国 家 电 子 政 务 外 网 标 准

GW0015—2022

政务外网终端一机两用安全管控技术指南

Security Control Technical Guidance for One PC Two Terminals of National E-Government Network

2022-7-1 发布　　2022-9-1 实施

国家电子政务外网管理中心

目 次

前　　言 I
引　　言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
3.1 1
3.2 1
3.3 1
3.4 1
3.5 2
4 缩略语 2
5 安全管控框架 2
5.1 安全管理框架 2
5.2 安全技术框架 3
6 广域网边界安全检测技术要求 4
7 城域网边界安全控制技术要求 4
7.1 统一管控模式城域网边界控制技术要求 4
7.2 自行管控模式城域网边界控制技术要求 5
8 局域网终端安全管控技术要求 5
8.1 基本要求 5
8.2 终端准入控制 5
8.3 终端安全隔离 6
9 终端安全管控模式建设指南 6
9.1 自行管控模式 6
9.2 统一管控模式 6
9.3 终端数据同步 6
附　录　A （资料性） 政务外网广域网检测部署实施指南 8
附　录　B （资料性） 统一管控模式终端控制部署实施指南 10
附　录　C （资料性） 自行管控模式终端安全管控部署实施指南 12
附　录　D （资料性） 跨层级或跨部门终端安全管控设施实施指南 14
附　录　E （资料性） 政务外网终端安全防护技术要求 15

前　言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件对当前政务外网安全标准中未涉及的政务外网终端“一机两用”情况的管控技术进行建设指导。

本文件由国家电子政务外网管理中心提出并归口。

本文件起草单位：国家电子政务外网管理中心、深圳市联软科技股份有限公司、深信服科技股份有限公司、华为技术有限公司、奇安信科技集团股份有限公司。

本文件主要起草人：徐春学、罗海宁、焦迪、王海军、蔡达、滕颖志、俞晓舟、王伟、张淑敏、熊志刚、李宁、程子栋、田之洋、任飞、王鹏彪。

引　言

为保障政务外网整体安全性，防范化解政务外网终端安全风险，本文件针对各级政务部门终端“一机两用”接入政务外网的情况，针对广域网、城域网及局域网，构建边界检测、边界控制及终端安全管控能力提出具体技术要求，并对于政务外网建设运维管理单位对本级终端统一管控或由各政务部门自行管控两种管理方式提出具体建设指南，便于各级政务外网建设运维管理单位根据自身管理情况开展建设。

政务外网终端一机两用安全管控技术指南

1 范围

本文件规定了政务外网终端“一机两用”安全管控框架，给出了广域网边界、城域网边界、局域网终端安全管控技术要求及终端安全管控模式建设指南。

本文件适用于指导政务外网终端“一机两用”情况下，各级政务部门和各级政务外网建设运维管理单位对接入政务外网的终端进行安全管控。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2010 信息安全技术 术语

GW 0103-2011 国家电子政务外网安全等级保护基本要求

GW 0206-2014 接入政务外网的局域网安全技术规范

3 术语和定义

GB/T 25069-2010界定的以及下列术语和定义适用于本文件。

3.1

政务外网终端一机两用 one PC two terminals of national e-government network

通过政务外网专线接入，既可访问政务外网业务，也可访问互联网或其他网络的办公终端。终端包括台式微型计算机系统、便携微型计算机系统、瘦客户机系统或虚拟终端系统等。

3.2

终端安全隔离 terminal safety isolation

政务外网终端一机两用时，通过网络隔离、会话隔离及数据隔离等措施，实现两网应用及数据的安全访问。

3.3

零信任 zero trust

经过身份鉴别、授权后获得访问目标资源，并基于主体、环境和行为等多维度属性及状态制定动态策略，持续评估，并动态调整资源访问权限的理念和方法。

3.4

沙箱 sandbox

通过驱动层或应用层重定向技术在终端上创建一个与个人环境完全逻辑隔离的环境，实现对沙箱中运行的软件（应用程序）所有系统操作的管控，并能对沙箱中运行的软件（应用程序）实施通信加密、落地文件加密、内外网络访问隔离、剪切板控制、外设管控、程序管控、文件外发管控等数据保护功能。

