国家电子政务外网标准

GW0103—2011

国家电子政务外网
安全等级保护基本要求

Baseline for classified protection of

National E-government Network

2011-12-31 发布　　2011-12-31 实施

国家电子政务外网管理中心

目　次

前　言

为了贯彻国家信息安全相关法律法规，落实信息安全等级保护相关技术要求，根据国家标准GB/T 22239-2008 《信息系统安全等级保护基本要求》的要求，为规范国家电子政务外网安全等级保护的工作，针对政务外网的具体情况，特制定本标准。

本标准由国家电子政务外网管理中心提出。

本标准由国家电子政务外网管理中心归口。

本标准主要起草单位：国家电子政务外网管理中心办公室、国家信息中心信息安全研究与服务中心

本标准主要起草人：孙大奇、周民、沈解伍、吴亚非、刘建国、邵国安、禄凯、陈永刚、罗海宁、吕品、徐春学、刘晓光

本标准由国家电子政务外网管理中心负责解释。

引　言

本标准是国家电子政务外网安全等级保护相关系列标准之一。

本标准与国标《计算机信息系统安全保护等级划分准则》（GB 17859-1999）、《信息系统安全等级保护基本要求》（GB/T 22239-2008）等标准共同构成了国家电子政务外网安全等级保护的相关配套标准。其中GB 17859-1999、GB/T 22239-2008是基础性标准，为政务外网安全等级保护遵从的基本标准。本标准是针对国家电子政务外网现状、技术特点和安全防护要求作进一步细化和扩展，是对GB/T 22239-2008的补充，本标准未提到部分均按 GB/T 22239-2008的信息系统安全等级保护基本要求执行。

与本标准相关的系列标准包括：

——《国家电子政务外网安全等级保护实施指南》

在本标准文本中，黑体字表示较低等级中没有出现或增强的要求。

对于承载涉及国家秘密信息系统的网络保护要求，按照国家相关法律法规和信息安全主管部门的相关规定和标准实施。

对于涉及密码的使用和管理，按照国家密码管理主管部门的相关规定和标准实施。

凡涉及政务外网数字证书的相关要求，参照国家电子政务外网管理中心印发的相关管理和技术规定执行。

国家电子政务外网安全等级保护基本要求

1　范围

本标准规定了国家电子政务外网（以下简称政务外网）不同安全保护等级网络的基本技术保护要求，适用于指导政务外网安全等级保护的建设、整改、自查和测评工作，可作为安全等级保护和信息安全主管部门对政务外网安全进行检查和指导时的依据。

本标准只涉及政务外网安全等级保护的基本技术要求，有关物理环境、主机/服务器、应用、数据和管理安全等共性要求，请按照国家标准 GB/T 22239-2008 执行。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。凡是不注明日期的引用文件，其最新版本适用于本标准。

GB/T 5271.8　信息技术　词汇　第 8 部分：安全

GB 17859　计算机信息系统安全保护等级划分准则

GB/T 20270 信息安全技术 网络基础安全技术要求

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 21061 国家电子政务网络技术和运行管理规范

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240 信息安全技术 信息系统安全等级保护定级指南

YD/T 1746　IP 承载网安全防护要求

《<信息安全等级保护商用密码管理办法>实施意见》（国密局发[2009]10 号）

《电子政务电子认证服务管理办法》（国密局发[2009]7 号）

3　术语和定义

GB/T 5271.8 和 GB 17859-1999 确定的以及下列术语和定义适用于本标准。

3.1

安全保护能力　Security Protection Ability

系统能够抵御威胁、发现安全事件以及在系统遭到损害后能够恢复先前状态等的程度。

3.2

虚拟专用网络 Virtual Private Network （VPN）

一种在 IP 承载网络上通过逻辑方式隔离出来的网络。它是一组封闭的网络网段，即使用同一台 IP 设备和开放互联协议与其他 VPN 共享同一主干网络，不同 VPN 之间的通信保持分离，路由不可达，形成隔离，在一个虚拟网内，所有用户共享相同的安全策略、优先级服务和管理策略，提供端到端的

