国家电子政务外网标准

GW0206—2014

接入政务外网的局域网安全技术规范

Security Technology Specification of

Local Area Networking Connecting to CEGN

2014－11－13 发布　　2015－1－1 实施

国家电子政务外网管理中心

目　　次

前　言

为指导各级政务部门局域网通过专线接入到国家电子政务外网（以下简称“政务外网”），并在各单位局域网接入后保障政务外网及所承载的政务业务安全，根据我国有关法律、法规和技术规范，结合政务外网实际应用需求及建设经验编制本规范。

局域网自身安全防护建设由各单位按照信息安全等级保护相关要求和标准执行。

本规范由国家电子政务外网管理中心提出并归口。

本规范主要起草单位：国家电子政务外网管理中心、北京天融信科技有限公司、北京星网锐捷网络技术有限公司、杭州迪普科技有限公司、深信服网络科技有限公司、北京艾科网信科技有限公司、北京国联天成信息技术有限公司。

本规范主要起草人：罗海宁、吕品、周民、邵国安、张锐卿、路剑华、徐涛、弓睿智、闫春保、梁鹏、韩帅、赵迪。

引　言

各级政务部门局域网在接入政务外网后，局域网终端既可访问互联网，又可访问政务外网相关业务系统。由于各单位局域网建设和管理均由各单位自行负责，信息安全等级保护和运维保障情况各不相同，为保障政务外网相关业务连续性和整体安全性，本规范提出了局域网总体、接入政务外网边界和局域网终端接入等安全技术要求。

接入政务外网的局域网安全技术规范

1 范围

本规范适用于指导各级政务外网建设、运维和管理单位对专线接入政务外网的局域网提出具体安全要求，也可为各级政务部门局域网接入政务外网前的安全自查、整改提供参考。

2 规范性引用文件

下列文件条款通过本指南引用而成为本指南条款。凡是注明日期引用文件，其后所有修改版（不包括勘误内容）或修订版均不适用于本指南。凡是不注明日期引用文件，其最新版本适用于本指南。

GB/T 5271.8-2001 信息技术 词汇 第8部分：安全

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 30278-2013 信息安全技术 政务计算机终端核心配置规范

《国家电子政务外网IPSec VPN安全接入技术要求与实施指南》（政务外网[2011]11号）

《国家电子政务外网安全等级保护基本要求》（政务外网[2011]15号）

《国家电子政务外网安全等级保护实施指南》（政务外网[2014]1号）

3 术语和定义

GB/T 5271.8-2001确定的以及下列术语和定义适用于本规范。

3.1

DMZ

Demilitarized Zone（非军事区）的简称，它是一个对外提供网络服务的网络区域，一般设置在内部网络和外部网络之间，受防火墙等访问控制措施保护，通过防火墙与内部网络、外部网络隔离，执行与内部网络不同的安全策略，也有的称之为对外服务区。

3.2

AP

Access Point（接入点）的简称，它作为有线网络向外延伸的接口之一，通过Wi-Fi方式可将各类无线终端接入到有线网络。

3.3

移动智能终端

具有独立操作系统、用户自安装软件并可通过移动通讯网络来实现无线网络接入的终端，本规范中特指政务部门内部办公人员在移动办公环境下所使用的智能手机和平板电脑。

3.4

国家电子政务外网安全接入平台

利用Internet、移动通信网络（2G、3G、4G等）、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、现场执法人员和公众用户，提供安全接入到政务外网网络

或业务的服务平台。

4 总体安全要求

a) 局域网内部安全由接入单位按照信息安全等级保护相关标准进行安全防护；
b) 局域网应根据业务需求划分安全域，进行区域隔离；
c) 局域网在接入政务外网时，边界安全应符合以下要求：
   1) 局域网接入政务外网时，应根据不同业务安全需求，进行边界安全防护；
   2) 对原有的互联网出口进行安全防护；
   3) 局域网与其他专有网络出口边界安全防护应遵循专网的安全要求。
d) 局域网终端安全应符合以下要求：
   1) 终端跨网访问时，应采取必要安全隔离与控制措施；
   2) 对计算机终端接入进行安全防护与准入控制；
   3) 对移动智能终端接入进行安全防护与准入控制。
e) 局域网内对外提供服务节点应进行安全防护。

5 局域网安全等级保护要求

接入政务外网的局域网应依据信息安全等级保护的要求进行建设。

6 局域网安全域划分与隔离防护

接入单位可将局域网逻辑划分为内部业务区、终端接入区、AP 接入区、安全管理区以及不同 DMZ 区等安全域（如图 1 所示），局域网的外部边界主要有政务外网提供的公用网络区接入、互联网接入区接入、专用网络区接入三个边界以及原有互联网出口边界、AP 接入区接入边界等，各区域边界处通过划分虚拟局域网 VLAN、设置路由策略与交换机访问控制列表、部署防火墙等措施实施不同强度的逻辑隔离防护。