3.5

应用支撑 application support

面向政务外网公共应用提供应用代理访问支撑服务。

4 缩略语

下列缩略语适用于本文件。

CA：证书颁发机构（Certificate Authority）

MAC：媒体接入控制（Media Access Control）

IP：网际互联协议（Internet Protocol）

5 安全管控框架

5.1 安全管理框架

5.1.1 安全管理框架基本要求

政务外网建设运维管理单位和政务部门应按照“全盘统筹、多级部署、分层管控、属地管理”的原则，根据业务部署场景构建相应的政务外网终端“一机两用”安全管控体系。

5.1.2 统一管控模式管理框架

对于政务外网业务集中部署在本层级政务云的场景，采用统一管控模式构建政务外网终端“一机两用”安全管理框架，具体如下图所示：

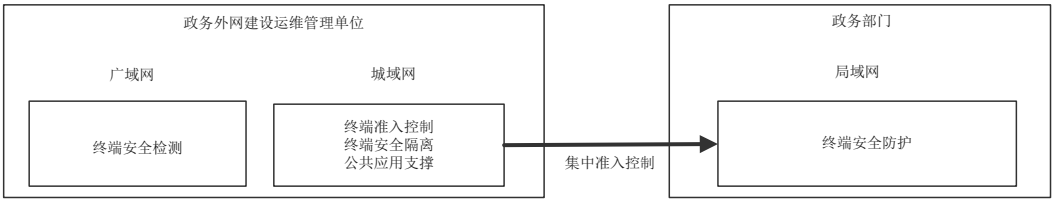


图 1 统一管控模式管理框架

统一管控模式管理框架包括如下内容：

a） 政务外网建设运维管理单位应在城域网边界实施统一准入、安全隔离及应用支撑，在广域网边界实施终端安全检测；

b） 政务部门应自行负责终端安全防护。

5.1.3 自行管控模式管理框架

对于政务外网业务分散部署在政务部门局域网内的场景，采用自行管控模式构建政务外网终端“一机两用”安全管理框架，具体如下图所示：

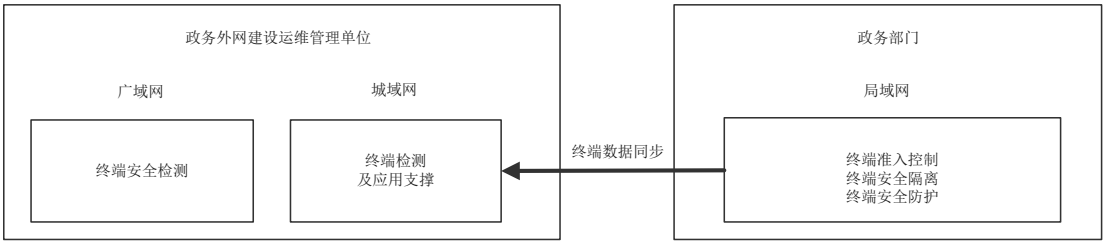


图 2 自行管控管理框架

自行管控模式管理框架包括如下内容：

a） 政务部门应自行负责终端安全防护，包括终端准入控制、终端安全隔离和终端安全防护；

b） 政务外网建设运维管理单位应在城域网边界实施终端检测、应用支撑和安全集中监控，在广域网边界实施终端安全检测；

c） 各级政务部门应将终端管控相关管理数据同步给所在层级的政务外网建设运维管理单位。

5.2 安全技术框架

中央、省、市各级政务外网按照终端安全管控的一般技术要求，分别在广域网、城域网、局域网采取不同的安全管控技术措施，形成整体技术框架如下图所示：

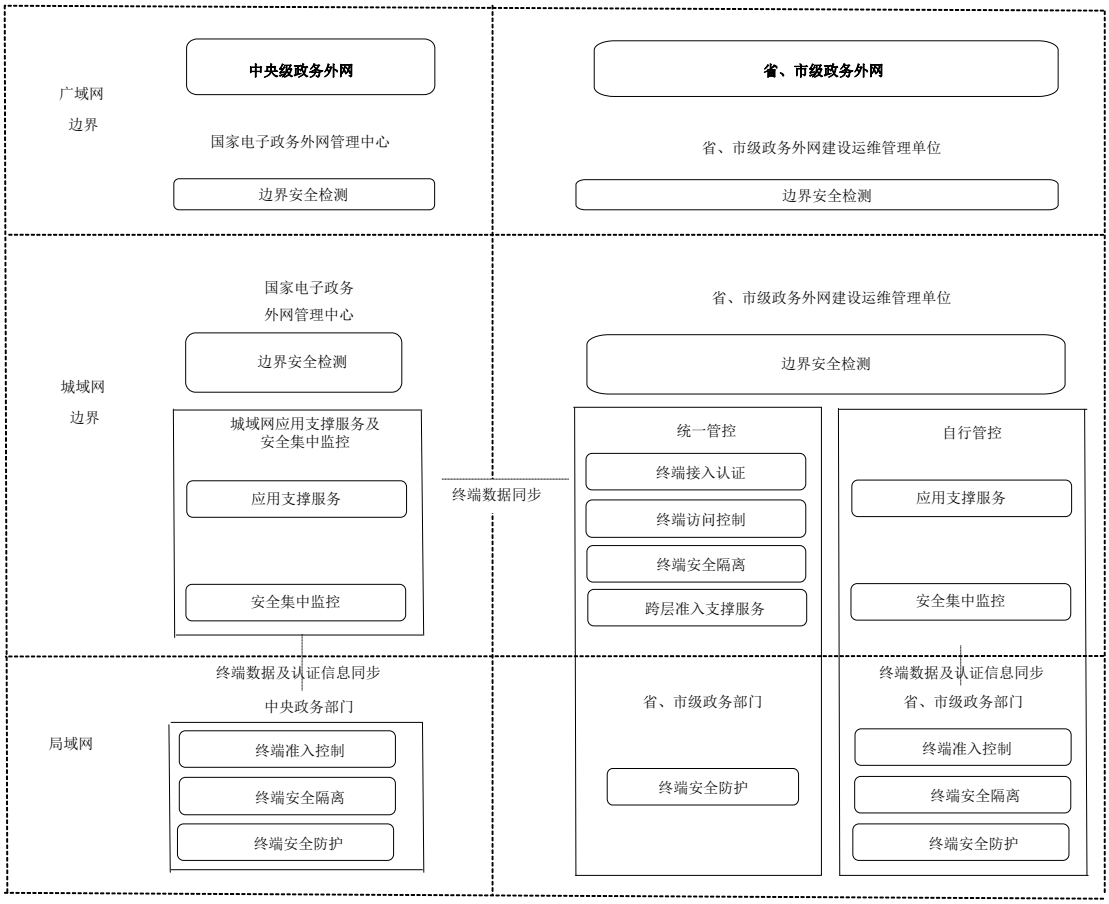


图 3 政务外网终端安全管控技术框架

总体技术框架包括如下内容。

a） 广域网边界安全控制：中央、省级、市级各级政务外网建设运维管理单位应在广域网边界构建安全检测设施，对政务外网终端访问流量进行安全检测，重点实现对异常或恶意行为进行告警，重大应急情况下可实施阻断。

b） 城域网边界安全控制：中央、省级、市级各级政务外网建设运维管理单位应在流量安全检测的基础上，根据业务是否集中部署构建相应的终端控制设施。

（1） 统一管控模式：对于业务集中场景，各级政务外网建设运维管理单位应在城域网边界构建统一终端控制设施，对本级政务外网终端实施终端接入认证、终端安全隔离、访问控制和整体监控。可对问题终端实施封堵，具备终端会话层精准阻断能力，并具备面向跨层级业终端提供统一准入支撑服务的能力。

（2） 自行管控模式：对于业务非集中场景，各级政务部门应自行负责终端安全防护设施建设，政务外网建设运维管理单位应负责提供应用支撑服务及安全集中监控。

c） 局域网终端安全控制：根据业务是否集中部署构建相应的终端控制设施。

（1） 统一管控模式：对于业务集中部署场景，各级政务部门主要负责终端安全防护建设，包括恶意代码防范、终端入侵防护、非法外联控制、终端精准阻断等。

