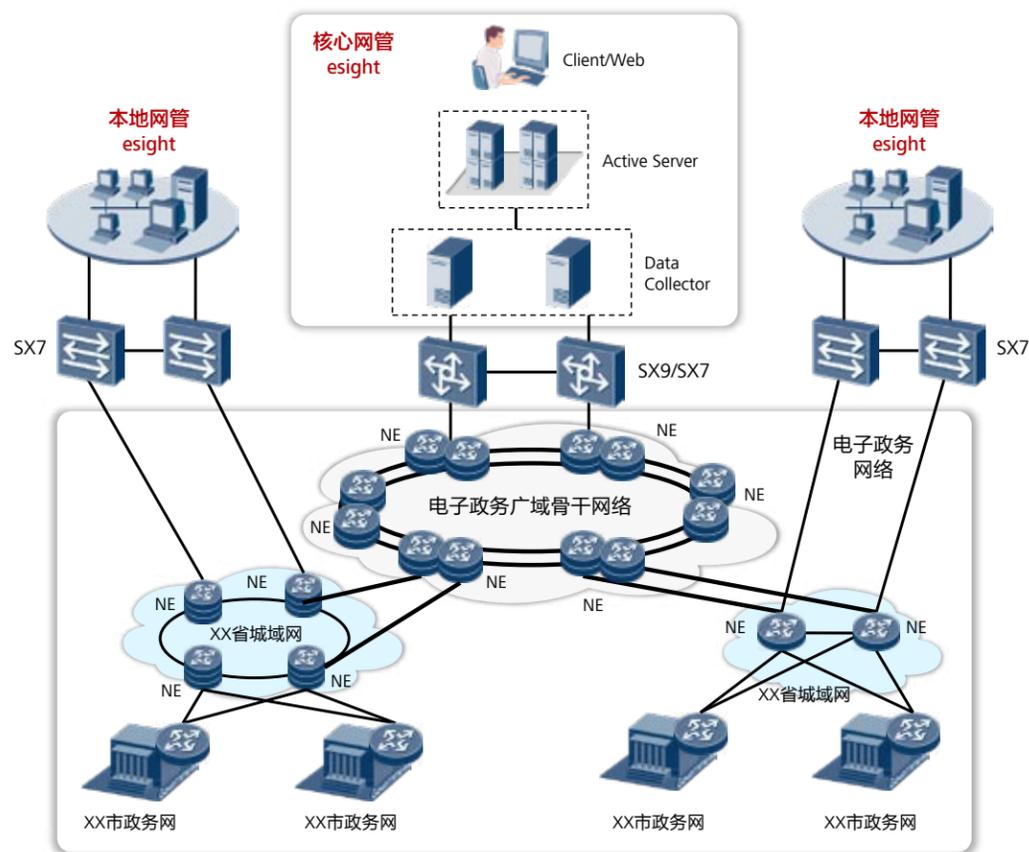


图11：可视运维网管解决方案

方案特点

- 可视运维网管方案，系统兼容性强，可以跨厂商设备统一管理、多业务设备IP&IT管理；
- 网络结构可视、智能报表、性能预警、网管平台接口开放；
- 降低维护OPEX及TCO；可视统一管理，政务网络管理效率高；
- 配置方便，业务熟练情况下完成100台AP业务开通仅为10分钟。

华为电子政务专网解决方案 — 业务保障方案



场景分析

政府业务的信息主要包括音频、视频和数据资料三类，我们需要优化网络管理、提升信息流通的安全保障能力：

- 数据业务：不同部委间按需隔离与共享，对信息安全要求高，要保证关键数据优先性；
- 视频业务：要保证关键政务信息的画面清晰流畅、视频语音同步，同时简便的操作有利于主管部门的应急响应和决策；
- 语音业务：E2E QoS保障、无丢包，无掉话、无杂音，无抖动、无延迟，能同步。

方案概述

电子政务业务保障方案，从网络物理层、网络层到业务层，全方位的保障政府数据的传输、交换和最终的用户体验，方案应用MPLS VPN技术和可视化网络管理系统，使电子政务网络在恢复能力、性能优化能力、关键业务优先、视频和语言高清流程方面大大提升，体现政府优质的服务能力。

