ICS 35.020
CCS L70

# 团　　体　　标　　准

T/DGAG 023—2024

# 电子政务外网单位接入网安全接入技术规范

Technical requirements for securing access of department access network with E-Government network

2024－03－28 发布　　2024－04－01 实施

广东省数字政务协会　　发 布

# 目　　次

# 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专利的责任。

本文件由广东省数字政务协会归口。

本文件起草单位：华南师范大学、数字广东网络建设有限公司、工业和信息化部电子第五研究所、国家计算机网络与信息安全管理中心广东分中心、深信服科技股份有限公司、深圳奥联信息安全技术有限公司、广东省信息安全测评中心、华为技术有限公司、深圳市联软科技股份有限公司、广州绿盟网络安全技术有限公司、深圳市智慧城市通信有限公司、广东中科实数科技有限公司、广州力麒智能科技有限公司、广州启睿信息科技有限公司。

本文件主要起草人：郑伟平、赵弘洋、陈伟洪、王宜阳、常晓宇、战鹏、龚征、赵淦森、王文佳、罗文晋、夏艺、谢英婷、洪伟杰、石炜君、陈嘉旺、李立、曾磊、林晓明、蔡先勇、邓思贤、薛佳瑞、郑召坤、黄其森、吕立民、丁丽萍、陈乜云、罗海飙、刘宁。

# 电子政务外网单位接入网安全接入技术规范

## 1 范围

本文件规定了广东省单位接入网接入电子政务外网的安全技术规范。

本文件适用于指导广东省各单位接入网按安全技术规范接入电子政务外网。单位接入网内的网络及其安全工作由各单位自行建设管理。

## 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。

GW 0015-2022 政务外网终端一机两用安全管控技术指南

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

下列术语和定义适用于本文件。

3.1

**电子政务外网 E-Government Network**

我国电子政务的重要基础设施，与互联网安全逻辑隔离，与政务内网物理隔离，满足各级政务部门经济调节、市场监管、社会管理和公共服务等方面需要的政务公用网络。

[来源：GDZW 0080.6-2023，3.1]

3.2

**城域网 Metropolitan Area Network**

用于实现本级行政区域内政务部门的横向连接，包括中央、省、市、县四级城域网。

[来源：GDZW 0080.6-2023，3.2]

3.3

**单位接入网 Department Access Network**

电子政务外网接入单位自行建设和管理的内部局域网络或业务专网。

[来源：GDZW 0080.6-2023，3.4]

3.4

**业务专网 Service Private Network**

由行业或业务主管部门自行建设管理满足其行业用户或组织内部网络通信需求、独立于电子政务外网运行的专用网络。

[来源：GDZW 0080.6-2023，3.7]

3.5

**终端 Terminal**

通过固定网络或移动通讯网络接入的输入输出设备。本规范内一般指单位接入网内办公人员日常办公或辅助办公所用的计算机终端、移动终端、物联终端，如台式计算机、笔记本电脑、智能手机或视频会议终端、摄像头、打印机、IP电话、门禁等。

3.6

**应用系统 Application System**

指为支撑特定业务需求，而提供某一系列功能的一个实例，一般包括应用软件、OS软件、服务器、数据存储等IT组件。

[来源：GDZW 0080.6-2023，3.6]

3.7

**网络平面 Network Plane**

基于基础承载网络，使用虚拟专用网络技术建设的虚拟网络。

[来源：GDZW 0080.6-2023，3.8]

注：广东省电子政务外网通过在统一的政务外网基础承载网络上，划分一类共用业务网络平面和多个专用业务网络平面。共用业务网络平面是由政务外网主管单位管理的虚拟网络，主要承载接入单位之间内部协同办公、数据共享等公共类业务（如公共业务网络平面），以及具有共性网络需求的应用（如视频业务网络平面、物联感知业务网络平面）；专用业务网络平面（如财政业务网络平面、医卫业务网络平面等）是经政务外网主管单位批准建设的，由业务主管单位（在某行业或专用领域有规模联网需求的机关单位）管理的虚拟网络，主要承载其行业或专用领域内的业务。[来源：GDZW 0080.5-2023，5.1]