（2） 自行管控模式：对于业务非集中部署场景，各级政务部门应自行负责终端安全防护设施建设，具备终端准入控制、终端安全隔离和终端安全防护能力。其中准入控制包括身份认证、终端安全检查、资源访问控制。终端安全隔离包括网络隔离、会话隔离、数据隔离。

区县及以下政务部门终端安全管控应由市级或省级政务外网建设运维管理单位统筹建设，或参照标准自行建设。

6 广域网边界安全检测技术要求

广域网边界安全检测技术要求包括如下内容：

a） 应在广域网边界对政务外网终端访问流量进行安全检测，且支持对加密流量的安全检测，重点对僵木蠕、C&C 异常、渗透攻击等异常或恶意行为进行告警，重大应急情况下可实施阻断；

b） 应对终端同时连接政务外网和互联网的行为进行检测、告警，并具备阻断能力；

c） 在政务外网广域网边界部署针对终端的安全控制类设备时，应满足双机热备、双主控、双活等高可用要求，网络时延不高于 10 微秒。

7 城域网边界安全控制技术要求

7.1 统一管控模式城域网边界控制技术要求

对于业务集中部署场景，各级政务外网建设运维管理单位应统一建设城域网边界控制设施，除了满足广域网边界检测技术要求之外，还应对接入城域网的终端进行集中准入管理。

a） 应对接入政务外网终端在城域网侧实施访问权限管理，基于城域网构建的统一身份管理或网络资源目录平台，登记注册涉及终端访问的业务应用，并以目录管理的方式实现终端与业务的授权。

b） 在城域网侧终端准入设施上以网关或代理类设施实现应用重定向和终端接入认证，或与终端侧控制软件实施策略联动，终端接入认证采用扫码认证、MAC 认证等。

c） 城域网侧终端认证可按照接入单位类型、终端单网性质、局域网安全状态等综合情况进行分类，实施终端访问控制。

d） 城域网边界终端准入设施应具备面向跨层级业务终端提供统一准入支撑服务。
e） 城域网侧终端准入设施和局域网侧终端控制设施应实现两级对接，包括并不限于身份信息、业务授权信息、终端安全审计信息。
f） 应支持多层 NAT 场景下基于会话的精准阻断，并支持配置策略生效时段和老化时间。
g） 应对 NAT 场景下的政务外网终端实现源 IP 溯源审计。
h） 应对接入政务外网终端运行的安全情况进行集中监控。

7.2 自行管控模式城域网边界控制技术要求

对于业务非集中部署场景，各级政务外网建设运维管理单位除了满足广域网边界检测技术要求之外，还应建设城域网应用支撑服务和安全集中监控设施。

a） 面向本级政务部门提供重要公共应用安全防护支撑服务。
b） 应对接入政务外网终端运行的安全情况进行集中监控。

8 局域网终端安全管控技术要求

8.1 基本要求

在统一管控模式或自行管控模式下，都应对各政务部门局域网内一机两网的政务终端实施终端准入控制、终端安全隔离，实现对终端进行有效安全管控，保障政务外网终端访问安全性。

8.2 终端准入控制

8.2.1 身份认证

终端接入政务外网之前，用户终端应通过身份认证，非授权的用户终端不允许接入政务外网，应当满足以下要求：

a） 接入政务外网的用户终端应具备唯一标识，唯一标识的信息应至少包括使用者信息和终端设备信息，并实现用户与终端实名绑定，以便后续审计溯源；
b） 应采用口令认证、密码技术、生物技术或 MAC 认证等鉴别技术对用户进行认证；
c） 登录用户的身份鉴别信息应具有复杂度要求并定期更换。