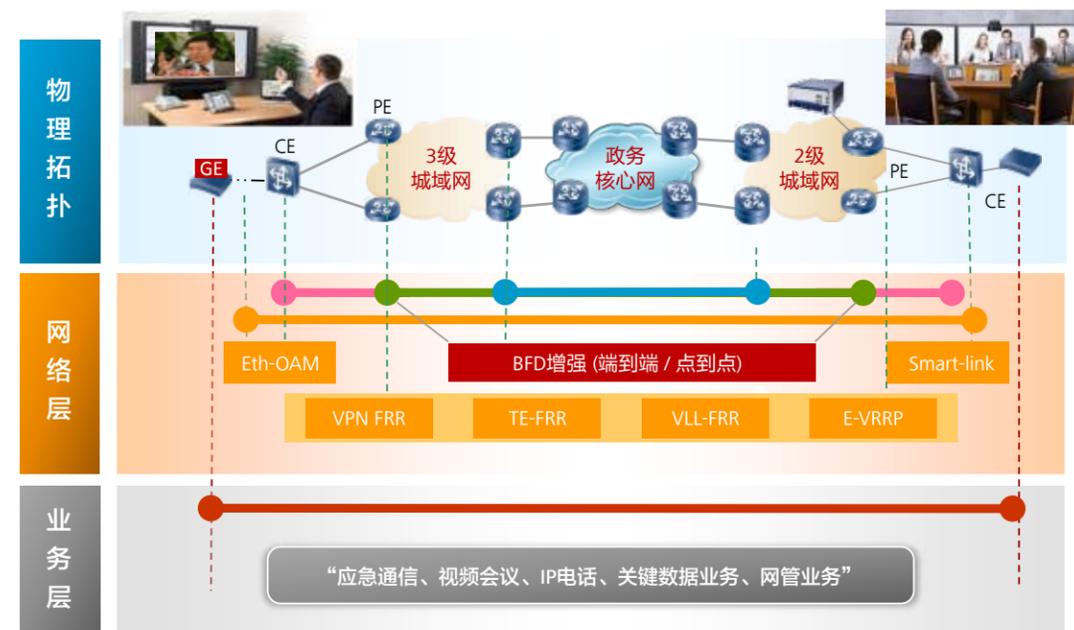


图12：业务保障解决方案

方案特点

1) 网络故障快速恢复机制

- 端到端故障检测和恢复，准确定位故障点和故障原因；
- 节点、链路故障恢复；
- 业界领先的业务端到端200ms故障恢复。

2) 骨干网性能优化能力

- MPLS TE 结合了MPLS 技术与流量工程，通过建立到达指定路径的LSP 隧道进行资源预留，使网络流量绕开拥塞节点，达到平衡网络流量的目的；
- 在资源紧张的情况下，MPLS TE能够抢占低优先级LSP隧道带宽资源，满足大带宽LSP或重要业务的需求；
- 通过部署MPLS TE最大可以节省40%的传输成本。

3) 关键业务优先保障

- 基于TE的MPLS-HQoS技术既能控制用户的流量，又能同时对用户业务的优先级进行调度；
- 根据需要建立高优先级的VPN，如应急指挥系统；
- VPN内根据业务不同，进行优先级调度，保证高优先级带宽，如视频会议、IP语音业务；

- VPN内普通政务数据业务进行剩余带宽的公平调度，如关键数据业务及一般数据业务；
- 自研专用TM芯片，调度不影响设备性能。

4) 高清视频会议视频流畅

- 内置iVSE视频增强卡，识别，缓存GOP；
- 在RTP & RTCP协议层实现关键帧重传；
- PE适应丢包重传，减少网络额外带宽开销；
- 实现15%突发丢包，视频体验无影响。

5) QoS保障音视频业务应用

- 根据数据的用途和优先级对报文进行分类和标记；
- 进行拥塞避免，减少拥塞的发生以及避免TCP全局同步，在网络没有发生拥塞以前根据队列状态进行有选择性的丢包；
- 保证不同优先级的报文得到不同的QoS待遇，包括时延、带宽；
- 搭配多样的流分类、精度达到5%的流量监管、丰富的调度算法和先进的拥塞避免技术。



