基于SDWAN承载技术的生态环境厅业务专网升级

徐益强

（江苏省生态环境监控中心，江苏 南京 210043）

摘　要：江苏省生态环境厅业务专网面临升级改造，成立业务专网升级改造项目团队，进行大量的技术体制论证研究工作，确定以软件定义广域网（SDWAN）技术为基础进行专网升级改造工作。阐述了江苏省生态环境厅业务专网现状，并进行需求分析，从整体方案设计、SDWAN方案设计、安全防护设计以及网络管理设计等方面提出满足江苏省生态环境厅业务专网升级改造的技术方案。

关键词：软件定义广域网；安全防护；网络管理

中图分类号：TP393

文献标志码：A

doi: 10.11959/j.issn.1000−0801.2024046

Upgrade of the dedicated network for the Department of Ecology and Environment based on SDWAN bearer technology

XU Yiqiang

Jiangsu Provincial Ecological Environmental Monitoring Center, Nanjing 210043, China

Abstract: The dedicated network of the Jiangsu Provincial Department of Ecology and Environment is in need of upgrades and transformation. A project team was established to conduct extensive research and analysis on technical systems. After a lot of technical system demonstration and research work, it was decided that the upgrade and transformation should be based on software-defined wide area network (SDWAN) technology. An overview of the current state of the dedicated network was proposed, a needs analysis was conducted, and a technical solution was proposed to meet the requirements of the upgrade. The proposed solution includes overall solution design, SDWAN solution design, security protection design, and network management design.

Key words: SDWAN, security protection, network management

0　引言

江苏省生态环境厅现有业务专网，用于承载全省生态环境系统视频会议服务、自动监控数据的上传和数据交换。随着江苏省政务信息化的发展，现有业务专网已经无法满足业务需求，同时根据有关规定，生态环境厅业务专网需要并入全省电子政务外网。

结合省生态环境厅的实际应用和发展要求，对现有业务专网进行整体改造，以省生态环境厅

收稿日期：2024−01−11；修回日期：2024−04−30

为核心，连接全省13个地市生态环境局、120个区县生态环境局和下属单位。本文经过详细的技术体系论证分析及试点测试，确定采用基于软件定义广域网（software-defined wide area network，SDWAN）技术[1]的网络承载方案。SDWAN技术通过统一整合全网资源、多维观测网络状态、智能分析运行数据，使整个网络实现多角度、全方位的可视化，实现应用驱动的广域网服务。SDWAN技术具备如下优势。

（1）全开放。架构开放，网络的各个层次、不同组件是解耦的，可以很容易做到网络的扩展；网络各组件之间通过开放、标准的接口来通信，从设备到控制器、控制器到编排器提供多层次的、不同抽象度的应用程序接口（application program interface，API），赋予网络灵活的可编程、可定义能力。

（2）场景化。基于场景化的开发思路，提供面向业务的功能应用，满足不同场景的用户需求。

（3）全流程。全流程重构广域网，整网视角管理和控制网络，简化运维管理。

（4）自动化。设备接入自动化、业务部署自动化、流量调度自动化。

（5）端到端。业务驱动网络，基于业务应用的不同需求动态部署调度策略、服务质量（quality of service，QoS）、安全策略等，提供端到端的网络服务。

采用SDWAN技术不仅满足自动监控数据上传和数据交换的基本要求，也满足对视频会议、各远程现场监测点视频监控以及各种环境管理数据传输的需求。升级改造后省生态环境厅业务承载网络保证现有业务的可靠运行，并与电子政务外网安全对接。

1 网络现状及需求分析

1.1 网络现状

目前，江苏省生态环境业务专网以省生态环境厅为核心，使用多业务传送平台（multi- service transport platform，MSTP）专线，连接全省13个地市生态环境局，以及监测中心、应急中心等省厅直属单位。全省生态环境业务专网由1个省中心节点、13个地市级节点、120个区县节点组成。根据生态环境系统上下级的隶属关系及后期生态环境业务模式，省生态环境主干网的业务流向以省厅⟷市局、市局⟷区县局的纵向流为主。