业务连接。所谓“虚拟”指网络连接特性是逻辑的而不是物理的。VPN 技术可用于网关与网关之间的连接、网关与端点之间的连接、端点与端点之间的连接。

3.3

多协议标签交换的虚拟专用网 Multi-Protocol Label Switch VPN （MPLS VPN）

MPLS-VPN 是指采用多协议标签交换（MPLS）技术在骨干的宽带 IP 网络上构建虚拟专用网络，实现跨地域、安全、高速、可靠的数据、语音、图像多业务通信，并结合差别服务、流量工程等相关技术，将公众网可靠的性能、良好的扩展性、丰富的功能与专用网的安全 、灵活、高效结合在一起，为用户提供高质量的服务。

3.4

广域网 Wide Area Networks （WAN）

把城市之间连接起来的宽带网络称广域网，政务外网从中央到各省的网络称为中央广域网、省到各地（市）网络称为省级广域网、地（市）到各县的广域网称为地（市）级广域网。实现国家、省、市、县纵向业务的互联网通。

3.5

城域网 Metropolitan Area Networks （MAN）

把同一城市内不同单位的局域网络连接起来的网络称为城域网，实现不同单位跨部门业务的数据共享与交换。

3.6

局域网 Local Area Network （LAN）

把本单位终端、主机/服务器、存储等设备，通过网络设备连接起来的网络，实现本单位业务系统、数据的互访、共享等，称为局域网。局域网是政务部门开展电子政务业务的基础，其安全、建设、运维等相关工作由网络所属单位自行负责。

3.7

逻辑隔离 Logic Isolation

逻辑隔离是一种不同网络间的安全防护措施，被隔离的两端仍然存在物理上数据通道连线。一般使用协议转换、数据格式剥离或数据流控制的方法来实现在两个逻辑隔离区域之间传输数据，并且传输的方向可以是单向或双向。

3.8

国家电子政务外网 National E-Government Network

国家电子政务外网是国家电子政务重要基础设施，是承载各级政务部门用于经济调节、市场监管、社会管理和公共服务等非涉及国家秘密的业务应用系统的政务公用网络。包括中央级政务外网和地方

政务外网，二者均由相应的广域网和城域网构成。中央广域网与31个省、直辖市、自治区和新疆生产建设兵团的省级政务外网互联。中央城域网用于连接在京中央政务部门，并与中央广域网高速互联。地方政务外网由省、地（市）和县级广域网和相应的城域网构成。

3.9

公用网络区　Public Network Area

公用网络区采用统一分配的公共IP地址，是实现各部门、各地区互联互通，为跨地区、跨部门的业务应用提供数据共享与交换的网络支撑平台。

3.10

专用网络区　Private Network Area

依托国家政务外网基础设施，为特定需求的部门或业务设置VPN区域，主要满足部门横向、纵向业务的需要，实现部委、省、地（市）和县端到端业务和数据的互联互通，实现与其它业务之间的逻辑隔离。

3.11

互联网接入区　Internet Access Area

是各级政务部门通过逻辑隔离安全接入互联网的网络区域,满足各级政务部门访问互联网的需要。同时也是移动办公的公务人员通过政务外网数字证书，经网关认证后安全接入政务外网的途径。按属地化管理的原则，中央和地方分别管理各自的互联网出入口。

3.12

网络管理区　Network Management Area

网络管理区主要承载网络管理信息系统，负责管理辖区内的各种网络设备、域名服务器等相关设备及系统的安全管理，实现工单处理、操作任务委派、值班管理、资料管理等在内的日常维护生产任务的电子化、流程化。

3.13

安全管理区　Security Management Area

安全管理区主要承载安全管理信息系统,对管辖范围内网络中部署的安全防护设备进行日志采集、关联分析、对网络病毒和攻击进行告警、对安全事故提出预警和采取措施的建议，定期总结并提出分析报告。

3.14

政务外网安全防护范围　Goverment Network Security Protection Scope

按网络区划分：中央、省、地（市）广域网、各级城域网、用户接入局域网。

按业务区域划分：公用网络区、互联网接入区、专用网络区、用户接入区、网络和安全管理区、

电子认证区。

3.15

数字证书 Digital Certificate

数字证书为实现双方安全通信提供了电子身份认证。在利用互联网、政务外网或局域网时，使用数字证书实现身份识别和电子信息加密。数字证书中含有密钥对（公钥和私钥）所有者的识别信息，通过验证识别信息的真伪实现对证书持有者身份的认证，数字证书包含公开密钥拥有者的信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