华为电子政务专网解决方案 — 电子政务专网信息安全方案



场景分析

网络环境复杂多变，安全威胁无处不在，而网络和信息数据安全保障对政府尤为重要，为了杜绝黑客攻击、垃圾邮件、病毒侵入、非法使用、窃听、假冒、抵赖等安全威胁引发的信息安全事件，需要全方位、立体式、主动性防御的信息安全方案，消除来自终端接入、网络攻击造成的威胁。

解决方案

电子政务专网信息安全整体解决方案，可以满足政府对信息安全越来越高的要求，全方位多角度的消除信息安全事件的发生，不论威胁是来自内部的还是外部的，都能很好的应对已发生的、未发生的安全事件。主要通过两个子解决方案来实现信息安全，由外部引发的安全事件解决方案，实现网络数据的高过滤、有效阻断外部攻击；由内部引发的安全事件解决方案，实现网络数据全面管理和内部人员权限管理。

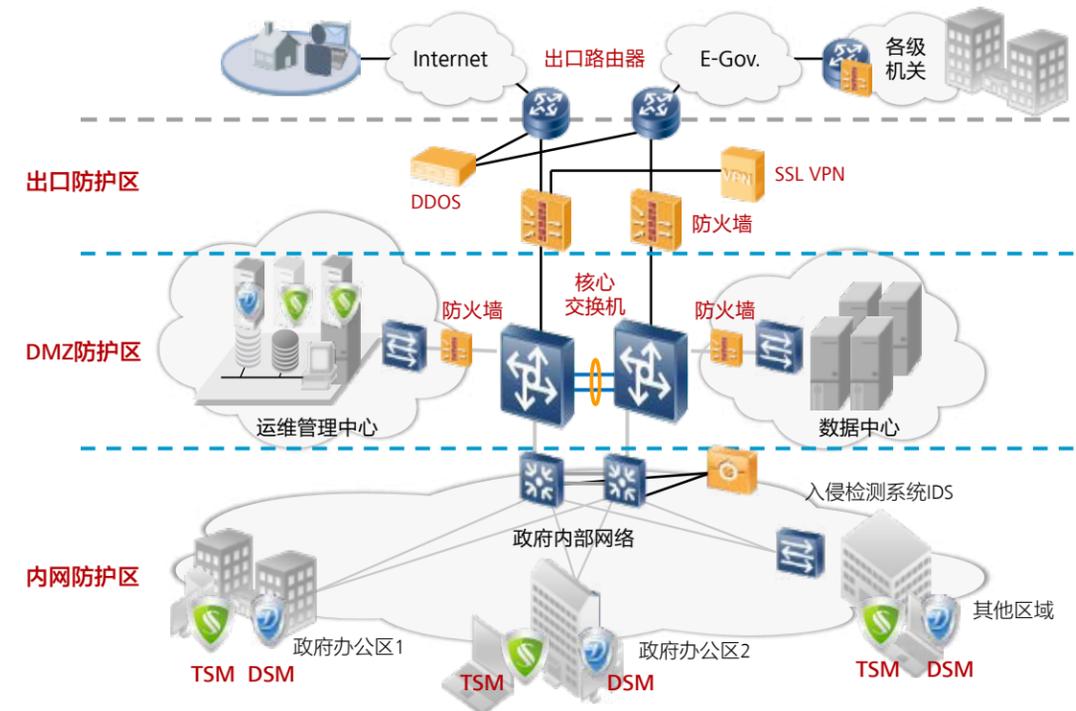


图13：电子政务专网信息安全整体解决方案



子方案一：纵深防御-政务外部防护

政府网络时刻面临着来自外界的安全威胁，例如外部入侵、篡改、垃圾邮件等。华为纵深防御解决方案主要通过物理隔离、逻辑隔离、策略隔离、应用隔离、准入隔离等手段，达到防御目的。