当前全省生态环境业务专网存在如下问题。

全省生态环境业务专网采用租用运营商MSTP专线实现业务承载，价格昂贵，且全部采用单链路方式，可靠性低。

（1）省厅与市局之间带宽仅为100 Mbit/s，市局与区县局之间带宽仅为20 Mbit/s，带宽不足。

（2）省厅、地市局以及区县局之间通过裸网际互连协议（Internet protocol，IP）实现互联互通，存在数据泄露的风险。

（3）全省生态环境业务专网传输路径固化，当链路质量下降时，无法进行灵活调度。同时，由于没有相应的统一网络管理系统，无法实现运维可视化和业务配置的自动下发。

1.2 需求分析

1.2.1 安全接入电子政务外网

目前全省生态环境业务专网采用独立运行的方式，已使用5年多，且未接入电子政务外网。同时，业务专网租用运营商MSTP专线，价格昂贵，合同即将到期。根据部门专网并入电子政务外网的相关要求，需要进行升级改造，完成业务专网与电子政务外网的安全对接，停用原有业务专网，使用政务外网进行互联互通。

1.2.2 视频会议、数据业务高稳定

当前全省生态环境业务专网采用租用运营商MSTP专线实现业务承载，租用的运营商MSTP省—市之间带宽为100 Mbit/s，市—县之间带宽

为20 Mbit/s。随着视频会议、数据接入、数据交换等业务的快速发展，全省生态环境业务专网省—市之间带宽需求提升至500 Mbit/s，而市—县之间带宽需求提升至100 Mbit/s，当前MSTP的带宽已经无法满足业务需求。

特别针对视频会议等突发性业务，当前传统IP技术无法处理视频流量峰值，面临时延高、丢包等网络质量问题，严重影响视频会议质量，亟须采用新技术进行网络升级改造。

1.2.3　网络及用户业务快调度

目前全省生态环境业务专网采用传统IP技术，通过虚拟局域网（virtual local area network，VLAN）实现业务隔离。广域网（wide area network，WAN）侧，各个地市及区县过于分散，直接通过裸IP实现与省生态环境厅数据中心的互联互通，缺少安全防护。同时，由于当前均采用单链路方式，可靠性低，亟须采用加密隧道技术提高安全性，同时采用冗余链路提升链路可靠性，并具备智能选路能力。

1.2.4　网络及业务可视化

当前全省生态环境业务专网有一套网管系统，但是只能简单查看网络拓扑和设备告警，且采用基于查询模式简单网络管理协议（simple network management protocol，SNMP），无法实现高精度网络质量监控，同时，无法查看业务质量。本方案需要提供高精度运维管理平台，实现设备秒级故障检测，同时实时进行全网业务质量监控，具备完善的告警机制，可以快速定位到故障点，并实现业务调度。

针对以上需求，传统的MSTP传输专网由于价格昂贵、带宽小、无法灵活调度以及运维复杂等弊端，已经无法满足省生态环境业务需求。根据部门专网并入电子政务外网的相关要求，本技术方案采用电子政务外网作为省厅、市局、区县局互联网络，电子政务外网设备端口带宽均为100 Gbit/s，可以满足省生态环境业务带宽需求。

电子政务外网采用多协议标签交换虚拟专用网络（multi-protocol label switching virtual private network，MPLS VPN）技术，能够很好地实现不同单位的网络隔离，但是无法满足业务快速开通及质量调优、链路灵活调度、配置自动下发等需求。经过多轮技术研讨及试点测试，确定以SDWAN技术为基础进行专网升级改造工作。SDWAN把软件引入网络[2]，通过软件程序配置分布在全省各地的分支机构的网络连接，实现分支与总部的灵活、快速连接。SDWAN采用管控析一体化解决方案，不仅实现总部、分支灵活拓扑的展示，同时可以基于虚拟专用网络（virtual private network，VPN）及QoS等进行业务端到端一键下发，本技术方案采用IPSec VPN over SDWAN的方式，对传输数据进行加密，保障了数据传输的安全。