8.2.2 安全检查

终端接入政务外网之前，应通过安全接入检查，不符合要求的终端不允许接入政务外网，应检查以下内容：

a） 应检查终端是否安装运行了防病毒软件；
b） 应检查终端是否存在弱口令账户；
c） 应检查终端是否运行了恶意进程或软件；
d） 应检查终端是否存在未修复的高危漏洞。

8.2.3 传输加密

终端接入通过身份认证和安全检查后，应采用密码技术保证通信传输安全，应当满足以下要求：

a） 应采用密码技术保证数据在传输过程中的保密性,包括但不限于鉴别数据、重要业务数据和重要个人信息等；
b） 应当支持国密算法，并满足国家密码应用的标准要求。

8.2.4 应用访问控制

终端接入政务外网后，应实现应用访问控制，应当满足以下要求：

a） 终端接入政务外网时，应实现基于角色的应用访问控制，并实现最小授权；

b） 应对终端环境进行持续检测和评估，根据评估情况动态调整其应用访问权限。

8.3 终端安全隔离

政务外网终端存在访问多个网络的情况下，应当满足以下要求：

a） 应支持网络隔离，确保终端获得准入授权后通过安全隧道访问政务外网，不能同时访问互联网或与互联网连通的其他网络；

b） 应支持会话隔离，确保每个终端访问政务外网时采用唯一会话，可通过添加有效期内唯一的会话状态信息来实现；

c） 应采用沙箱技术，确保终端访问政务外网敏感应用系统下载的数据只能落入沙箱加密隔离存放，且数据使用和外发行为受控，防止终端数据泄露，且沙箱所使用密码技术应满足国家密码应用的标准要求。

9 终端安全管控模式建设指南

9.1 自行管控模式

对于业务非集中部署场景，应当按自行管控模式建设。

a） 对于业务系统分散部署于各级政务部门局域网的场景，应按照“8.局域网终端安全管控技术要求”建设终端控制设施，对本单位的终端进行安全管理，建设实施可参考附录 C、E；

b） 政务外网建设运维管理单位应按照“6 广域网边界安全检测技术要求”和“7.2 自行管控模式城域网边界控制技术要求”建设相关设施。广域网边界安全检测设施建设实施可参考附录 A。

9.2 统一管控模式

对于业务集中部署场景，应当按统一管控模式建设。

a） 对于业务系统集中部署于城域网统一政务云平台的场景，各级政务外网建设运维管理单位应按照“7.1 统一管控该模式城域网边界控制技术要求”统筹建设终端安全管控设施，对接入政务外网的终端实现统一准入控制、安全隔离等，各级政务部门无需重复建设，建设实施可参考附录 B；

b） 针对跨层级和跨部门终端安全访问控制场景，技术要求参考附录 D；

c） 局域网终端安全防护原则上归政务部门自行管理，技术要求参考附录 E。

9.3 终端数据同步

各级政务外网建设运维管理单位和政务部门应当按以下要求实现终端数据统计分析和终端数据同步。

a） 各级政务外网建设运维管理单位应对本级政务部门接入政务外网终端数据统计分析，且以可视化方式呈现终端安全运行相关态势，至少应分析展示以下内容：终端总数、操作系统情况、客户端安装数、终端安全情况等信息；

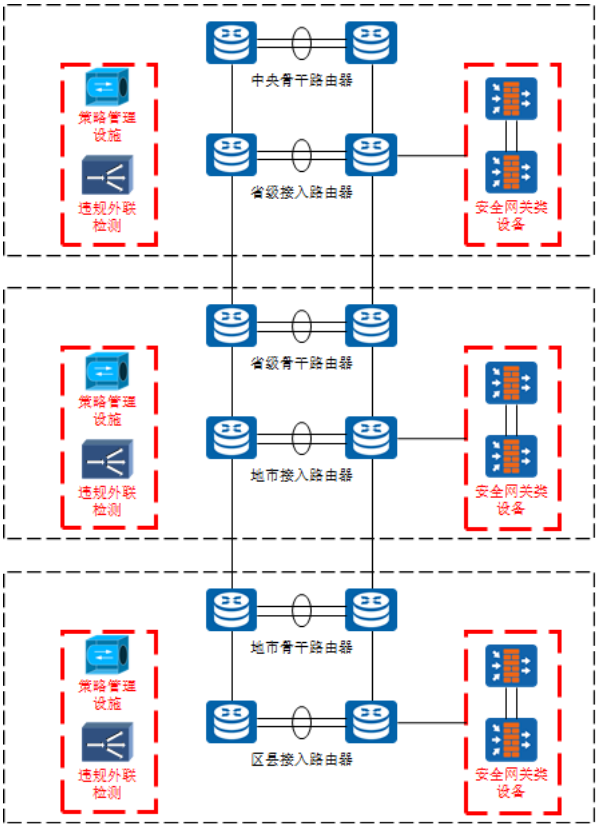
b） 下级政务外网建设运维管理单位应向上级政务外网建设运维管理单位同步相关数据，至少应同步终端总数、操作系统情况、客户端安装数、终端安全事件等信息；