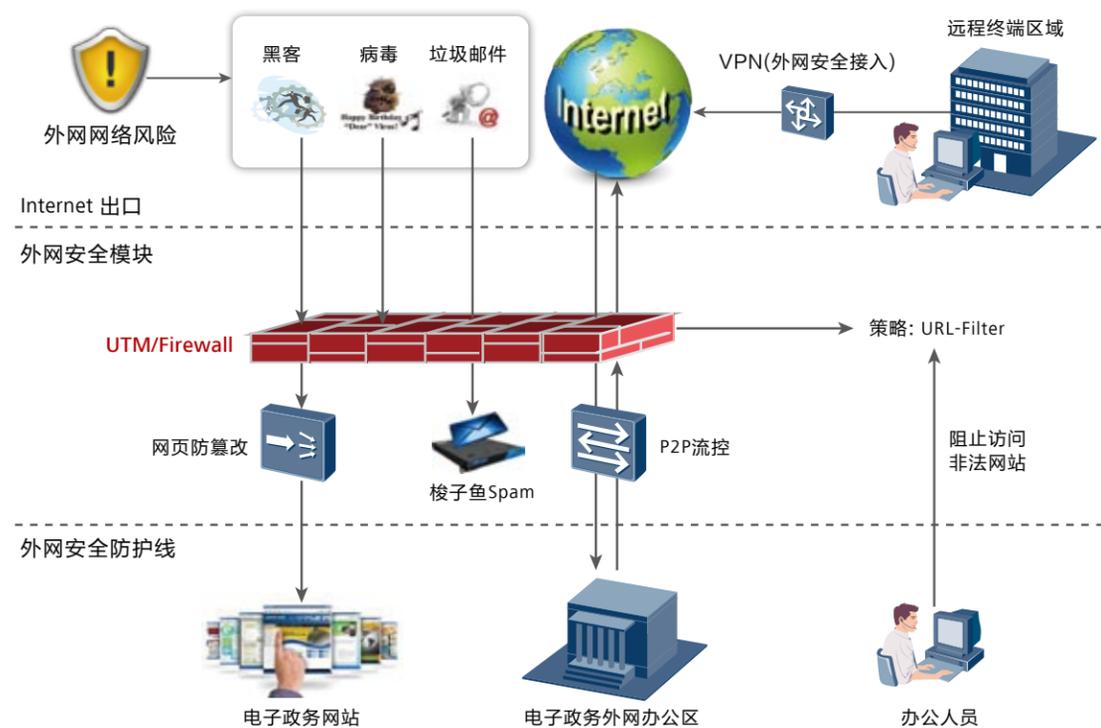


图14：政务内部防护解决方案

方案特点

该方案从设备和网络层面为政府网络提供安全保障，通过一系列的安全防护措施使整个环境达到高安全、高可靠。

- 提供网络侧端到端的7层深入主动防御；
- 业界领先的防火墙、安全策略关键性能指标，软硬件体系完善可靠；
- 功能全面，UTM技术，防火墙产品集成AV、IPS、AS、DDOS、URL过滤模块。

子方案二：安全免疫-政务内部防护

政府内部办公环境也存在着不同程度的安全隐患，为了确保关键数据信息不被破坏、传播等，内部安全免疫方案通过部署TSM/DSM系统，使用系统的文件加密、权限划分等功能有效的杜绝安全事件发生。