2　SDWAN网络承载方案

2.1　整体方案设计

全省生态环境业务专网升级改造设计包含SDWAN方案设计、安全防护设计、网络管理设计，整体设计采用分层化、模块化的设计思想。整体方案设计充分考虑扩展灵活、技术先进、高可靠、易运维，同时兼顾成本。

整网架构采用分层结构设计，网络层次清晰、扩展能力强、灵活性高。本方案采用基于SDWAN技术的IPSec VPN隧道方案，相比传统IPSec VPN固定星形网络结构，该方案可支持站点间任意灵活动态拓扑调整，实现网络的高可用性。SDWAN灵活拓扑如图1所示。

方案选用国际标准化、开放的技术协议，兼顾用户自身技术运用状况，采用适用的动态路由、定制化QoS等技术实施，配合先进成熟技术，包括内部网关协议（interior gateway protocol，IGP）快速收敛等技术部署，为全省生态环境系统核心业务不间断转发提供技术保证。路由

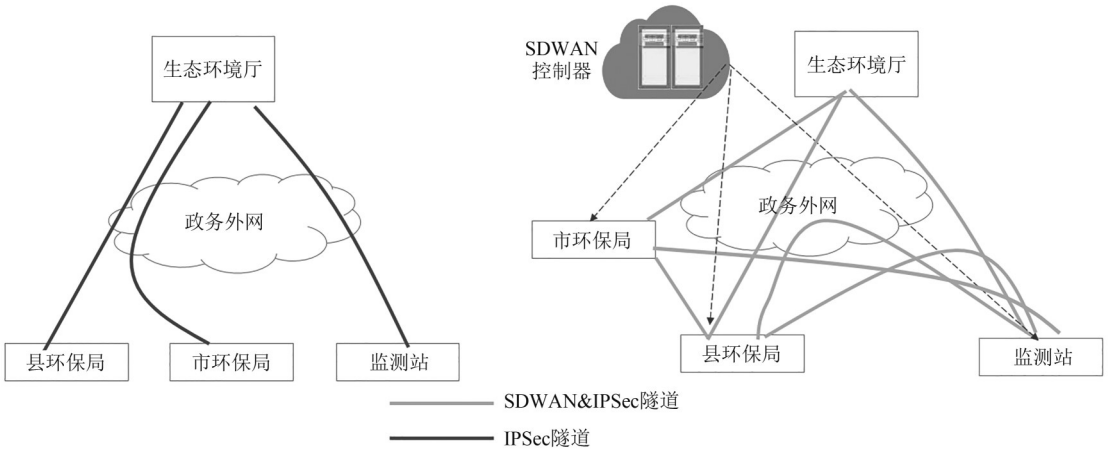


图1 SDWAN灵活拓扑

交换和防火墙设备具备高带宽扩展能力，核心路由器和市级节点均具备万兆的扩展能力，为全省生态环境高速网络平台提供强大扩展能力，具有良好使用性价比。

省生态环境厅专网承载重要的生态环境系统应用业务，因此需要具备7×24 h的网络支撑能力，业务专网部署基于类的QoS策略部署，如基于分类的队列（class-based queueing，CBQ）、低延迟队列（low latency queuing，LLQ）以及基于类的防拥塞控制加权随机先期检测（weighted random early detection，WRED）等技术部署，解决了无法实现全网QoS策略的问题。业务专网采用SDWAN高效智能运维系统，网络管理任务除了基本网络拓扑、设备管理之外，还涵盖了网络流量管理，包括设备端口采集的五元组信息、核心业务流的带宽利用信息统计等。

2.2 SDWAN方案设计

本文采用SDWAN分支解决方案[3]，给用户提供与传统部署和管理广域网所不同的业务体验和业务保障，能极大降低用户的网络运维难度和部署及业务保障成本。根据省生态环境厅专网改造设计思想及其应用需求，此次网络改造在总体建设上停用原有架构（MSTP电路），采用SDWAN解决方案，使用IPSec VPN over SDWAN的方式，采用业务与网络分层构建、逐层保护的指导原则。