3.16

资产 Asset

任何对组织有价值的东西。

3.17

安全策略 Security Policy

安全策略是组织所接受的一系列管理政策，信息安全的目标是控制或管理主体（例如用户和过程等）对客体（例如数据和程序）的访问。这些控制措施由一系列的政策和目标来约束，这些政策和目标就称为安全策略。

3.18

信息安全 Information Security

保证信息的保密性、完整性、可用性；另外也可包括诸如真实性、可核查性、不可否认性和可靠性等特性。

3.19

信息安全事态 Information Security Event

信息安全事态是指被识别的一种系统、服务或网络状态的发生，表明一次可能的信息安全策略违规或某些防护措施失效，或者一种可能与安全相关但以前不为人知的一种情况。

3.20

信息安全事件 Information Security Incident

一个信息安全事件由单个或一系列的有害或意外信息安全事态组成，极有可能危害业务运作和威胁信息安全。

4 政务外网资产、威胁分析和脆弱性

4.1 资产分析

政务外网由于各地建设、运维及管理的差异，对资产的选取、识别和划分更应保持科学性、合理性和可管理性。政务外网的资产大致包括各类网络设备、主机、文档、业务、人员、物理环境设施等。政务外网资产分析包括但不限于表 1 所列范围：

表 1　资产类别

类　别	资　产
网络和安全设备	**表1**　网络设备：包括各类路由器、交换机等。 **表2**　传输设备：包括自建的光端机、SDH 或 MSTP 设备和光缆等（不包括租用基础电信运营商和其他提供基础通信服务企业的通信设备）。 **表3**　专线链路及流量控制设备等。 **表4**　安全设备：包括各类防火墙、入侵检测、网关、审计及其他安全防护设备等。
主机/服务器	1、网络管理系统设备：包括各类管理主机/服务器、终端、存储、辅助设备等。 2、安全管理系统设备：包括各类管理主机/服务器、终端、存储、辅助设备等。 3、域名系统设备：包括域名解析服务器、辅助设备等。 （与设备、主机密切相关的软、硬件可作为一个整体，不必细分）
独立商业软件	可独立识别的操作系统、数据库、中间件等商业软件及应用系统软件等。
文档数据	1、设备数据：网络、安全设备相关的业务、功能、管理、配置等方面的数据和信息等，包括电子文档和纸质文档。 2、文件资料：各类形式的文件、档案、资料（如设计文档、技术资料、管理规定、工作手册、财务报表、数据手册等。）
服务/业务	各类网络提供的功能、业务和服务，如 VPN 等。
网络资源	网络相关的链路、带宽、各类设备的容量、网络地址空间等。
人员	与政务外网建设、运维相关的管理和技术人员等。
环境设施	包括机房，电力供应设施，电磁防护系统，防火、防水、防盗系统，防静电、防雷击、温湿度控制系统及相关设备等软硬件设施。

4.2 威胁分析

政务外网的威胁根据来源可分为技术威胁、环境威胁和人为威胁。环境威胁包括自然界不可抗拒的自然灾害和其他物理威胁。根据威胁的动机，人为威胁分为恶意和非恶意两种，政务外网的威胁类别应包括但不限于表 2 所列范围：

表 2　威胁类别

类　别	威 胁
技术威胁	1、未充分考虑设备冗余、可靠性及业务安全、应用需求等原因，使得相关功能存在缺陷或隐患造成的安全事件等。 2、系统差错、节点/链路可靠性不足造成的故障等。 3、错误响应和恢复等。 4、相关数据、信息在备份、保存、恢复过程中发生的差错、损坏、丢失等。 5、地址、带宽、处理能力、存储空间等资源滥用、浪费、过度消耗等。

		6、突发流量和异常数据流量等。
环境威胁	物理环境	**附　录**　A供电故障，灰尘、潮湿、温度超标，静电、电磁干扰等。 **附　录**　B意外事故或租用电信运营商线路故障等。 3、机房火灾、空调故障等事故。
	灾　害	1、鼠蚁虫害等。 2、地震、洪灾、火灾、泥石流、山体滑坡、台风、雷电等自然灾害。 3、战争、社会动乱、恐怖活动等。
人为威胁	恶意攻击	1、针对网络的恶意拥塞。 2、针对业务、设备等相关数据的拦截、篡改、删除等攻击行为。 3、恶意代码、病毒等。 4、非授权访问，越权操作等。 5、伪造和欺骗等。 6、物理攻击、损坏和盗窃等。
	非恶意人员	A　误操作。 B　对系统不了解、技术技能不足。 C　相关数据、信息的无意泄露。 D　组织、安全管理制度不完善，制度推行不力，因缺乏资源非规范操作等。