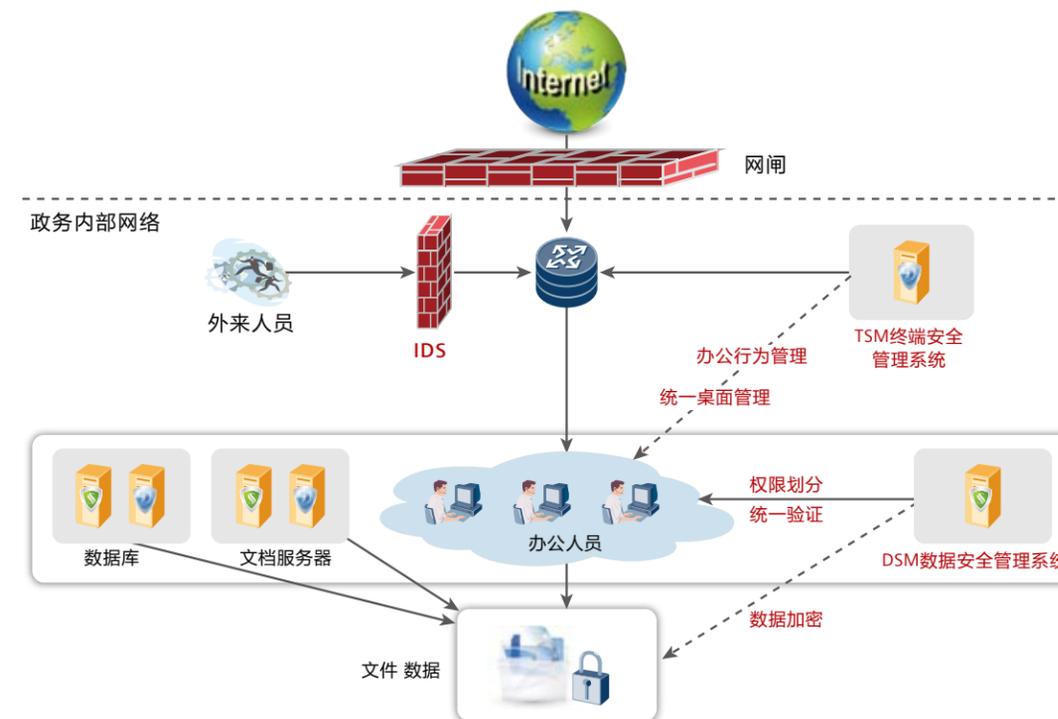


图15：政务外部防护解决方案

方案特点

- 通过终端安全管理系统和数据安全管理系统，对对外来人员终端的接入、应用终端进行安全检查，解决雇员与外来人员对信息安全带来的威胁；
- 规范办公行为，设置权限划分、数据加密加强系统的统一管理；
- 检查结果清晰可见，后续可生成各种统计报表，供领导决策分析；
- 灵活的部署和管理，支持集中、分布、分级三种部署方式，适应各种政府系统与网络环境，最小化网络带宽占用。



子方案三：可信增值-终端安全防护

在政府办公网络内部署secospace终端安全系统，可以自上而下下达审计监控任务，对用户终端的安全性状况进行检查，登记在案并生成审计报告；也可以由用户自行发起自检，帮助用户提高本机安全性，防止无意泄密。

