**3.1货物清单（中标设备须为国产品牌）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 技术需求 | 数量 | 推荐品牌 |
| 1 | CE路由器 | 详见3.2主要技术参数规范需求表 | 1 | 华为、华三、瞻博 |
| 2 | 安全网关 | 详见3.2主要技术参数规范需求表 | 1 | 奇安信、华三、瞻博 |
| 3 | 核心交换机 | 详见3.2主要技术参数规范需求表 | 1 | 华为、华三、瞻博 |

**3.2主要技术参数规范需求表**

###### 1、CE路由器

|  |  |
| --- | --- |
| **功能类别** | **技术要求及指标** |
| ★**包转发率** | 包转发率≥200Mpps，提供官网截图 |
| ★**架构** | 控制转发物理分离 |
| **★配置** | 双主控，双电源，10GE Combo接口 |
| **★槽位数** | 槽位数≥6 |
| **★电源** | 支持电源数量≥4，本次实配两个电源 |
| **板卡种类** | 支持通道化E1、非通道化E1、异步串口、同异步串口、3/4G全制式扩展板卡等广域网接口扩展 |
| **电源** | 支持（1+1）冗余内置模块化电源 |
| **★虚拟化** | 支持虚拟化特性，将物理上两台设备虚拟化成一台逻辑设备，权威第三方机构的测试报告 |
| **★广域网优化** | 支持对HTTP/FTP等TCP业务流量进行优化传输技术，提高广域网带宽利用率，权威第三方机构的测试报告 |
| **★URL过滤黑名单功能** | 支持对终端用户域名访问控制功能，权威第三方机构的测试报告 |
| **★支持openflow功能** | 支持openflow功能，权威第三方机构的测试报告 |
| **★基于域的防火墙** | 支持划分安全域，用于管理防火墙设备上安全需求相同的多个接口，权威第三方机构的测试报告 |
| **★IPS入侵防御功能** | 支持对已知网络攻击进行安全防御，提高网络安全性，权威第三方机构的测试报告 |
| **★ADVPN功能** | 通过动态VPN技术，实现动态获取对端分支节点当前的公网地址，从而实现两个节点之间动态建立跨越IP核心网络的ADVPN隧道简化VPN网络部署复杂度和提高管理效率，权威第三方机构的测试报告 |
| **★GDVPN功能** | 支持密钥和IPSEC安全策略集中管理，基于IPSEC安全模型，属于同一组的所有成员共享相同的策略及密钥，权威第三方机构的测试报告 |
| **VXLAN功能** | 支持VXLAN数据中心特性，并提供支持此特性权威第三方机构的测试报告 |
| **短信开局** | 支持利用短信下发的方式实现设备开局部署，并提供支持此功能的权威第三方机构的测试报告 |
| **U盘0配置部署** | 支持利用U盘0配置方式实现设备开局部署，并提供支持此功能的权威第三方机构的测试报告 |
| **★嵌入式自动化** | 支持对系统软硬部件的内部事件、状态进行监控，出现特定事件后能够自动调整网络设备业务和控制策略，实现智能自动化控制  支持对系统软硬件的内部事件、状态进行监控，出现问题时收集实时信息并自动修复将实时信息发送到指定服务器  要求支持此功能，权威第三方机构的测试报告 |