4.3 脆弱性分析

政务外网的脆弱性包括技术脆弱性和管理脆弱性二个方面，脆弱性的识别对象以资产为核心，政务外网的脆弱性分析应包括但不限于表 3 所列范围：

表 3　脆弱性类别

类　别	对　象	脆　弱　性
技术脆弱性	传输设备和网络设备	1、网络规划和拓扑、设备部署、资源配置的缺陷等。 2、网络保护和恢复的缺陷等。
	安全	1、各类安全防护设备的部署位置不当的缺陷。 2、安全技术措施和策略方面的漏洞等。 3、各类知识库、病毒库实时更新方面的缺陷。
	主机/服务器	包括设备软硬件安全性方面的漏洞。 1、可靠性、稳定性、业务支持能力和数据处理能力、容错和恢复能力的缺陷。 2、设备访问的连接、授权、鉴别、代理和控制方面的安全漏洞，以及授权接入的口令、方式、安全链接、用户鉴别、代理等访问控制方面的漏洞隐患等。 3、相关数据信息在使用、传输、保存、备份、恢复等环节中的安全保护技术缺陷和安全策略方面的漏洞等。
	物理环境	物理环境方面的安全防护能力的缺陷，可分为：机房场地的选择，防火、供配电、防静电、接地与防雷、电磁防护、温

		湿度控制、租用电信运营商的线路、机房设施及设备的防护等。
管理脆弱性		包括组织体制、人员、保障、应急预案、外包服务等方面安全机制和管理制度在制定和实施过程中各环节的漏洞及缺陷。可分为： a） 机构方面（如岗位设置、授权与审批程序、沟通与合作等）。 b） 制度方面（如管理制度和相应的评审、考核、检查、修订等）。 c） 建设方面（如安全方案不完善、软件开发不合程序、工程验收不合规定等）。 d） 运维方面（物理环境的管理、设备维护、技术支持、关键设备性能指标监控、攻击预防措施、数据备份与恢复、访问控制、操作管理及应急保障措施等）。 e） 业务方面（如相关的接入、访问、服务优先级、资源管理、数据信息检查等业务接入管理方面的缺陷等）。

5 政务外网安全等级保护概述

5.1 政务外网安全保护等级

政务外网开展安全等级保护工作的重点是广域网和各级城域网。政务外网中央至省、省至地（市）广域网和中央、省级、地（市）级城域网应达到安全等级保护第三级要求，地（市）级至区县广域网和地（市）以下城域网应至少达到安全等级保护第二级的要求。

政务外网主要满足各级政务部门业务应用系统传输和跨部门数据交换与共享的需要，保证其在广域网和城域网上的畅通、安全和可靠。不同安全等级保护的政务外网互联，应在配置网络边界访问控制的情况下，确保业务的畅通。

政务外网可以承载各级政务部门安全等级为 1 至 5 级的电子政务信息系统，其中如各政务外网接入单位确定为四级及以上的信息系统传输时，可采用密码技术对数据进行端到端加密传输，其系统和数据的安全由接入单位自行负责。

对于接入单位尚未开展信息系统安全等级保护工作或安全等级保护在 2 级及以下的单位局域网接入时，应加强政务外网边界访问控制和监测措施，保证政务外网的安全。

5.2 不同等级的安全保护能力

第二级安全保护能力：应能够防护网络免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击，能够抵抗一般的自然灾难，以及其他相当危害程度的威胁所造成的重要损害，能够发现重要的安全漏洞和安全事件。在网络遭到损害后，**其影响范围在地（市）到县的广域网和县级城域网，**并能够在一段时间内恢复部分功能。

第三级安全保护能力：应能够在统一安全策略下防护网络免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击，能够抵抗较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够及时发现安全漏洞和安全事件。在网络遭到损害后，**其影响范围是省级及以上广域网和地（市）级及以上城域网**，并能够较快恢复绝大部分功能。