3.8

**安全接入平台 Secure Access Platform**

利用互联网、移动互联网（如4G）、VPDN等基础网络，面向不具备专线接入条件的各级政务部门、企事业单位、移动办公人员、现场执法人员等，提供安全接入到政务外网网络或业务的服务平台。

[来源：GDZW 0080.3-2023，3.6]

3.9

**安全防护区 Security Protection Zone**

由多种安全设备和引流节点构成的安全功能区，主要为接入政务外网的应用系统、终端业务等流量提供安全防护服务，防范威胁横向扩散，实现政务外网安全加固。

[来源：GDZW 0080.3-2023，3.7]

## 4 缩略语

下列缩略语适用于本文件。

IP：网际互连协议（Internet Protocol）
IPv6：网际互连协议第6版（Internet Protocol Version 6）
VPDN：虚拟专有拨号网络（Virtual Private Dial Network）
IPS：入侵防御系统（Intrusion Prevention System）
DDOS：分布式拒绝服务攻击（Distributed Denial of Service）
ICP：网络内容服务商（Internet Content Provider）
IPSec：IP安全协议（Internet Protocol Security）
SSL：安全套接层（Secure Socket Layer）
VPN：虚拟专用网 （Virtual Private Network)
MAC：介质访问控制（Media Access Control）
NAT：网络地址转换（Network Address Translation）
AP：无线接入点（Access Point）
CPE：客户终端设备（Customer Premise Equipment）
PE：接入路由器（Provider Edge）
MCU：多点控制单元（Multipoint Control Unit）

## 5 电子政务外网单位接入网安全接入基础架构

### 5.1 网络接入模式

单位接入网接入电子政务外网的接入模式分为终端接入、系统接入和整网对接三种，接入单位应采用其中一种或多种接入模式接入电子政务外网：

a) 终端接入模式适用于单位接入网内仅有终端设备接入需求的场景；
b) 系统接入模式适用于单位接入网内仅有应用系统接入需求的场景；
c) 整网对接模式适用于非涉密业务专网与电子政务外网对接的场景。