c） 自行管控建设模式，政务部门应向本级政务外网运维管理单位至少同步终端总数、操作系统情况、客户端安装数、终端安全事件等信息。

附 录 A
（资料性）
政务外网广域网检测部署实施指南

A.1 概述

各级政务外网建设运维管理单位应在广域网边界构建终端检测设施，对政务外网终端访问流量进行安全检测，重点实现对异常或恶意行为进行告警，重大应急情况下可实施阻断。



图A.1 政务外网广域网边界终端检测部署示意图

A.2 功能说明

A.2.1 安全网关类设备：通过透明部署或者物理旁路逻辑串联等方式部署于广域网边界。

a） 安全网关设备通过入侵防御、病毒检测功能对政务外网终端访问流量进行安全检测，并对加密流量进行安全检测，重点对僵木蠕、C&C 异常、渗透攻击、APT 攻击等异常或恶意行为进行告警，重大应急情况下可实施阻断。

b） 态势感知平台、非法外联检测系统等检测到的威胁攻击行为，通过调用安全网关设备开放的策略阻断北向接口，实现威胁攻击行为的阻断。

A.2.2 违规外联检测：各级电子政务外网建设运维管理单位可选择在广域网边界进行部署。违规外联检测系统通过主动探测、镜像流量检测、客户端主动检测和上报等方式，对终端同时连接政务外网和互联网的行为进行检测、告警，并能够联动安全网关设备实现基于会话的阻断。

A.2.3　策略管理设施：

a） 对违规外联检测发现的违规外联行为进行策略编排，并下发到指定安全网关类设备或客户端进行处置；

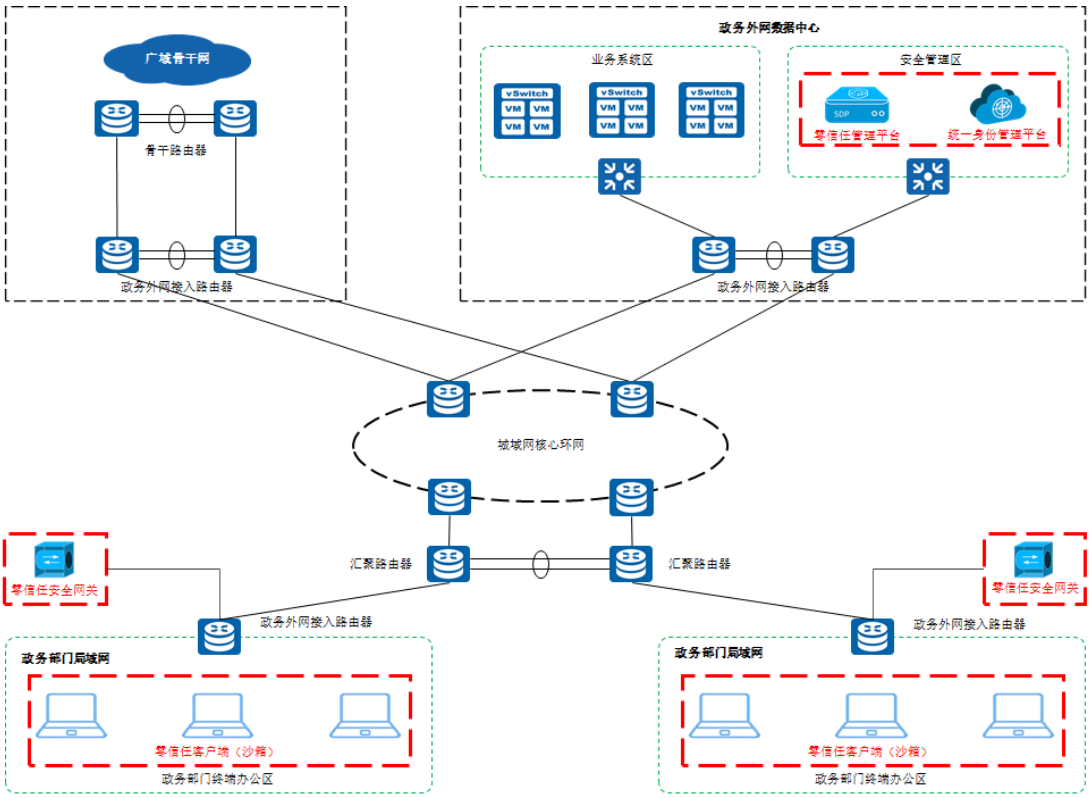
b） 对安全检测类设备发现的恶意攻击行为进行策略编排，并下发到指定安全网关类设备进行处置。

c） 对安全网关设备进行集中配置管理，实现安全策略配置、下发、编排、冗余分析等。

附　录　B
（资料性）
统一管控模式终端控制部署实施指南

B.1 概述

对于业务集中部署在城域网的场景，各级政务外网建设运维管理单位应在终端流量安全检测的基础上，在城域网边界构建终端控制设施，通过终端安全控制设施对本级政务外网终端分类实施终端接入认证、访问控制和整体监控，可对问题终端实施封堵，具备终端会话层精准阻断能力，并具备面向跨层级重要业务终端提供统一准入支撑服务的能力。