6 第二级基本要求

6.1 IP 承载网

6.1.1 广域网

6.1.1.1 结构安全（G2）

a) 关键设备的业务处理能力应具有一定的设备和链路冗余等保护措施，网络的组织和分布应满足各类业务稳定性、可靠性和安全性的要求；
b) 广域网的链路带宽应满足承载业务和数据传输的需要；
c) IP 层的网络设备时钟应与上级设备时钟同步。

6.1.1.2 网络保护与恢复(A2)

a) 应能根据各级政务部门业务应用的需要采用链路倒换、聚合等安全保护措施，相关技术指标应达到网络和业务的需要；
b) 链路的倒换、聚合应不影响各级政务部门重要信息系统和业务的正常使用；
c) 广域网络设备原则上应与城域网的核心节点互联。

6.1.1.3 访问控制(A2)

a) 应在广域网与城域网或用户局域网之间的网络边界部署相关访问控制设备，启用访问控制功能；
b) 根据政务外网的网络承载力，应对网络中的广播、组播进行必要的控制；
c) 在广域网内，专用网络区与公用网络区应采用 MPLS VPN 技术隔离，专用网络区及公共网络区域之间路由不可达，数据不能直接访问。

6.1.1.4 安全审计(S2)

a) 安全审计日志记录要求保存至少半年以上；
b) 应能够根据记录数据进行分析，并生成审计报表，相关信息应报送安全管理系统。

6.1.2 城域网

6.1.2.1 结构安全(G2)

a) 城域网的核心设备应具有一定的设备冗余，核心设备之间的骨干应至少保证不同路由主备链路或环进行保护，其链路带宽应满足业务的需要；
b) 城域网的骨干路由带宽应满足业务的需要；
c) 应根据实际需要及接入单位的分布合理设置汇接节点；
d) 城域网络设备的时钟应能与广域网络设备的时钟同步。

6.1.2.2 访问控制(A2)

a) 应在城域网与用户局域网连接边界及安全等级不同的网络边界配置相应的访问控制功能；
b) 公用网络区与互联网接入区等区域之间需要进行数据交换时，应采用防火墙、路由控制等相关安全措施，并对交换数据进行病毒扫描和审计。

6.1.2.3 用户局域网

1) 用户局域网内的安全防护和安全责任由用户单位自行负责；
2) 用户单位的信息系统已按国家要求进行了安全等级保护二级或三级备案时，在接入政务外网时应提供信息系统安全等级保护备案证明；
3) 局域网内的终端如既能访问政务外网的业务、又能访问互联网，各政务部门应根据自身业务的重要性，采取技术措施，逐步达到控制该终端访问互联网，其现有的技术手段如下，但不

仅限于此：

i. 通过接入互联网侧防火墙的访问控制策略对该终端访问互联网加以必要的限制；

ii. 通过对终端硬盘分区，加密保存业务数据或相关工作文档，通过安全管理软件，当进行工作文档编写、数据处理时，能自动断开该终端的互联网连接；

iii. 通过插入 USBKey 时自动断开该终端的互联网连接，只能访问指定的政务外网服务器和应用系统；

iv. 可采用虚拟终端等技术，保证同一台终端不能同时访问并操作政务外网业务和互联网业务。

6.2 业务区域网络

6.2.1 公用网络区

6.2.1.1 结构安全(G2)

a) 公用业务服务器应采用统一规划的 IP 地址，保证跨部门、跨地区业务的交换与共享；

b) 应根据所部署系统的重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；

c) 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵时候优先保护重要业务的畅通。

6.2.1.2 访问控制(A2)

a) 通过互联网或其他公众通信网络对公用网络区的信息系统进行远程访问，须采用 VPN 网关、信道加密，以及身份认证、IP 地址绑定、审计等安全措施；

b) 应通过身份认证、授权管理系统等对公用网络区的信息系统进行保护。

6.2.2 互联网接入区

6.2.2.1 结构安全(G2)

1) 应选用一个及以上电信运营商或互联网业务提供商（ISP）作为访问互联网的出口；

2) 在采用主备或负载均衡等方式时，不同链路的安全策略应该保持一致；

6.2.2.2 访问控制(A2)