三种单位接入网的安全接入模式场景示意如图1所示。

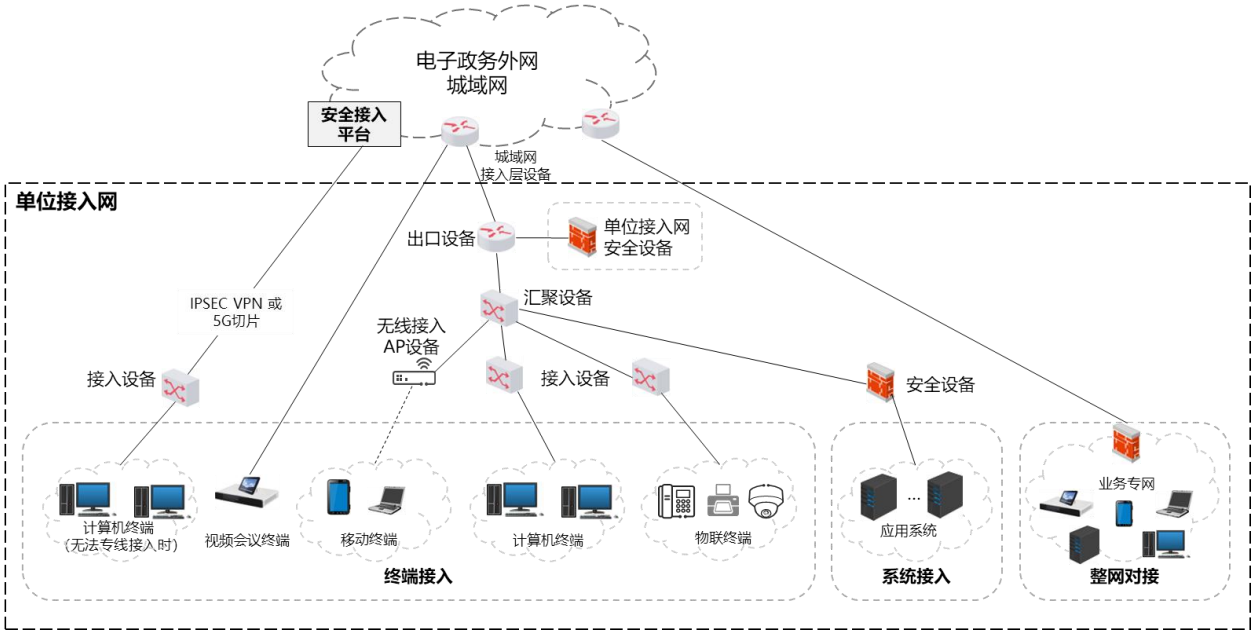


图 1　三种单位接入网安全接入模式示意

单位接入网接入电子政务外网的接入形式以专线接入为主。针对固定场所无专线资源的，可基于互联网通过政务外网安全接入平台，采用IPSEC VPN的方式安全接入政务外网；也可通过专用政务外网5G CPE设备，采用端到端5G切片方式安全接入政务外网。

终端直接接入政务外网安全接入平台，未经过接入单位网络设施承载的，不属于单位接入网范畴，如移动办公或者现场执法终端，通过移动互联网，采用SSL VPN安全隧道方式或VPDN方式接入政务外网安全接入平台，或物联终端通过5G方式接入政务外网。

## 5.2　网络安全架构

单位接入网内部安全防护由各接入单位保障。在电子政务外网城域网侧有安全防护区和安全接入平台，安全防护区为单位接入网提供访问权限控制和流量清洗防护等功能，实现政务外网的安全补盲和安全加固；安全接入平台利用互联网、移动互联网（如4G、5G）、VPDN等基础网络，面向不具备专线接入条件的单位或人员，提供安全接入到政务外网网络或业务的功能。单位接入网、安全防护区和安全接入平台及访问流量的逻辑关系如图2所示。