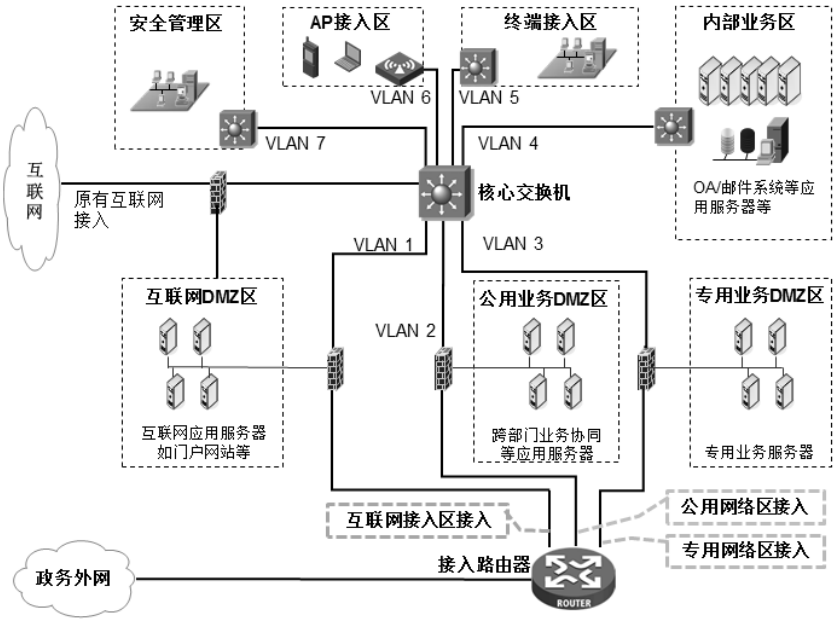

图 1 局域网逻辑示意图

7　边界安全要求

7.1　接入政务外网边界安全要求

7.1.1　公用网络区接入边界安全要求

公用网络区边界为接入单位局域网与本级政务外网城域网的接入边界，接入单位局域网应通过防火墙系统、入侵防御系统和安全审计系统等与政务外网进行逻辑隔离并对局域网进行安全防护。

本项要求包括：

a)　访问控制

1)　根据会话状态信息为数据流提供明确的允许/拒绝访问能力，控制粒度至少达到端口级；

2)　应对用户设置有限权限访问政务外网资源，并限制政务外网地址访问局域网；

3)　对外提供服务节点时，应设置公用网络业务DMZ区，对该区单独实施安全策略，允许公用网络区访问内部业务区，禁止内部业务区服务器向外访问。

b)　入侵防范

1)　进行病毒过滤和入侵防御，并及时升级病毒和攻击特征库；

2)　对病毒和入侵攻击行为进行实时告警及阻断。

c)　安全审计

1)　记录攻击源IP、攻击类型、攻击目的IP、攻击时间等关键信息；

2)　记录公用网络访问行为、网络地址转换日志等信息；

3)　审计信息应至少保存6个月。

7.1.2　互联网接入区接入边界安全要求

利用政务外网互联网接入区接入的单位，应单独设置防火墙系统、入侵防御系统、安全审计系统等进行安全防护。接入单位部署IPSec VPN、SSL VPN等安全接入设备时，应符合《国家电子政务外网IPSec VPN安全接入技术要求与实施指南》和《国家电子政务外网安全接入平台技术规范》要求。

本项要求包括：

a)　访问控制

1)　根据会话状态信息为数据流提供明确的允许或拒绝访问能力，控制粒度至少达到端口级；

2)　能够对互联网流量和最大连接数进行控制，控制粒度为终端用户级；

3)　应对用户访问互联网进行流量控制和管理；

4)　对外提供服务节点时，应设置互联网DMZ区，对该区单独实施安全策略，允许互联网访问互联网DMZ区服务器，禁止互联网DMZ区服务器向外访问。

b)　入侵防范

1)　应对攻击行为进行实时告警；

2)　应针对端口扫描、强力攻击、木马后门攻击、缓冲区溢出攻击、IP碎片和网络蠕虫等攻击行为进行阻断；

3)　应提供针对文件型、混合型病毒过滤功能，并及时更新病毒特征库。

c)　安全审计

1)　记录攻击源IP、攻击类型、攻击目的IP、攻击时间等关键信息；

2)　记录互联网访问行为、网络地址转换NAT日志等信息；

3)　审计信息应至少保存6个月。

7.1.3　专用网络区接入边界安全要求

专用网络区边界安全由接入单位按照该专用网络区的纵向业务主管单位要求进行防护。访问控制、入侵防范和安全审计等要求可参照公用网络区接入边界安全要求。

7.2 原有互联网出口边界安全要求

接入单位可参照国家标准《信息安全技术 政府部门互联网安全接入要求》实施边界保护。利用原有互联网出口部署IPSec VPN、SSL VPN等安全接入设备时，应参照《国家电子政务外网IPSec VPN安全接入技术要求与实施指南》和《国家电子政务外网安全接入平台技术规范》要求。