同时，Secospace终端安全管理系统可以统一完成对终端操作系统的统一管理和安全服务，比如完善补丁、防病毒库，方便快捷的杜绝安全隐患。

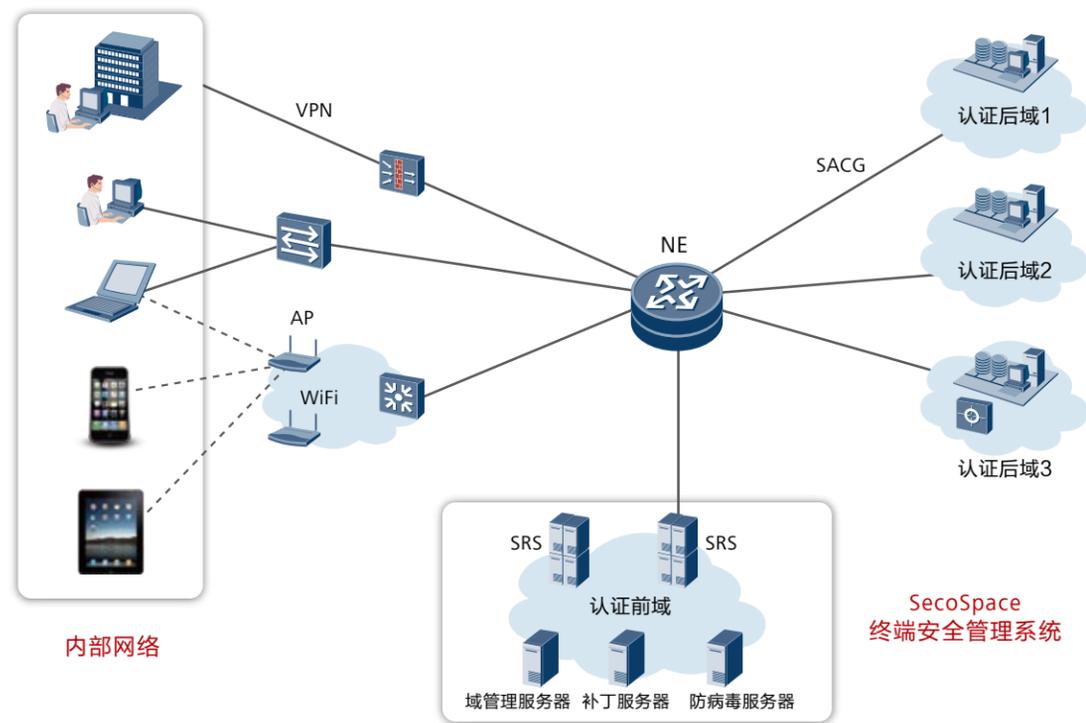


图16：终端安全防护解决方案



应用及商业利益

电子政务专网解决方案，运用最优的设计方案从技术和业务层面解决诸多问题，宏观的讲电子政务专网解决方案可以帮助政府改善了本国经济环境，吸引外商投资、拓宽了市民与政府沟通的渠道。微观的讲可以优化和规范办事流程、提高办事效率、降低投资成本、提升管理运维水平、确保资源高利用率、而系统的高安全、高可靠性可以消除信息资源安全方面的一切后顾之忧。

成功案例：国家电子政务外网



国家政务外网是中国电子政务的重要基础设施，它是以国家电子政务传输网为基础，由中央政务外网和地方政务外网组成，主要服务于各级党委、人大、政府、政协、法院和检察院等政务部门，为部门业务应用提供网络承载服务，支持业务网络的互联互通，支持跨地区、跨部门的业务应用、信息共享和业务协同，满足各级政务部门社会管理、公共服务等方面的需要。

网络建设之初就面临很多挑战和问题：

- 国家各省市、部门均建立了自己的办公网络，面临重复建设、功能重叠且维护成本巨大的问题，需要对其进行有效整合；
- 各省市、部门办公网络形成信息孤岛，彼此缺乏有效互联；
- 缺乏统一的信息安全管理。

政务外网进行分期建设，华为全程参与了一期的网络规划设计、网络部署和验收工作。国家信息中心采用华为公司NE系列高端路由器产品（6台NE80E和50余台NE40）分别部署于中央城域网、广域骨干网、互联网出口、中央网络管理中心、省市接入网、中央部委局署接入网等重要节点，利用华为成熟稳定的MPLS VPN技术实现业务隔离/互访，并在网络中部署华为网管软件。

方案实现“多种VPN业务、单点集中运维”，可以大幅降低管理成本，提高工作效率。同时实现业务分级处理和空间重用，多种业务共享带宽的设计充分提高带宽利用率；当节点或传输失效时，可以实现快速自动保护倒换，提高网络的健壮性和可靠性。

国家政务外网一期工程2009年通过验收，该网目前已连接53个中央政务部门，31个省、自治区、直辖市和新疆生产建设兵团，160多个地市州、420多个区县，接入政务外网的各级政务部门达9400多个，接入终端近31万台，成为中国覆盖面最广，连接部门最多，规模最大的政务公用网络。

目前，政务外网已承载了国家应急平台系统、监察部纠风业务系统、文化部文化共享工程、“金安”工程、新华社新华频媒项目等11个部委的12项全国性业务应用。从2008年“518”汶川大地震中唐家山堰塞湖排险，到2009年交通部海上搜救演习的成功，国家电子政务外网有效支撑了各部门业务应用，实现跨部门、跨地区电子政务业务应用的快速部署，使政务外网在各级政务部门开展资源整合、信息共享、业务协同等方面发挥重要作用。

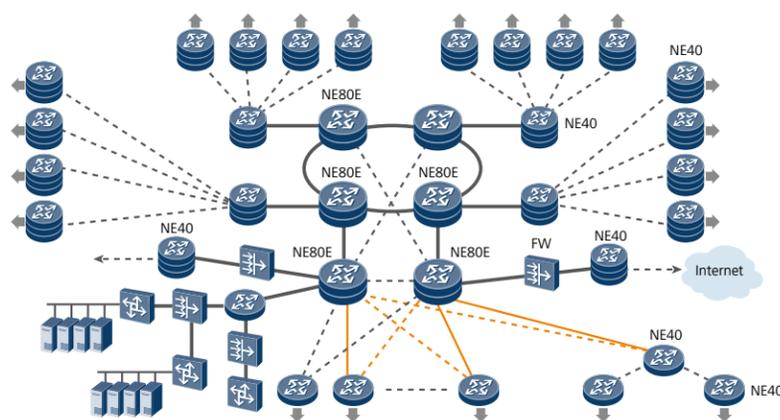


图17：国家电子政务外网网络拓扑图