2.2.1 SDWAN系统架构[4-5]

本文SDWAN技术方案是构建网络的一种架构，其本质和目标主要包含如下。

（1）软件定义网络。通过软件定义的思想来设计新的网络架构，让网络能够主动适应用户业务和流量变化，而不是被动地承载流量。

（2）应用驱动网络。以应用为源头，用自动化的方式驱动网络进行动态调整，快速满足实际的业务需求。

（3）软件简化运维。通过软件驱动应用参与网络的整个生命周期，实现自动化的业务部署、可视的网络呈现、灵活的流量调度，最终简化网络的管理运维。

SDWAN系统架构统一融合智能网络管理、智能控制、智能分析，实现“管”“控”“析”三位一体的融合网络控制中枢和智能“大脑”，网络全域覆盖，实现端到端的网络和业务自动化、可视化、精细化的网络管理。

（1）统一支撑底盘定位是整个网络的“大脑”，基于容器化平台[6]，采用服务化的软件架构，为用户提供数据中心、园区、广域网多场景融合服务；提供标准RESTful API北向接口，更

加开放、灵活地集成不同的操作支撑系统（operation support system，OSS）/基站子系统（base station subsystem，BSS）中。

（2）管理组件。提供设备版本管理、配置管理、告警、性能、拓扑等传统管理能力，并提供QoS等增值服务能力。

（3）控制组件。提供零配置自动开局（zero touch provisioning，ZTP）部署、WAN优化、网络流量调优等功能，优先保障高优先级业务需求。

（4）分析组件。基于Telemetry遥测技术实现网络状态快速感知、秒级运维。向用户展示呈现网络中最关键的价值元素，辅助运维。分析服务将人工智能（artificial intelligence，AI）应用于运维领域，实现降低运维成本、提高企业产品的竞争力的目标。

2.2.2　网络拓扑设计

网络拓扑设计充分考虑线路的可靠性和设备的可靠性，省生态环境厅改造后的主干网络拓扑如图2所示。

SDWAN区域部署情况如下。

（1）省级核心交换机与SDWAN设备之间部署防火墙，口字型连接。

（2）采用三级组网模式，省←→市，市←→县部署IPSec VPN，业务地址不变。

（3）区县间互访通过市级节点互访。

（4）整体设计与MPLS VPN无关，只要政务外网网络可达，任意节点可以直接建立IPSec VPN，特殊情况县—省也可建立IPSec VPN。

（5）省级SDWAN路由器兼作RR设备，所有市级以及部分县级SDWAN路由器作为CPE设备与RR建立SDWAN通道。RR上部署路由策略，通过修改EVPN路由的下一跳地址[7-8]，实现灵活改变overlay网络拓扑。SDWAN通道[9-10]建立示意图如图3所示。