本项要求包括：

a) 访问控制
   1) 应设置策略防止利用原有互联网出口在局域网内设置代理或桥接方式访问政务外网内各业务区；
   2) 对外提供服务节点应设置在互联网业务DMZ区，对该区单独实施安全策略，允许互联网访问互联网DMZ区服务器，禁止互联网DMZ区服务器向外访问。
b) 入侵防范、安全审计等其他要求可参照互联网接入区接入边界安全要求。

7.3 AP 接入区接入边界安全要求

a) 划分独立虚拟局域网 VLAN 对 AP 接入区单独管理，该区域与局域网内其他区域逻辑隔离；
b) AP 接入区的终端设备仅能直接访问互联网，访问政务外网或局域网内其他区域必须通过国家电子政务外网安全接入平台，安全接入平台具体要求参照《国家电子政务外网安全接入平台技术规范》；
c) 终端设备未经允许不能接入局域网的 AP 接入区；
d) 启用“WPA 企业/WPA2 企业”加密方式、关闭 SSID 广播功能；
e) IP 地址由统一 DHCP 服务器分配或使用本单位统一规划的静态 IP，并采取准入控制措施。

7.4 其他网络边界安全要求

局域网与其他专网边界安全防护应符合该专网的安全要求，也可参照专用网络区接入边界安全要求。

8 接入终端安全要求

8.1 计算机终端

a) 身份鉴别
   1) 接入局域网终端必须进行注册，注册信息至少要包括 MAC 地址、使用者信息和终端配置信息；
   2) 使用 CA 证书认证时，应与用户实名绑定；
   3) 口令至少由 8 位字符组成，包含字母、数字和特殊字符等两种以上类型，至少每 6 个月修改一次，连续 6 次内口令不重复。
b) 准入控制
   1) 终端应通过接入单位安全准入检查；
   2) 接入设备应进行 IP、MAC 和端口绑定；
   3) 可采用数字证书、虚拟化、沙盒和主机防火墙等技术，实现终端访问互联网与访问政务外网公用网络区及专用网络区业务的安全隔离。
c) 安全防护
   1) 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特征库；
   2) 及时对终端系统漏洞进行修补；
   3) 不允许终端开启代理服务、无线热点等功能；
   4) 及时告警并阻断局域网内终端非法外联；
   5) 终端配置要求参见国家标准 GB/T30278-2013《信息安全技术 政务计算机终端核心配置规范》。

d) 安全审计

1) 对用户操作行为和终端系统日志进行审计；

2) 审计记录应提供统计、查询和分析功能，并至少保存 6 个月。

e) 远程接入

终端利用互联网远程接入到政务外网或本局域网内时应符合《国家电子政务外网 IPSec VPN 安全接入技术要求与实施指南》和《国家电子政务外网安全接入平台技术规范》要求。

8.2 移动智能终端

a) 软硬件安全

1) 移动智能终端硬件应取得国家入网许可；

2) 具备病毒防护和系统漏洞扫描功能；

3) 具备身份认证与签名验签功能；

4) 具备用户数据隔离、加密存储、数据备份和授权远程清除等功能；

5) 提供安全策略统一配置工具或软硬件后台管理功能。

b) 接入控制

1) 对移动智能终端用户、电话号码、IMSI（国际移动用户识别码）、IMEI（国际移动设备识别码）、设备序列号、设备型号和系统版本等信息进行统一登记注册；

2) 对接入终端进行实名制认证，并核查 IMSI（国际移动用户识别码）和 IMEI（国际移动设备识别码）；

3) 应采取远程拨号安全措施通过国家电子政务外网安全接入平台接入政务外网或局域网。

c) 安全防护

1) 安装防火墙、防病毒和入侵防御等安全软件；

2) 采取加密算法时应符合国家密码管理局制定的相关规范要求；

3) 应提供登录失败处理功能，可限制非法登录次数或锁定移动智能终端软硬件；

4) 移动智能终端遗失后在用户授权下可远程清除应用数据及配置信息；

5) 访问不宜在互联网公开的信息时应关闭互联网连接；

6) 应关闭移动智能终端无线热点分享和 USB 网络分享功能。

d) 安全审计

1) 对移动智能终端接入行为进行日志记录；

2) 审计记录应提供统计、查询和分析功能，并至少保存 6 个月。