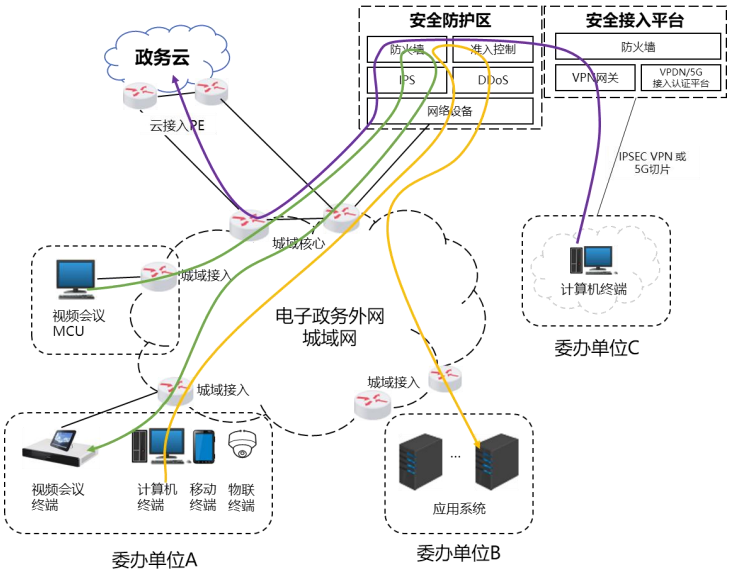


图 2　单位接入网接入电子政务外网网络安全架构示意

# 6 电子政务外网单位接入网安全接入要求

## 6.1 终端接入安全技术要求

### 6.1.1 总体要求

终端接入安全总体要求如下：

a) 各单位接入终端需明确接入终端范围及各终端的接入方式；
b) 各单位接入终端需通过身份认证技术要求，明确接入终端的合法身份；
c) 办公终端安全要求应包括准入控制、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、终端精准阻断等方面，具体应满足 GW 0015—2022 的要求；
d) 移动终端安全要求应包括软硬件环境安全、准入控制、隧道加密、数据安全防护等方面。移动终端访问政务外网敏感业务时，应采用沙箱技术，实现终端数据安全防护，具体应满足 GW 0015-2022 的要求；
e) 各单位接入终端接入多个网络时，应满足安全隔离要求，实现接入政务外网时与其他网络的隔离；
f) 接入终端访问政务外网敏感业务时，应采用沙箱及密码技术，确保敏感数据落入终端沙箱后加密存储，限制终端数据外发途径，防止终端数据的泄露；
g) 物联终端应通过网络准入认证后方可接入电子政务外网，应识别物联终端资产类型，主动发现私接、仿冒等终端异常接入电子政务外网的行为；
h) 对于终端用户的登录行为应留存日志，并标记为终端安全日志，便于快速审计定位。

### 6.1.2 身份认证

用户使用终端接入政务外网时，应使用身份鉴别的认证机制，确保非授权的终端与用户无法接入政务外网。终端与用户的身份认证应满足以下要求：

a) 接入政务外网的用户终端应实现用户与终端实名绑定，以便后续审计溯源；
b) 对于接入政务外网的移动智能终端、计算机终端应采用口令认证、基于密码技术的认证或硬件 MAC 地址认证等鉴别技术提供多因子统一身份认证功能；对于视频会议终端，应结合视频传输协议，采用硬件 MAC 地址、端口或目的地址等设备唯一性因素进行合法性鉴别；
c) 支持实时或定时对各类入网设备的设备类型、操作系统等进行识别，并及时发现入网设备仿冒行为；
d) 身份认证触发异常场景时，应完成基于用户生物特征识别或非对称密码技术的增强认证后方可登录。异常场景包括但不限于：账号首次登录、用户在某终端首次登录、空闲帐号登录、弱密码登录、非常规时间登录、非常用地点登录等；
e) 登录用户的身份鉴别信息应具有复杂度要求并定期更换。

### 6.1.3 安全检查

终端接入政务外网前，单位接入网内的安全检测设备应对终端进行安全检查，不符合要求的终端不允许接入政务外网。终端安全检查应包括但不限于以下内容：

a) 终端是否安装运行了防病毒软件；
b) 终端是否存在弱口令账户；
c) 终端是否运行了恶意进程或软件；
d) 终端是否开启系统防火墙；
e) 终端登录的时间和地点是否在规定范围内；
f) 终端网络行为和流量是否存在异常，禁止私接和异常访问行为。

### 6.1.4 传输加密

终端应采用国家核准的密码技术保证通信传输的安全，包括但不限于采用SSL或IPSec等密码技术手段，对终端通信数据进行加密传输，保证数据在传输过程中的安全性。

#### 6.1.5 权限控制

单位接入终端对政务外网的访问进行动态权限控制，应包括但不限于以下内容；

a) 根据终端接入方式、终端类型等不同接入形式，采用网络隔离、虚拟化等方式进行管控；
b) 按权限最小化原则严格控制访问资源，包括但不限于终端所能访问的网段或指定应用端口及协议；按近源策略控制原则防御终端风险，防止终端风险在接入网内部进行扩散；
c) 对接入终端进行持续的信任评估，结合终端类型、用户身份、安全状态、网络行为、访问时间、接入位置等信息动态调整信任评估值，并根据信任评估值对接入用户实现动态准入控制、动态授权管理等。