###### 2、安全网关

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| **系统架构** | 系统要求为下一代防火墙产品，原厂商要求参与第二代防火墙标准GA/T1177-2014《信息安全技术 第二代防火墙安全技术要求》标准编制，投标时要求提供相关证明复印件 |
| 系统采用多核处理架构，硬件设计采用高性能一体化智能安全处理引擎，要求提供计算机软件著作权登记证书。 |
| ▲**硬件要求** | 性能：三层吞吐量≥8G，应用层吞吐量≥2G ，并发连接数≥200万，新建连接数≥12万，支持IPV6，带防火墙、IPS、行为管理、僵尸网络检测、实时漏洞分析、WAF、防病毒等功能模块；  接口：≥4个千兆电口，≥4个千兆光口；  服务：原厂三年质保服务。 |
| **部署模式** | 支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式； |
| **网络协议** | 支持支持3G/4G接入，并可实现3G/4G连接与有线链路之间的互为备份**（需要提供能够体现上述功能的截图，并加盖原厂公章）**；  支持MPLS流量透传；支持针对MPLS流量的安全审查，包括入侵防护、反病毒、URL过滤、基于终端状态访问控制功能**（需要提供能够体现上述功能及配置选项的截图，并加盖原厂公章）** |
| **路由协议** | 支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；**（需要提供能够体现上述功能及配置选项的截图，并加盖原厂公章）** |
| 支持基于策略的路由负载，支持根据应用和服务进行智能选路，不少于12种路由负载均衡方式  支持ISP路由负载均衡，支持自定义负载权重，支持基于优先级的ISP路由链路备份  支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试 |
| **高可靠性** | 支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA高可靠性部署支持接口联动，某个端口失效（DOWN），属于同一接口组中其他端口都会进入失效状态（DOWN）；HA高可靠性部署支持配置接口权重；支持链路探测 |
| **访问控制** | 支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查 |
| **应用识别与控制** | 支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，支持配置基于IP、用户、应用的流量管理规则，可深度识别每种应用的属性，  为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类 |
| **病毒防护** | 能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀  支持对最多6级的压缩文件进行解压查杀  支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀 |
| **入侵防御** | 支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的漏洞防护 |
| 支持漏洞防护特征库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息；（投标文件需要提供设备包含上述所有高危漏洞攻击的特征及对应详细信息的截图） |
| 支持间谍软件防护功能，同时将间谍软件特征库分类，至少包括木马后门、病毒蠕虫、僵尸网络等三种分类;支持在防火墙间谍软件签名库直接查阅攻击的名称、严重性、描述等信息；间谍软件防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的间谍软件防护 |
| **VPN功能** | 支持支持IPSec VPN功能，支持基于主模式（Main Mode）、积极模式（Aggressive Mode）、国密三种协商模式建立的网关-网关加密隧道；支持本地CA并可为参与IPSec VPN隧道建立的设备颁发用于身份认证的证书 |
| 支持支持GRE隧道，支持GRE over IPSec VPN  支持L2TP、支持L2TP over IPSec、支持PPTP ，并支持本地认证以及LDAP/Radius/证书/Active Directory/TACACS+/POP3等第三方用户认证系统。支持客户端地址分配 |
| 支持SSL VPN，支持使用SSL VPN客户端与防火墙建立SSL VPN加密隧道，支持对远程用户进行口令认证或证书认证，或证书认证+口令认证双因素；口令认证支持本地认证以及LDAP/Radius/证书/Active Directory/TACACS+/POP3等第三方用户认证系统；支持USB-key证书；支持本地CA并可为SSL VPN客户端颁发用于身份认证的证书 |