（1）控制通道建立

RR和CPE之间发布TTE信息和私网路由的通道

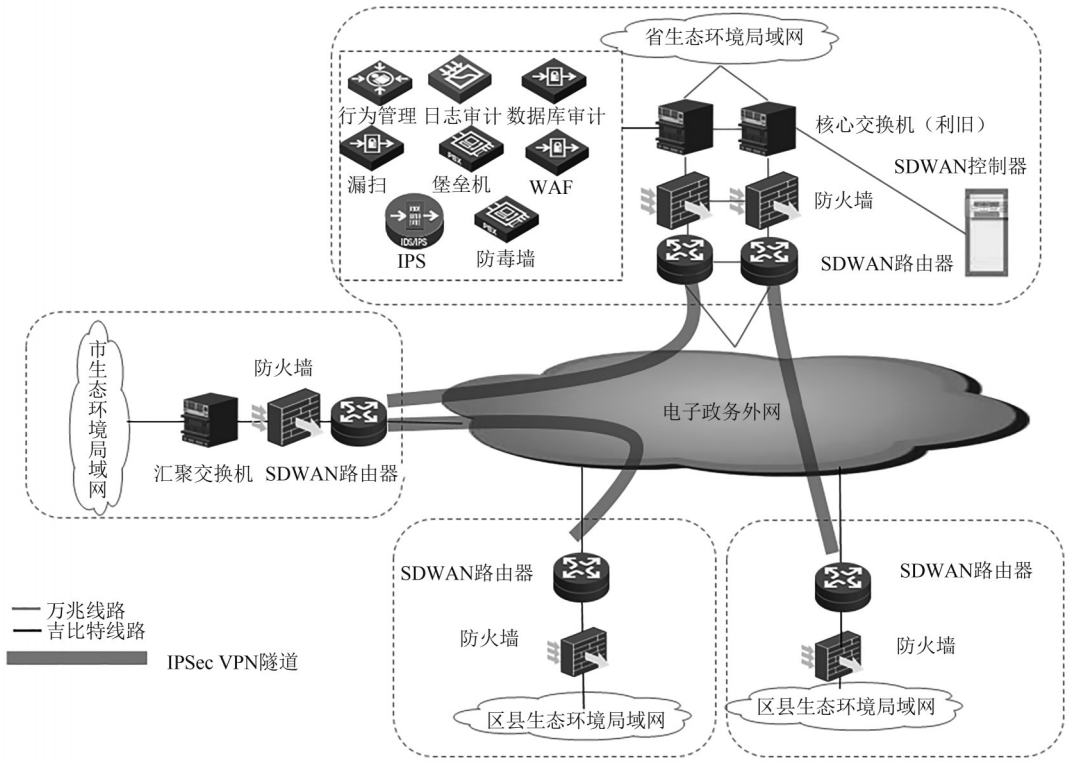


图2　主干网络拓扑

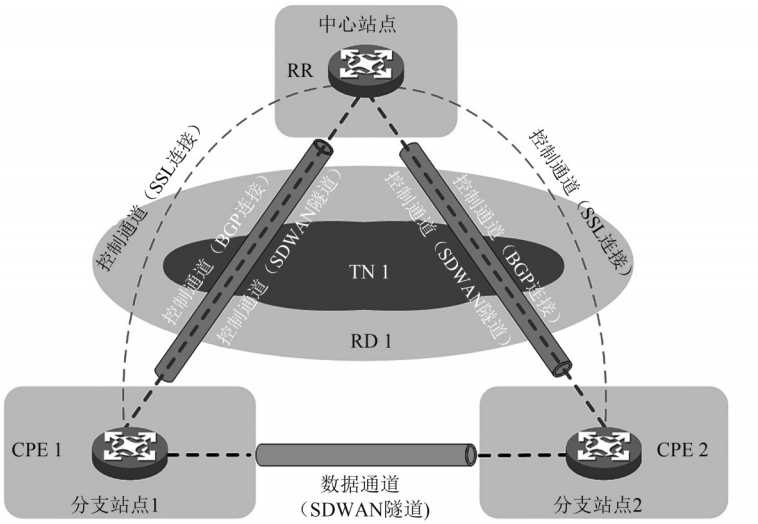


图3　SDWAN通道建立示意图

注：CPE：customer provided edge，用户网络的边缘设备。RR：route reflector，用于在CPE之间反射TTE信息和私网路由等。TN：transport network，运营商提供的广域接入网络，用来实现分支站点之间的互联。RD：routing domain，由彼此之间路由可达的不同传输网络构成的区域。只能在位于同一个路由域内的CPE之间或CPE与RR之间建立SDWAN隧道。SDWAN隧道：2个SDWAN设备之间的点到多点逻辑通道。TTE：transport tunnel endpoint，SDWAN设备接入传输网的连接点和SDWAN隧道的端点。TTE连接：2个TTE之间的点到点逻辑连接。通常一个SDWAN隧道上建立多个TTE连接。

- CPE与RR之间建立SSL连接（控制通道1）。
- CPE与RR之间互相发送TTE信息。
- CPE与RR收到对端发送的TTE信息后，比较TTE信息中携带的路由域。若路由域相同，则建立到达对端的SDWAN隧道（控制通道2）；若路由域不同，则不建立SDWAN隧道。
- 完成SDWAN隧道建立后，CPE、RR自动在本地添加到达对端Systerm IP的路由。
- CPE、RR之间基于Systerm IP建立IPv4 Tnl-Encap-Ext地址族下的BGP连接。