1.1 如需对其互联网区的信息系统或服务器进行远程维护和管理，应采用身份认证、信道加密、指定管理终端等安全措施；

1.2 应能有效防止以下攻击行为：病毒攻击、端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、SQL 注入、跨站攻击和网络蠕虫攻击等；

1.3 应具备流量分析控制、异常告警等功能，能区分各类 HTTP、FTP、TELNET、SMTP、POP3、P2P 等网络协议并进行过滤。

6.3 管理区域网络

6.3.1 网络管理区(S2)

a) 政务外网 IP 承载网相关网络设备与网管系统应作为一个整体，明确边界，按信息系统安全等级保护的要求实施保护；

b) 应绘制与当前运行情况相符的网络拓扑结构图、有相应的网络配置表，包含设备 IP 地址等主要信息，并及时更新、妥善保管并做好备份，且不得对外公开；

c) 应保证网管系统数据安全、可靠；

d) 网络管理系统应具有资产管理、图形展现、实时告警并具有声、光、电等功能，告警信息能

通过各种技术手段及时通知相关人员；

e) 网络管理用的终端应专用，有专人负责，并不得访问互联网；

f) 应确保网管系统与设备间、网管系统之间的管理信息通信通畅。

6.3.2 安全管理区(S2)

图A.1 安全管理系统（或平台）可与安全防护设备、网关、审计系统等，作为一个信息系统的整体，按信息系统安全等级保护的要求实施保护；

图A.2 安全管理系统应能对管辖内的安全防护设备的日志、故障、病毒攻击、安全运行状态进行监测；

图A.3 安全管理用的终端应专用，有专人负责，并不得访问互联网；

图A.4 应按日、周、月、季、年或按管理部门的要求出具安全运行报告。

7 第三级基本要求

7.1 IP 承载网

7.1.1 广域网

7.1.1.1 结构安全(G3)

a) 关键设备的业务处理能力应具有一定的节设备和链路冗余等保护措施，网络的组织和分布应满足各类业务稳定性、可靠性和安全性的要求；

b) 广域网的链路带宽应满足承载业务和数据传输的需要，**其带宽至少为历史峰值的 1.5 倍；**

c) IP 层的网络设备时钟应与上级设备时钟同步；

d) 主用与备用的核心网络设备应放置在不同物理位置的机房；

e) 应采用物理路由分离的两条骨干链路来提供“1+1”的网络保护方式，两条链路在技术和性能等方面应保持一致；

f) 地（市）级及以上网络设备应支持 MPLS VPN 的业务，并保证国家相关业务部门到省、地（市）、县业务的连通；

g) 应根据需要采用有效的 QoS 和流量管理策略，保证管理和控制信息具有较高的优先级；

h) 应保证国家、省、地（市）广域网的高速畅通，不允许串接相关安全防护设备。

7.1.1.2 网络保护与恢复(A3)

11 **国家、省、地（市）的广域网主要设备、模块及链路应采用主备方式；**

12 应能根据各级政务部门业务应用的需要采用链路倒换、聚合等安全保护措施，相关技术指标应达到网络和业务的需要；

13 链路的倒换、聚合应不影响各级政务部门重要信息系统和业务的正常使用；

14 广域网络设备原则上应与城域网的核心节点互联。

7.1.1.3 访问控制(A3)

a) 应在广域网与城域网或用户局域网之间的网络边界部署相关访问控制设备，启用访问控制功能；

b) 根据政务外网的网络承载力，应对网络中的广播、组播进行必要的控制；

c) 在广域网内，专用网络区与公用网络区应采用 MPLS VPN 技术隔离，不同的专用网络区及公共网络区域之间路由不可达，数据不能直接访问；

d) 应具备限制网络最大流量数及网络连接数的能力；

e) 根据国家有关互联网出口属地化原则，政务外网中央和省级广域网不得承载互联网

的流量。

7.1.1.4 安全审计(S3)

a) 安全审计日志记录要求保存至少半年以上；

b) 应能够根据记录数据进行分析，并生成审计报表，相关信息应报送安全管理系统。

7.1.2 城域网

7.1.2.1 结构安全(G3)