图B.1 政务外网城域网终端控制部署示意图

各级政务外网建设运维管理单位在城域网边界建设基于零信任理念的终端控制设施，实现政务外网终端准入控制（包括身份认证、终端安全检查、资源访问控制）、终端安全隔离（包括网络隔离、会话隔离、数据隔离），同时对于敏感的业务数据访问，可采用沙箱技术实现政务外网终端数据隔离，防止终端数据泄露。

B.2 部署

由政务外网建设运维管理单位统一建设，包括零信任管理平台、零信任安全网关、零信任客户端三部分，其中零信任管理平台部署于政务外网数据中心，零信任安全网关原则部署于接入路由器（各单位可以依据网络自身情况可调整部署位置），零信任客户端部署于接入

政务外网局域网终端。另外零信任管理平台和零信任安全网关要求支持高可用部署，并要求支持IPv6。

其中零信任客户端作为承载政务外网局域网终端安全能力的组件，提供终端准入控制、终端安全隔离等能力，并应支持Windows、Linux以及主流的国产化操作系统。零信任安全网关负责对政务外网所有局域网用户终端进行认证，并实现数据加密传输、网络隔离和资源访问控制等功能。零信任管理平台主要负责终端准入、终端安全隔离、终端安全防护等策略集中制定和下发。

B.3 实现：

B.3.1 终端接入管控：各级政务部门用户终端发起访问政务外网业务应用的请求，由零信任安全网关推送重定向页面，用户下载安装零信任客户端并通过身份认证检查后，可以访问政务外网业务应用。

B.3.2 重点应用保护：各级政务部门将要发布的业务注册到零信任管理平台，各级政务外网建设运维管理单位审核授权后，零信任管理平台将授权策略下发到零信任安全网关执行。

B.3.3 数据隔离：终端通过沙箱访问政务外网业务，应具备网络隔离（沙箱内应用只能访问政务外网，不能访问互联网，沙箱外应用只能访问互联网或其他网络，不能访问政务外网），进程隔离（沙箱内外应用无法相互通信），文件加密与隔离（沙箱内所有文件写入应加密并保存至沙箱虚拟存储区），数据流转权限控制（应支持基于用户维度的数据流转权限管控，管控内容包括但不限于外发控制、剪切板控制、打印控制等）。

备注：对于“7.2 自行管控模式城域网边界控制技术要求”中的面向本级政务部门提供重要公共应用安全防护支撑服务可参照上述实施指南构建。

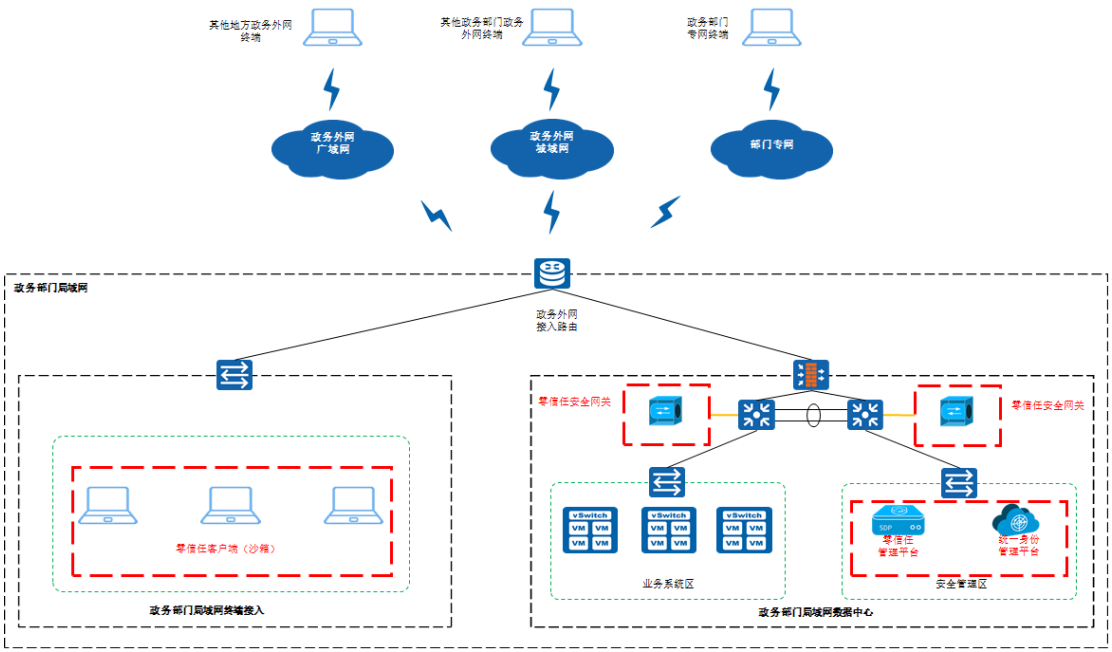
附 录 C
（资料性）
自行管控模式终端安全管控部署实施指南

C.1 概述

对于业务系统分散部署于各级政务部门局域网的场景，各级政务部门应按照局域网终端安全管控技术要求自行建设终端安全管控设施，对本单位的终端进行安全管理，并按“9.1自行管控模式”的要求与所在层级政务外网建设运维管理单位的终端检测及应用发布管理设施对接。