（2）数据通道建立

CPE之间转发数据报文的通道

- CPE通过IPv4 Tnl-encap-ext路由向RR发送TTE信息。
- RR将TTE信息反射给其他CPE。
- CPE收到由RR反射的TTE信息后，比较TTE信息中携带的路由域。若路由域相同，则建立到达对端CPE的SDWAN隧道；若路由域不同，则不建立SDWAN隧道。

2.2.3　网络部署方案[11]

（1）underlay网络设计

在SDWAN解决方案中，underlay网络设计主要考虑的是区域内网underlay协议设计以及区域间underlay设计。

区域内underlay设计，首先要考虑区域内组网结构，网关类部署一般是指SDWAN设备作为网关设备，下连交换机后直连终端设备，此时设备直接作为网关提供如动态主机配置协议（dynamic host configuration protocol，DHCP）server等服务。本方案中，SDWAN设备作为出口设备，按照路由类部署，区域内underlay采用OSPF协议实现本地站点与CPE之间的路由传递。

区域间underlay设计，主要考虑作为网络出口，与外网设备进行对接时，需要配置的参数。本方案中，如果远端CPE上某个VPN实例的import target属性与路由的export target属性中存在相同的属性值，则接收该IP前缀路由并将其添加到VPN路由表中，其中路由的出接口为接收该路

由的SDWAN隧道接口，下一跳为远端CPE的system IP。

（2）overlay网络设计

overlay网络设计，首先需要将客户内网流量进行分类，对不同类型的流量进行不同的overlay策略设计。设计原则如下。

- 按照业务部门来划分，如将一个工作组的人员划分到一个安全组。
- 按照终端类型来划分，如将打印机划分到一个安全组。
- 按照安全级别来划分，如同一安全级别的人划分到一个安全组，具有相同权限。

在SDWAN组网中，使用VPN实例为不同业务提供隔离功能。

- 控制平面：CPE之间交互的以太网虚拟专用网络（Ethernet virtual private network，EVPN）路由中携带VN ID标识不同业务的私网路由，每个VPN实例之间互相独立，拥有自己的转发表和路由表。
- 数据平面：不同业务通过CPE上的接口接入设备，CPE通过该接口上关联的VPN实例识别业务所属的VPN。查找该VPN实例的转发表，为业务报文添加SDWAN封装后，将报文转发到远端CPE。

这种隔离方式可以实现多个VPN共享同一条SDWAN隧道，在实现流量隔离的同时，减少设备间隧道数量，减少网络资源的消耗。

2.2.4　智能选路设计

当前生态环境厅业务专网采用传统IP技术实现互联互通[12]，链路优选基于链路开销或者路由策略，无法根据实际的业务需求选择最适合的链路，不能满足所有业务的服务等级协议（service-level agreement，SLA）网络质量要求。本方案中，采用智能选路（resilient intelligent routing，RIR）技术，可以根据不同业务流量的链路需求，如链路质量、链路带宽等，为其选择最适合的链路。

（1）基于链路优先级选路

基于SDWAN隧道部署智能选路时，可以在业务流量模板下基于传输网络名称，为SDWAN隧道配置链路优先级。设备为某业务流量选路时，会按照业务流量模板下配置的链路优先级从高到低的顺序，依次选路。

- 如果该优先级下没有链路符合业务要求，则继续选择次优先级下的链路。
- 如果该优先级下有且只有一条链路符合业务要求，则选择该链路进行传输。

（2）基于链路质量选路

在SDWAN中，基于每个TTE连接启动智能网络质量分析（intelligent network quality analyzer，iNQA）测量实例，探测TTE连接的丢包率、时延和抖动。RIR根据综合质量指标（comprehensive quality indicator，CQI）算法评估各链路的质量优劣。

为避免链路频繁切换，设备选路时使用综合质量近似CQI值来评估链路优劣。综合质量近似CQI值为不大于综合质量最大CQI值的5倍。CPE基于链路质量为业务流量选路时，如果为该业务流量指定了质量策略，则CPE会根据链路探测和SLA计算综合质量近似CQI值，并基于该值进行选路。本方案采用基于链路质量策略选路，为不同业务设置相应的时延、抖动、丢包指标，并根据CQI算法计算满足网络质量要求的链路，从而为不同业务选择符合SLA网络质量要求的最优链路，保证如视频会议等业务的可靠传输。