| **▲网络异常感知** | 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断 |
| 支持基于主机或威胁情报视图，统计网络中存在安全风险的主机数量以及对应的风险等级，至少可查看遭遇风险的时间、威胁类别、情报来源、威胁简介、失陷主机IP、用户名、资产等信息**（提供截图）** |
| 支持与威胁感知设备协同，实现主机状态检测及告警； **（需提供包含云端配置的威胁感知设备的截图并加盖原厂公章）** |
| 支持统计网络内威胁事件的数量及对应的风险等级；支持一键跳转查看详情并自动显示关联日志；可基于网络连接、应用名称、威胁事件处置威胁事件；**（需提供能够体现以上功能的截图，并加盖原厂公章）** |
| 支持用户自定义重点URL分类和应用，并可基于定义的重点关注对象进行用户维度关联，并结合分析中心进行基于关联的用户/地址、URL分类、应用进行二次递进式深度分析，挖掘异常用户及异常网络行为。 |
| **安全事件分析** | 提供关联分析面板，可将Top应用、Top威胁、Top URL分类、Top源地址、Top目的地址等信息关联，并支持以任意元素于为过滤条件且不少于35个维度进行数据钻取 |
| 支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为 |
| 提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL过滤、文件过滤等安全模块检查的日志集中显示，**(提供截图)** |
| **策略与处置** | 可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项。 |
| 支持基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括1天、7天、30天、90天、永久等；**(提供截图)** |
| 支持接收针对突发重大安全事件的“应急响应消息”，并至少在界面显示安全事件名称、类型、当前防护状态、处置状态以及相应的操作等信息；并可根据设备安全配置的变化动态显示应急响应的处理结果  支持持针对“应急响应消息”的手动或自动处置，处置方法至少包括基于漏洞的处置和基于威胁情报的处置（**提供截图**） |
| **运维管理** | 支持双系统备份，三权分立管理（**提供截图**） |
| 支持加密的WebUI和CLI管理，且支持网页命令行管理（WebUI中内嵌CLI管理界面）(**提供截图)** |
| ▲具有独立审计用户，支持标准Syslog日志审计方式，支持Syslog端口自定义（支持内外端机主机名更改，强化日志审计及集中管理功能，能够对功能访问模块拒绝访问进行日志记录，支持对日志的高性能处理和存储，提供高性能Syslog日志处理和存储证书。 |
| **▲云端协同** | 支持与云端联动，至少实现病毒云查杀、URL云识别、应用云识别、云沙箱、威胁情报云检测等功能**（提供截图）** |
| **▲安全联动** | 支持通过统一管理系统进行统一策略配置，策略下发，支持日志的统一管理，并进行分析。 |
| 支持与网络威胁感知系统联动，将本地终端产生的异常行为、攻击活动等数据上报至网络威胁感知系统，网络威胁感知系统可实时监控网络内的攻击事件并预警可疑的受感染主机，同时支持接收来自网络威胁感知系统推送的情报信息。 |
| 所投产品需支持与现网中终端威胁防御系统联动，实现基于终端健康状态的访问控制；从而增强防火墙对木马特征的识别能力（投标文件需要提供能够体现上述功能及配置选项的截图）； |
| **市场成熟度** | 考虑产品主流性、成熟度，要求提供CCID赛迪顾问出具的2014、2015和2016年防火墙市场连续三年排名前3名的证明文件复印件 |
| **产品资质（复印件）** | 计算机信息系统安全专用产品销售许可证； |
| 中国国家信息安全认证产品型号证书； |
| 涉密信息系统产品检测证书； |
| 电信进网许可证 |
| 高性能IPv6防火墙系统计算机软件著作权登记证书； |
| 国家信息安全测评信息技术产品安全测评证书（EAL4+级）； |
| **厂商资质（复印件）** | ISO20000信息技术服务管理体系认证证书 |
| 具备中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》 |
| 国测信息安全服务资质（安全开发类）（一级） |
| 设备制造商要求为“信息安全等级保护关键技术国家工程实验室”理事单位 |
| 设备厂商是CNNVD技术支撑单位(一级) |
| **服务** | 签订合同时提供三年原厂商质保服务承诺函及授权书。 |