- 城域网的核心设备应具有一定的设备冗余，核心设备之间的骨干应至少保证不同路由主备链路或环进行保护，其链路带宽应满足业务的需要；
- 城域网的骨干路由带宽应满足业务的需要；
- 应根据实际需要及接入单位的分布合理设置汇接节点；
- 城域网络设备的时钟应能与广域网络设备的时钟同步；
- **国家、省级城域网的核心原则上应采用网状或环状网络结构；**
- **汇接节点与核心节点原则上应至少保有两条不同物理路径的连接，防止设备或链路故障影响业务系统的正常使用；**
- **应根据需要采用有效的 QoS 和流量管理策略，保证重要信息系统和数据具有较高的优先级；**
- **自建用于政务外网的传输系统（含管理软件、SDH 设备、MSTP 多业务传输平台等），可与 IP 承载网同步定级，其安全等级应与城域网安全等级一致。**

7.1.2.2 访问控制(A3)

1) 应在城域网与用户局域网连接边界及安全等级不同的网络边界配置相应的访问控制功能；

2) 城域网内根据接入业务的需要划分其他区域（或服务层）时，应按业务和安全的要求，制定相应访问控制策略，保证数据和信息系统的安全；

3) 应在广域网与城域网或用户接入网之间的网络边界部署相关访问控制设备，启用访问控制功能，对接入用户的边界访问控制，根据条件其访问控制设备也可放在汇聚层；

4) 城域网应支持 MPLS VPN 技术，按接入业务的需要和数据交换与共享的要求区分不同的网络区域；

5) 城域网中的专用网络区、公用网络区和互联网接入区等其他网络区域应采用 VPN 隔离措施，不同区域的系统和数据不能直接访问；

6) 公用网络区与互联网接入区等区域之间需要进行数据交换时，应采用防火墙、路由控制、**网闸、数字证书**等相关安全措施，并对交换数据进行病毒扫描和审计。

7.1.3 用户局域网

a) 用户局域网内的安全防护和安全责任由用户单位自行负责；

b) 用户单位的信息系统已按国家要求进行了安全等级保护二级或三级备案时，在接入政务外网时需提供信息系统安全等级保护备案证明；

c) 局域网内的终端如既能访问政务外网的业务、又能访问互联网，各政务部门可根据自身业务的重要性，采取技术措施，逐步达到控制该终端访问互联网，其现有的技术手段如下，但不仅限于此：

a.1.1 通过接入互联网侧的防火墙的访问控制策略对该终端访问互联网加以必要的限制；

a.1.2 通过对终端硬盘分区，加密保存业务数据或相关工作文档，通过安全软件，当进行工作文档编写、数据处理时，自动断开该终端的互联网连接；

a.1.3 通过插入 USBKey 时自动断开该终端的互联网连接，只能访问指定的政务外网服务器和应用系统；

a.1.4 可采用虚拟终端等的技术，保证同一台终端不能同时访问政务外网业务和互联网业务。

7.2 业务区域网络

7.2.1 公用网络区

7.2.1.1 结构安全(G3)

a) 公用业务服务器应采用统一规划的 IP 地址，保证跨部门、跨地区业务的交换与共享；

b) 应根据所部署系统的重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；

c) 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵时候优先保护重要业务的畅通；

d) 公用网络区的主要网络设备应具备设备冗余、链路冗余等保护措施，应满足各类业务带宽、稳定性、可靠性和安全性的要求。

7.2.1.2 访问控制(A3)

a) 通过互联网或其他公众通信网络对公用网络区的信息系统进行远程访问时，须采用 VPN 网关、信道加密，以及数字证书、IP 地址绑定、审计等安全措施；

b) 应通过身份认证、授权管理系统等对公用网络区的信息系统进行保护；

c) 公用网络区与互联网接入区采用 MPLS VPN 进行逻辑隔离，二个区域的数据和系统不能直接访问；

d) 当公用网络区的主机/服务器需要从互联网接入区获取数据时，应采用安全隔离设备、防火墙、路由策略、身份认证、设备认证、审计等安全措施。

7.2.2 互联网接入区

7.2.2.1 结构安全(G3)