另外，对于业务系统已集中部署于城域网的政务部门，无需建设局域网终端安全管控设施，直接利用城域网建设的统一终端安全管控设施即可。

C.2 物理部署



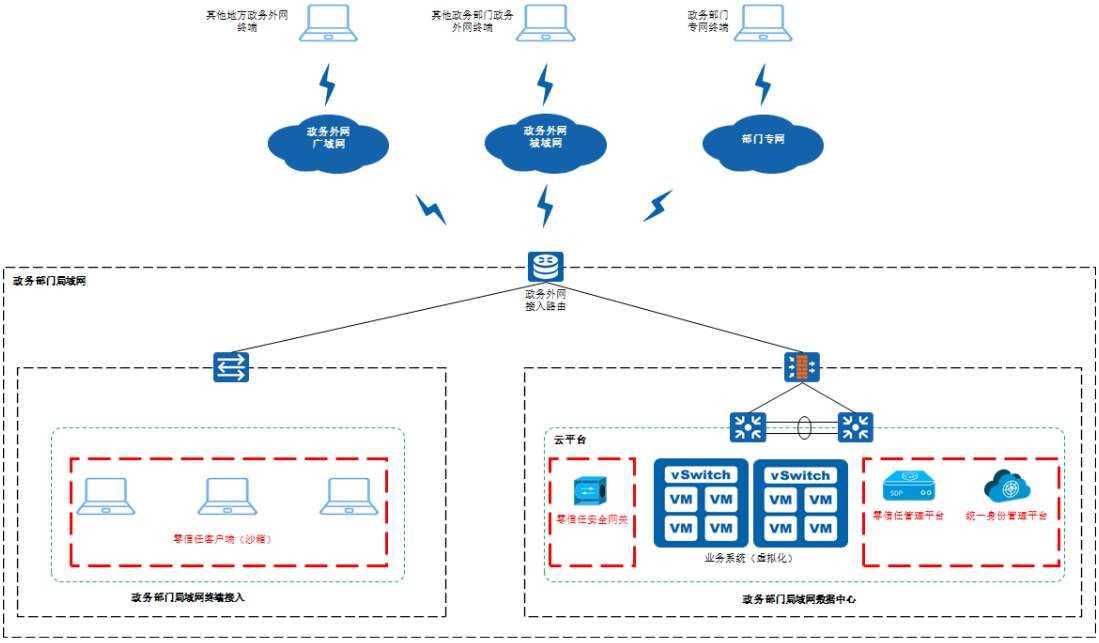
图C.1 物理部署示意图

部署：由各级政务部门自行负责建设，包括零信任管理平台、零信任安全网关、零信任客户端三部分，其中零信任安全管理平台部署于政务部门局域网数据中心，零信任安全网关部署于数据中心核心交换机，零信任客户端部署在需要访问政务部门业务的终端。与本部门统一身份管理平台对接，另外零信任管理平台和零信任安全网关要求支持高可用部署，并要求支持IPv6。

其中零信任客户端作为承载政务外网局域网终端安全能力的组件，提供终端准入控制、终端安全隔离、终端安全防护等能力，并应支持Windows、Linux以及主流的国产化操作系统。零信任安全网关负责对政务外网所有局域网用户终端进行认证，并实现数据加密传输、网络隔离和资源访问控制等功能。零信任管理平台主要负责终端准入、终端安全隔离、终端安全防护等策略集中制定和下发。

C.3 虚拟化部署

为便于实施，可在政务外网局域网数据中心以虚拟化方式部署零信任安全网关和零信任管理平台，来实现终端的准入、安全隔离和终端安全防护。



图C.2 虚拟化部署示意图

附 录 D
（资料性）
跨层级或跨部门终端安全管控设施实施指南

D.1 概述

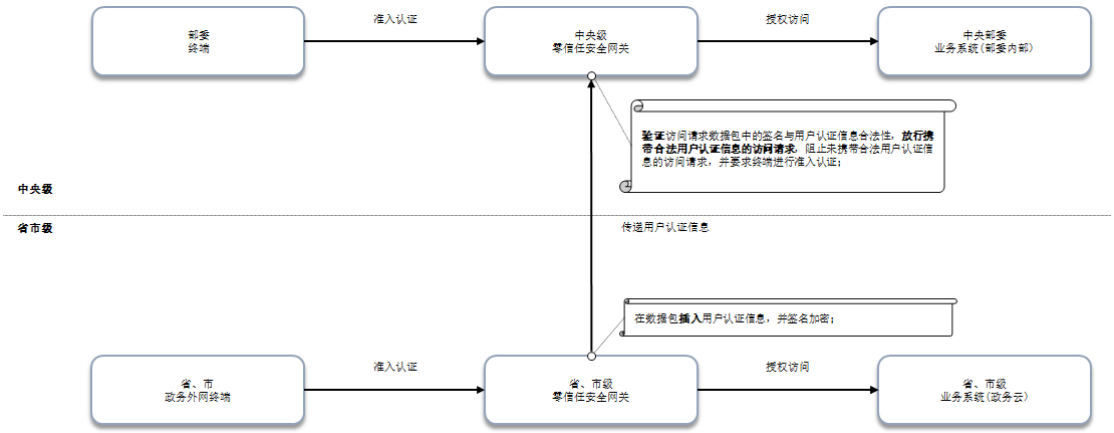
针对跨层级或跨部门终端访问业务场景，由于各级政务外网终端安全管控采用了分级建设、分层管理的模式，需要考虑不同部门、不同层级之间的终端管控设施的联动。