###### 3、核心交换机

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| **★业务插槽数** | 业务插槽数≥3 |
| **★交换容量** | ≥19Tbps，提供官网链接及截图证明，当存在双指标时以较小值为准（例如：10Tbps/30Tbps，以10Tbps为准） |
| **★转发能力** | ≥2880Mpps，提供官网链接及截图证明，当存在双指标时以较小值为准（例如：1000Mpps/3000Mpps，以1000Mpps为准） |
| **主控引擎** | 支持主控引擎模块≥2，满足1+1冗余  主控引擎支持固化千兆光业务口≥24个（24光+4万兆主控）  主控引擎支持固化千兆电业务口≥24个（24电+4万兆主控）  提供证明资料加盖原厂章 |
| **电源冗余** | 电源模块冗余 |
| **关键部件热插拔** | 主控交换卡、电源、接口模块、风扇、网板等关键部件可热插拔 |
| **★接口要求** | 以太网支持千兆电口，千兆光口，10GE端口、40G端口、100G端口 |
| 单槽位线速万兆端口密度≥16 |
| 单槽位线速40G端口密度≥4 |
| 单槽位12端口40G，或4端口100G，且支持端口零丢包切换，提供权威第三方测试报告加盖原厂章 |
| 单槽位24端口万兆/5G/2.5G/1G自适应端口 |
| 单槽位100G端口密度≥2，提供官网链接证明 |
| 单槽位能够同时提供千兆光口、千兆电口、万兆光口，且实际可用端口总数≥48，提高槽位利用率和业务可靠性，提供商用板卡公开手册的官网链接证明（24电+20光+4万兆） |
| 支持FCoE接口 |
| 支持EPON OLT及10G EPON OLT接口，提供权威第三方测试报告加盖原厂章 |
| 支持RPR，提供权威第三方测试报告加盖原厂章 |
| 支持POE+，满足新一代园区网以太网供电需求，提供工信部权威第三方测试报告，提供官网配置手册截图和链接 |
| **★虚拟化** | 多虚一技术(N:1)，支持4框虚拟化技术，提供证明资料 |
| 一虚多技术（1:N） |
| 支持多虚一技术和一虚多技术的配合使用 |
| 支持远程端口扩展，作为控制设备（Controlling Bridge,CB）实现对端口扩展模块（Port Extender,PE）的集中控制  支持和配套的端口扩展模块虚拟成单一的逻辑设备，在管理层面实现单一节点管理；虚拟化能力≥30：1，即通过单一管理节点可实现超过30台物理设备的统一管理。  整机支持的最大PE设备台数≥30 |
| **网络安全一体化** | 支持安全业务插卡FW、IPS、NSM、ACG、LB、SSL VPN |
| **★可视化** | 支持Telemetry流量可视化功能，提供权威第三方测试报告加盖原厂章 |
| **★有线无线一体化** | 支持AC板卡，POE，POE+ |
| 支持交换机内置AC功能**，**提供权威第三方测试报告加盖原厂章，支持原生的无线AC功能，无需独立的AC板卡或带AC功能的接口板，即支持无线AP管理功能。 |
| 支持有线无线一体化的终端准入认证 |
| **★网管功能一体化** | 内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级，提供权威第三方测试报告加盖原厂章 |
| **FCoE** | 支持FCF模式转发，VSAN的创建及配置，支持FC地址的分配及WWN地址和FC地址的绑定等功能，提供权威第三方测试报告加盖原厂章 |
| **SDN/OPENFLOW** | 支持OPENFLOW 1.3  支持普通模式和Openflow 模式切换  支持多控制器（EQUAL模式、主备模式）  支持多表流水线  支持Group table  支持Meter |
| **跨三层互联技术** | 支持主流的MAC in IP技术，如EVI/EVN/OTV等，实现跨三层网络的二层互联，提供权威第三方测试报告加盖原厂章 |
| **VxLAN** | 支持VxLAN 网关，提供工信部权威第三方测试报告，提供官网配置手册截图和链接 |
| **★安全特性** | 支持IPv4 uRPF |
| 支持DHCP Snooping |
| 支持ARP防攻击 |
| 支持端口隔离 |
| 支持IP+MAC+VLAN+PORT的绑定 |
| 支持报文过滤功能，黑洞路由、黑洞MAC |
| 支持IEEE 802.1ae介质访问控制安全技术，提供权威第三方测试报告加盖原厂章 |
| **成熟度** | 提供工信部入网证 |
| **资质** | 为响应国家低碳的要求，产品厂商在产品设计、研发、生产、过程需采取有效减少温室气体排放措施，符合国家温室气体排放和清除的量化和报告的规范。产品生产厂商需通过ISO 14064温室气体核查，提供证书复印件加盖原厂章  ★投标产品原厂商需具备科学、系统的知识产权管理体系。能够全面保护、并系统管理知识产权，支撑企业的技术创新能力，提供证书复印件 |
| ★**配置要求** | 本次配置单引擎，双电源，千兆电口≥48，千兆光口≥24，万兆光口≥4 |