应选用二个及以上电信运营商或互联网业务提供商（ISP）作为访问互联网的出口；

在采用主备方式或负载均衡等方式时，不同链路的安全策略应该保持一致；

7.2.2.2 访问控制(A3)

a) 如需对互联网接入区的信息系统或服务器进行远程维护和管理，应采用身份认证、信道加密、指定终端等安全措施；

b) 应能有效防止以下攻击行为：病毒攻击、端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、SOQ 注入、跨站攻击和网络蠕虫攻击等；

c) 应具备流量分析控制、异常告警等功能，能区分各类 HTTP、FTP、TELNET、SMTP、POP3、P2P 等网络协议并进行过滤；

d) 应具备监测检测恶意代码并实时告警的功能，在有条件的情况下，应能与防火墙、入侵检测等安全防护设备联动，有效阻止敏感信息的泄漏；

e) 通过互联网等公众通信网接入政务外网的各类移动业务，应尽量与政务部门访问互联网的出口业务分开，做好相应的访问控制。

7.2.3 专用网络区

7.2.3.1 结构安全（G3）

a) 各级政务部门根据业务需求在政务外网上构建专用网络承载其业务时，应采用 MPLS VPN 或其他 VPN 技术，实现与其他政务部门的业务逻辑隔离；

b) 为保证 VPN 的服务质量，应具备对 VPN 的网络性能等相关数据进行分析的能力，对重点接入

单位和重要信息系统应采用双链路上联政务外网，保证其可靠性；

c) 专用网络区内业务数据流向及安全措施等要求由相应部门自行确定；

d) 应保证广域网络技术的一致性，保证端到端业务的畅通、安全、可靠。

7.2.3.2 访问控制(A3)

a) 在接入边界处设置网关或防火墙等边界访问控制设备，防止非法用户业务流的进入；

b) 应具有网络流量控制能力，防止由于资源挤占而影响其他重要信息系统和网管信息的正常传送；

c) 通过互联网或其他公众通信网络接入 VPN 时，应采用政务外网数字证书、加密传输、安全网关等安全技术措施，保证数据和信息系统的安全；

d) 专用网络区内的信息系统的安全等级，相关的访问控制、入侵防护、数据安全等由相应部门自行确定。

7.3 管理区域网络

7.3.1 网络管理区(S3)

a) 政务外网的 IP 承载网的相关网络设备与网管系统应作为一个整体按信息系统安全等级保护的要求实施保护；

b) 根据网络结构、管理分界，原则上采用国家、省二级或国家、省、地（市）三级分域分级的管理方式，根据实际需要设置分级权限，实现对网络的灵活管理；

c) 应绘制与当前运行情况相符的网络拓扑结构图、有相应的网络配置表，包含设备 IP 地址等主要信息，并及时更新、妥善保管并做好备份，且不得对外公开；

d) 应保证网管系统数据安全、可靠；

e) 网络管理系统应具有资产管理、图形展现、实时告警并具有声、光、电等功能，告警信息能通过各种技术手段及时通知相关人员；

f) 网络管理用的终端应专用，有专人负责，并不得访问互联网；

g) 应确保网管系统与设备间、网管系统之间的管理信息通信通畅；

h) 网管网络应与电子政务业务网络逻辑隔离，确保网管数据的安全；

i) 应具备异构网络管理系统的互联功能，实现相关管理数据的共享；

j) 对重要主机/服务器的运行状况（如 CPU 利用率、内存使用情况等）进行监测；

k) 网络管理系统应对同一管理员采用两种或两种以上组合的鉴别技术进行身份鉴别。

7.3.2 安全管理区(S3)

a) 安全管理系统（或平台）可与安全防护设备、网关、审计系统等，作为一个信息系统的整体，按信息系统安全等级保护的要求实施保护；

b) 安全管理系统应能对管辖内的安全防护设备的日志、故障、病毒攻击、安全运行状态进行监测；

c) 安全管理用的终端应专用，有专人负责，并不得访问互联网；

d) 应按日、周、月、季、年或按管理部门的要求出具安全运行报告，**并对相关病毒攻击、信息安全事件提出建议；**

e) 对网络及管辖区域内安全风险提出预警、对安全运行情况及态势进行分析等；

f) 应具备异构安全管理系统的互联功能，实现相关管理数据的共享、分析，为全网的安全事件应急响应、安全事件预警提供技术支撑。

7.3.3 电子认证区

对于此区域的安全防护和要求，请参考国家法律法规和密码管理主管部门关于密码管理的相关规定及国家对信息系统的安全等级保护相关标准进行保护。