#### 6.1.6 安全隔离

终端接入电子政务外网时如需多网络访问，应对各网络访问进行安全隔离。隔离手段应满足：

a) 当终端同时访问互联网和政务外网时，应支持网络隔离，确保访问政务外网时，终端不能同时访问互联网，终端访问互联网时，不能同时访问政务外网；
b) 当终端访问政务外网敏感业务时，对终端数据进行安全隔离和加密存储，采用沙箱和密码技术，确保敏感数据落入终端沙箱后加密存储，限制终端数据外发途径，防止终端数据的泄露；
c) 二级单位独立建设接入网，通过一级单位接入网接入政务外网时，应在一级单位建立二级单位接入区，对访问流量进行策略控制、入侵检测和病毒检测。

#### 6.1.7 边界防护

电子政务外网城域网安全防护区应具备对终端访问的边界安全防护能力，包括但不限于：

a) 按权限最小化原则严格控制访问资源，控制粒度达端口级，能基于应用协议和应用内容对数据流实现访问控制；
b) 支持入侵防范安全策略部署，通过分析网络流量检测僵尸、木马、蠕虫等恶意威胁入侵，并通过入侵防御能力，实时地终止入侵行为；
c) 支持对病毒、蠕虫、僵尸网络等恶意流量的检测、分析、阻断和清除；支持对多层压缩文件查杀，支持基于文件散列值设置恶意文件或程序白名单。

### 6.2 系统接入安全技术要求

#### 6.2.1 总体要求

系统接入安全总体要求如下：

a) 各单位申请接入电子政务外网时，应明确本单位接入网的边界和范围，单位接入网内的应用系统应经登记备案后接入，后续若有调整，应向本级政务外网主管单位申请变更；
b) 各单位应根据 GW 0206-2014 的要求做好单位接入网内部的安全防护；
c) 各接入应用系统和网络设备等均应支持 IPv6 协议，宜部署双栈模式接入；不支持 IPv6 协议的，应逐步进行改造，改造详情可参照 GDZW 0034.3-2020 的要求执行；
d) 应用系统应使用政务外网 IP 地址接入，明细地址由接入单位在政务外网主管单位分配的 IP 地址段内进行二次分配；
e) 单位接入网内的应用系统若已使用私有 IP 地址且无法改造的，应采用一对一方式进行 NAT 地址转换；
f) 应用系统应分别汇聚后通过不同的物理端口或逻辑子接口与城域网接入层设备对接；
g) 单位接入网接入电子政务外网专用业务网络平面的，应遵循其网络平面管理单位制定的专用业务网络平面接入要求；
h) 接入的应用系统应具备运行情况监测、安全防护、行为审计和配置管理能力，小规模系统可采用设备自带的相关能力；
i) 应用系统在接入前应完成系统的等级保护测评、商密评估、ICP 备案（如需对外服务）等符合国家相关法律法规的工作；
j) 应用系统应在用户侧按需部署政务外网公共区、互联网区、专网区防火墙以实现接入。

### 6.2.2 身份认证

系统接入的身份认证应满足但不限于以下要求：

a) 单位接入网的政务外网接入网关应对接入应用系统的源及目的 IP 地址、业务端口、授权访问的资源等进行验证，并拒绝非授权的访问；
b) 单位接入网的政务外网接入网关应采用符合国家密码管理要求的密码技术（如数字证书、标识密码）对应用系统进行认证。

### 6.2.3 传输加密

单位接入网内应用系统和安全设备或汇聚设备之间，单位接入网的出口设备与城域网的接入设备之间应采用IPSec VPN 或SSL VPN进行传输加密防护，加密算法应符合国家密码管理政策的相关规范要求。

### 6.2.4 权限控制

系统接入的权限控制应满足但不限于以下要求：

a) 应用系统应按需申请政务外网访问权限并遵循最小需求原则，应用系统的设备变更、业务调整应先申请后实施；
b) 单位接入网的系统接入侧应部署防火墙，对相关访问权限进行配置校验，并对访问系统的流量进行入侵检测和病毒检测；
c) 单位接入网的系统设备接入应提供访问控制措施，包括但不限于根据设备的数字证书身份或标识密码身份设置接入设备的授权资源及访问权限，阻止非授权访问。