###### 4、专网整合实施

网络拓朴设计

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| **具体设计** | 新增加CE路由器用于上连政府侧的MCE路由器，下连防火墙再与新增的核心交换机（替换原办公外网核心交换机）相联，新增安全网关部署在政务网和专网之间，将两网安全打通，新增准入系统部署在环保侧的VPN2区域级联政府侧的准入设备加强入网安全，取消原连接省生态环境厅与各县（市）分局、监测站的路由器和线路。新增设备部署在金华环保大楼三楼机房。 |
| **信息安全** | 专网的合理设计是保障环保监控正常运行的关键内容核心，专网的合理设计是重中之重，需要专业的运维公司进行保障，需要服务公司具备通信网络代维（外包）企业资质（通信线路），需同时具备安全生产许可证和安全技术防范证书，具有通信信息网络系统集成资质（乙级），通信信息网络系统集成资质（甲级） |
| **设备说明** | 政府侧MCE路由器（多角色用户边缘设备），环保侧CE（用户边缘设备）设备功能，环保侧安全网关设备，环保侧三层交换机设备 |
| **网络安全和运行巡检** | 网络安全进行不少于每月一次巡检，巡检后提供巡检报告以及问题整改措施≥2年 |
| **网络安全和运行优化** | 进行不少于每二个月一次网络安全优化评估服务、评估后提供巡检报告以及优化建议及优化方案，征询同意后实施优化调整。 |
| **电话支持服务** | 1）提供7\*24小时不间断提供服务的400服务电话 |
| 2）除电话外的方式：如：e-mail、VPN、QQ、微信 |
| **故障响应** | 1）故障申告后响应时间：10分钟内 |
| 2）故障申告后远程支持响应时间：15分钟内 |
| 3）故障申告后现场支持响应时间：2小时内 |
| 4）故障分析报告和解决方案以及后续预防措施提供时间：故障排除后3天内 |
| **专职责任工程师** | 提供二对一固定专职工程师 |
| **技术支援请求** | 提供技术支援请求等级管理制度 |
| **复杂故障处置预案** | 10分钟内紧急响应，2小时内到达支持现场，同时在路途中不中断电话支持以求快速解决问题，保证3天内提供故障分析报告以及后续预防措施。 |
| **维保年限** | ≥2年 |
| **其他** | 其它设备及辅助设备（如准入控制系统、机柜等）由各县（市）根据需求自行设计配置 |

专网整合IP地址规划设计

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| **政府侧** | 主要是政务外网VPN2的地址规划，包括市县政务外网MCE至市县环保主管单位CE的VPN2互联地址规划及NAT地址规划。  VPN2互联地址规划：本次项目新增设备的互联地址需求如下：MEC-CE每个点分配1段30位掩码的地址段，需要市、县（市、区）政府在实施前统一进行规划分配。  NAT地址段分配：VPN2 NAT地址段采用之前分配给金华的59.202开头的地址段，需要市、县（市、区）政府按当地环保实际地址需求量统一进行分配（至少2个，一个用于新VPN3访问政务外网上的VPN2，一个用于原环保VPN2访问政务外网上的VPN2）。 |
| **市（本级）环保侧** | 原市环保专网内部IP（10.33.X.X）不改变，根据省厅统一规划新的IP地址网段，用于环保专用VPNPE-MCE、MCE-CE设备之间互联IP地址。CE与新增安全网关或新增核心交换机互联用原环保专网的（10.33.X.X）的地址。 |
| **信息安全** | 内部专网信息安全是保障环保部门业务正常运行的关键内容核心资产，信息安全是重中之重，需要专业的运维工程师资质证书人员进行保障，需要服务公司提供1名信息系统运维管理工程师，提供具有RHCE和RHCT的证书，华为资深网络工程师，IPv6协议与安全技术等相关证书人员各1名（连续六个月的社保缴费记录，原件备查） |
| **维保对象** | 1. 政府侧 |
| 2）市（本级）环保侧 |
| **维保年限** | 本案维保年限≥2年。 |
| **其他** | 包含维保过程所需工具、设备、备件、备机、交通费用等 |