D.2 就近准入认证

原则上中央、省、市政务部门用户终端都应就近实现准入认证，可以由零信任管理平台完成认证，也可与各单位现有身份认证系统对接完成认证，认证通过的用户具有政务外网的访问权限。各单位应用访问权限由业务系统主管单位管理。

D.3 应用支撑联动管理

在跨层级或跨部门重要应用访问场景下，会存在同时经过多个零信任安全网关的情况，零信任安全网关之间通过标准接口实现认证信息传递，保证一个客户端、一次认证完成跨层级或跨部门重要应用访问。



图D.1 跨层级或跨部门终端安全管控级联模式

附 录 E
（资料性）
政务外网终端安全防护技术要求

E.1 概述

局域网终端安全防护应当在遵守等保等安全规范要求基础上，参照本附录要求执行，原则上应对终端进行恶意代码防范、终端入侵防护、非法外联控制、安全基线检查、漏洞检测修复、数据安全防护、终端软件管理、终端补丁管理、终端资产管理、终端精准阻断。

E.2 技术要求

E.2.1 恶意代码防范

接入政务外网的用户终端应安装病毒与恶意代码防护软件，并及时更新病毒与恶意代码库，本项要求包括：

a） 应至少支持对终端磁盘、终端内存、终端引导区、移动存储介质等位置进行病毒检测；
b） 应至少支持对文件感染型病毒、宏病毒、蠕虫、木马程序、间谍软件、脚本恶意程序、后门程序、僵尸程序、勒索软件等恶意代码进行检测；
c） 应对检测到的病毒进行处理，至少包括阻止、删除、隔离、清除还原；
d） 应及时更新病毒库。

E.2.2 终端入侵防护

a） 应对终端实施安全审计，审计内容包括终端基本信息、终端事件记录、终端变更记录等，审计记录至少保存 6 个月；
b） 应能发现钓鱼邮件攻击、劫持、暴力破解、端口扫描等终端入侵行为，并支持入侵行为溯源取证。

E.2.3 非法外联控制

a） 终端连接政务外网时，应能检测终端通过无线热点、双网卡、非法网关连接互联网的行为，并应对该行为进行告警和阻断。

E.2.4 安全基线检查

接入政务外网的终端应通过安全检查策略配置，识别与基线不符的配置项，并提供相应安全整改建议，本项要求包括：

a） 应支持对终端网络环境进行检查，并根据检查结果进行加固；
b） 应支持终端安全检查，如终端安全策略检查、软件安全检查、补丁安装检查、防病毒软件检查、默认共享检查等，并根据检查结果进行加固。

E.2.5 漏洞检测修复

应及时通过检测发现政务外网终端存在的漏洞，并提供修复建议，本项要求包括：

a） 应支持对操作系统等对象进行安全扫描，及时发现终端操作系统等存在的漏洞，并提供修复建议；
b） 应可识别终端操作系统开放的端口及服务，及时发现高危端口或服务存在的安全漏洞，并提供修复建议；
c） 应对终端存在的漏洞进行补丁修复。

E.2.6 数据安全防护

a） 应对支持对通过邮件、即时通信、网盘、移动存储介质等通道泄露数据的行为进行控制，防止政务敏感数据外泄；
b） 应支持业务数据通信访问加密保护，防止政务数据外泄，且支持国密算法；
c） 可对剪贴、截屏等数据外泄行为进行控制；
d） 可对用户拍照、录屏等行为发生的用户终端进行审计溯源；
e） 可支持文件追踪，一旦泄露可追踪溯源。

E.2.7 终端软件管理

应提供政务终端软件资产、软件分发、软件安装卸载、软件使用的管理能力，本项要求包括：

a） 政务外网终端应仅安装必须的组件和应用程序，并可通过黑白名单管控机制，避免恶意进程或恶意软件在政务外网终端上运行；
b） 应支持软件分发、卸载、升级管理，可支持手动、自动安装；
c） 应支持客户端自我保护，禁止停止、修改、删除客户端。

E.2.8 终端补丁管理

应对终端补丁进行统一管理，本项要求包括：

a） 应支持从官方途径获取补丁修复信息，整合生成补丁库；
b） 应支持自动、手动补丁导入，导入补丁原则不能直接与互联网连通；
c） 应支持补丁分发、补丁安装等补丁管理。

E.2.9 终端资产管理

a） 针对接入政务外网的用户终端，应发现、识别政务外网中终端软硬件资产，形成资产清单，至少包括终端硬件、终端操作系统、终端软件等；
b） 应支持对设备硬件信息变化情况进行监控并可预警；
c） 应对移动存储介质进行管理，可支持移动存储介质注册使用、外来移动存储介质禁用等。

E.2.10 终端精准阻断

a） 针对接入政务外网的终端应具备响应处置能力，能对失陷终端进行精准处置，包括查杀、阻断；
b） 对于 NAT 场景下，应能够基于会话进行精准阻断。

参 考 文 献

[1] GB/T 1.1-2020 标准化工作导则 第 1 部分：标准化文件的结构和起草规则
[2] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[3] 中华人民和国国务院令 第 745 号 关键信息基础设施安全保护条例
[4] GB/T 30278-2013 信息安全技术 政务计算机终端核心配置规范
[5] GW 0104-2014 国家电子政务外网安全等级保护实施指南