## 6.3 整网对接安全技术要求

### 6.3.1 基本原则

整网对接应结合已有业务专网实际情况和对接后网络访问需求，按照“一事一议”原则，根据国家电子政务外网顶层互联技术标准配置安全措施。总体应遵循以下原则：

a) 接入单位应明确业务专网内访问政务外网的终端和系统范围，并在与政务外网的边界处启用访问控制措施，按最小化原则严格控制访问资源，控制粒度应达端口级，宜基于应用协议和应用内容对数据流实施更细粒度的访问控制；
b) 业务专网内地址到政务外网地址若存在 NAT 地址转换，宜采用一对一方式转换；
c) 政务外网接入网关应采取技术措施，对业务专网出口设备进行识别和验证，确保出口设备不被仿冒；
d) 政务外网城域网安全防护区应对业务专网与政务外网之间流量进行访问控制和安全防护，应根据接入单位申请，按最小化原则严格控制访问，控制粒度应达端口级，宜基于应用协议和应用内容对数据流实施更细粒度的访问控制。

### 6.3.2 边界防护

整网对接时，需对接入边界进行安全防护，应满足但不限于以下要求：

a) 按权限最小化原则严格控制访问资源，控制粒度达端口级，能基于应用协议和应用内容对数据流实现访问控制；
b) 支持入侵防范安全策略部署，通过分析网络流量检测僵尸、木马、蠕虫等恶意威胁入侵，并通过入侵防御能力，实时地终止入侵行为；
c) 支持对病毒、蠕虫、僵尸网络等恶意流量的检测、分析、阻断和清除，支持对多层压缩文件查杀，支持基于散列值设置恶意文件或程序白名单。

## 6.4 管理与审计

### 6.4.1 日常运行管理

日常运行管理满足以下要求：

a) 接入单位具体负责本单位接入设备的维护、安全监测等管理工作；制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

b) 接入单位明确运行管理部门及其职责，配备专职管理员，制定日常维护管理制度，形成健全的日常运维机制，建立完善的应急响应预案，保障接入设备的安全运行；
c) 接入单位应定期对接入设备状态、网络流量、应用及系统运行状态等情况进行巡检，分析各类设备日志及管理审计报表，及时发现异常情况，并根据告警提示采取相应的处理措施；
d) 接入系统应符合网络安全等级保护测评标准或入网安全评估的测评标准，完成高、中危漏洞整改并提供安全评估报告后方可接入；
e) 接入单位应对安全管理人员进行严格的背景审查，并签订保密协议；制定安全培训计划，定期对安全管理人员进行安全培训和教育，并定期进行考核。

### 6.4.2 系统资产管理

系统资产管理满足以下要求：

a) 接入单位应建立接入系统资产安全管理制度，根据资产所属关系、安全级别和所处位置等信息建立资产清单，应根据资产的重要程度对各类资产进行标识管理；
b) 接入单位应动态维护系统资产清单，确保资产清单的完整性。

### 6.4.3 安全审计

安全审计满足以下要求：

a) 接入单位应对接入系统及其设备所产生的日志（包括运行、告警、操作、消息、状态等）进行存储、审计、分析，识别发现潜在安全事件与安全风险，并按照规定留存相关的网络日志不少于六个月；
b) 接入单位应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。

# 参 考 文 献

[1] GW 0202-2014 国家电子政务外网标准 国家电子政务外网安全接入平台技术规范
[2] GDZW 0034.3-2020 广东省电子政务外网IPv6改造指南 第3部分：城域接入网
[3] GDZW 0080.3-2023 广东省数字政府电子政务外网建设指南 第3部分：城域网
[4] GDZW 0080.6-2023 广东省数字政府电子政务外网建设指南 第6部分：单位接入网接入规范