环保专用VPN路由互通原则设计

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| **全市环保单位内部互访** | 不改变原访问的目的IP和源IP，在新建的环保专用VPN内部实现。 |
| **环保专用VPN与政务外网VPN2非冲突（重叠地址段）互访** | 通过CE设备的缺省路由+源地址转换实现 |
| **环保专用VPN与政务外网VPN2冲突（重叠地址段）（互访** | 环保专网访问政务外网VPN2时，通过在CE上配置明细静态路由指向VPN2子接口，将流量引导至VPN2，加上源地址转换实现；政务外网VPN2访问环保专网内部应用时，在CE设备将环保专网内部应用的10.33或172段的该应用的地址或端口映射为政务外网VPN2地址（例如59段）后访问（目的IP/端口转换）。对于单个冲突IP，采用协调更改一方IP的方式解决 |
| **源地址分别转换** | 各地环保VPN2区域访问电子政务外网时源地址转换为A地址，各地环保VPN3区域访问电子政务外网时源地址转换为B地址 |
| **不允许环保专用VPN访问互联网** | 在CE设备将原环保专网地址NAT为政务外网VPN2的地址（例如59段）后，将此转换后的地址加入当地政府VPN2互联网出口处安全设备的黑名单，或不在该安全设备上进行出互联网的源地址转换，以达到禁止环保专网访问互联网的目的 |

环保专网整合路由规则设计

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备** | **VPN** | **路由方式** | **备注** |
| **1** | **政府侧PE** | VPN3 | 动态路由 | 由当地政务外网主管单位完成环保专有VPN内OSPF等相关路由及VPN配置（BGP与VPN3的OSPF互引入） |
| **2** | VPN2 | 静态路由 | 由当地政务外网主管单位分配给环保单位的NAT地址及静态映射类地址（如59网段的VPN2地址）的静态路由，并注入政务外网VPN2路由表。 |
| **3** | **政府侧MCE** | VPN3 | 动态路由 | 由当地政务外网主管单位完成环保专用VPN内相关OSPF等配置 |
| **4** | VPN2 | 静态路由 | 由当地政务外网主管单位分配给环保单位的NAT地址及静态映射类地址（如59网段的VPN2地址）的静态路由。指向CE。 |
| **5** | VPN2 | 缺省路由 | 实现政务外网非冲突地址互访，用于引导环保单位访问政务外网的业务流量。，指向PE。 |
| **6** | **环保主管单位CE设备** | VPN3 | 静态路由 | 将当地环保的业务网段回指向内部安全网关或核心交换机 |
| **7** | VPN3 | 静态路由 | 将环保全网路由（10和172两个A）指向VPN3子接口，用于引导访问环保内部网络的流量，防止因割接前期OSPF未学到环保全网路由导致业务中断。 |
| **8** | VPN3 | 动态路由 | 承载环保全网路由，实现环保内部互访。将VPN3的环保本地静态路由注入到OSPF中。 |
| **9** | VPN2 | 静态路由 | 如果政务外网的地址与目前环保网重叠，则通过在CE上配置指向VPN2子接口的明细路由，引导流量访问政务外网。 |
| **10** | VPN2 | 静态路由 | 如当地环保内部使用了VPN2地址（如59地址），在CE上配置环保单位的业务路由指向内部。 |
| **11** | VPN2 | 缺省路由 | CE配置指向VPN2的缺省路由，用于引导访问政务外网的流量。 |

市县两级政府侧PE设备路由设计

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| **设计原理和内容** | 通过在BGP下引入原环保专网业务网段的OSPF路由，（发布各环保主管单位的业务路由），使政务外网省、市、县各PE节点通过MPLS VPN承载网都能收到发布的环保专用VPN业务路由，从而实现环保专网网络互通。  通过在OSPF下引入环保专用VPNBGP路由，发布环保路由至每一台CE设备，使得CE可以学习到环保的全网路由。  通过在BGP下引入分配给环保单位的NAT地址路由和静态映射（如59网段的VPN2地址）路由，发布各环保主管单位的政务外网业务路由，使得环保主管单位通过MPLS VPN承载网能够访问政务外网。  通过在BGP下引入规划政务外网VPN静态路由，发布各环保主管单位的政务外网业务路由，使得环保主管单位通过MPLS VPN承载网能够访问政务外网。 |

市县两级政府侧MCE设备路由设计

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| **设计原理和内容** | 在CE-MCE路由器对接的链路上启用2个子接口，分别对应VPN2和VPN3。  VPN2：MCE路由器将分配给当地环保单位的政务外网地址段指向CE的VPN2接口，同时配置缺省路由指向PE的VPN2接口（用于通过VPN2访问政务外网），  VPN3：MCE路由器配置OSPF路由协议，在CE路由器上发布环保对应地址段，政务网MCE、PE路由自动学习环保地址段，便于后期路由维护。 |

市县两级环保侧CE设备路由设计

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| **设计原理和内容** | CE路由器配置缺省路由指向MCE的VPN2接口实现政务外网非冲突地址互访。配置ospf动态路由，将本地环保单位的地址段发布进ospf路由协议，同时通过ospf自动学习其他环保单位的地址段，实现环保内部互访。环保专用VPN中IP与原政务外网某个具体IP冲突的情况下，根据实际情况通过协调某一方更改IP的方式来解决。 |

ospf区域规划

|  |  |  |
| --- | --- | --- |
| 序号 | 地市 | ospf区域号 |
| 11 | 金华 | 79 |

相关设备及线路配置

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| **主要设备选型** | CE设备： CE设备要考虑到这一台设备既承担VPN3的流量，同时也承担着互联网出口整合工作后的VPN2流量，对性能有较高的要求。  安全网关设备：安全网关设备要考虑防火墙、IPS、流控/行为管理、WAF、防病毒等功能模块。对安全功能有多方面的需求。 |
| **线路** | 主要是电子政务外网专线和环保内部分支专线。  电子政务外网专线主要考虑线路带宽因素。要确保线路带宽足够承载互联网出口整合后内部环保用户通过VPN2访问电子政务外网和互联网的需求，还要满足VPN3内数据交互、应用访问、视频会议等对带宽的需求。本项目市级接入带宽为1000M，县级根据实际需求确定带宽,建议不低于100M。  内部分支专线主要考虑原环保专网专线的连接可达。要确保省厅将原环保专网专线取消后，支队（大队）、监测站、分局等内部分支原有的数据业务传输访问、视频会议等仍有专线连接的需求。接入带宽≥100M。市本级不在环保大楼办公的单位市局机关（财富大厦）、婺城分局（婺城区政府大楼）、开发区分局（双溪西路620号）、金华山、环科院和污普办（宝莲大厦）等单位通过连接专线到环保大楼三楼机房方式实现VPN3业务访问和数据报送，此专线带宽建议≥100M。其中原环保大楼到宝莲大厦、环保大楼到财富大厦、环保大楼到婺城区政府大楼、环保大楼到东阳监测站、环保大楼到永康监测站、环保大楼到武义监测站等联通公司光纤专线（原由省信息中心支付租凭费用，拟取消）取消后各地按需自行续费。 |