（3）基于链路带宽选路

为某个业务的流量进行智能选路时，设备会实时获取业务预计使用的带宽，并基于获取的带宽进行带宽检测；如果获取不到，则采用手工配置的业务预计使用的带宽进行带宽检测。如果同时满足以下条件，则认为待选链路当前可用带宽符合业务带宽要求，带宽检测通过。

- 待选链路所属物理接口的已使用带宽与业

务预计使用的带宽之和小于待选链路所属物理接口总带宽的80%。

• 待选链路已使用带宽与业务预计使用的带宽之和小于待选链路总带宽的80%。

（4）选路延迟和选路抑制

为提高报文转发效率，业务流量完成第一次智能选路后，后续相同业务的流量均按照第一次选路结果进行转发。当业务流量模板中的任一链路发生如下任一变化时，设备会重新选路。

• 链路质量由满足业务质量要求变为不满足业务质量要求或由不满足业务质量要求变为满足业务质量要求。

• 链路已使用带宽达到该链路最大带宽的90%，或者链路所属的物理接口已使用带宽达到所属物理接口最大带宽的90%。

设备执行一次选路后，如果配置了选路抑制周期，则会进入选路抑制周期。当选路延迟时间内设备链路状态变为不满足重新选路条件，设备不会重新选路。

2.2.5 广域网优化设计

通过智能选路方案[13]，可以为不同业务选择满足SLA要求的链路，提升了省生态环境厅整体业务专网服务质量。但是针对视频会议突发性流量，智能选路依然不能够完全解决峰值丢包问题。为保证省生态环境厅视频会议的高可靠性，本方案针对广域网侧网络进行优化设计。广域网优化设计包括发送端、传输路径、接收端3个方面，本广域网优化设计是在传输路径已经确定的条件下开展的，因此从发送端和接收端两端进行设计。

• 发送端尽量减少发送数据量，通过数据压缩、重复数据删除等技术手段实现，本方案采用广域网应用服务（wide area application service，WAAS）技术。

• 针对视频会议场景，发送端考虑数据冗余，确保视频会议流畅度，本方案采用前向纠错（forward error correction，FEC）。

• 接收端尽量缓存热点数据，加速用户访问效率，提升用户访问体验，本方案采用网站缓存技术。

（1）WAAS

WAAS设备通过配置优化动作，改善广域网链路高时延、低带宽的缺陷。WAAS优化动作包括传输层流优化（transport flow optimization，TFO）、数据冗余消除（data redundancy elimination，DRE）和LZ压缩（Lempel-Ziv compression）。

• TFO是传输层流优化技术。在不改变TCP流量的源、目的IP地址和端口号的情况下，在广域网链路两端对TCP连接进行透明代理，并对广域网链路两端的TCP流量进行优化。

• DRE是消除冗余数据技术。在相互通信的WAAS设备上保存重复数据块与字典索引对应的数据字典。用字典索引替换重复数据块的过程称为DRE压缩，用重复数据块替换字典索引的过程称为DRE解压缩。

• LZ压缩是一种数据无损压缩技术。主要通过自建字典方法来进行压缩替换，其压缩字典存在于压缩结果中。

（2）FEC

FEC主要解决实时音、视频的网络丢包问题，保障重要音、视频流穿越广域网后仍能流畅播放，增强RTP流在广域网传输的可靠性。发送端将多个原始报文，通过RS算法编码计算并增加冗余包后，以编码块为单位发送。

根据平均抗丢包率的配置方式不同，FEC分为固定的FEC（determined-FEC，D-FEC）和自适应的FEC（adaptive-FEC，A-FEC）这两种类型。

• D-FEC使用固定的平均抗丢包率，适用于链路丢包率比较稳定的场景。

• A-FEC根据实时链路丢包率动态调节平均抗丢包率，实现机制比D-FEC复杂。可在

保证通信质量和可靠性的前提下，尽量减少冗余包数量，提高传输效率。在广域网环境下，A-FEC 应用更广泛。

本文采用 A-FEC 技术。

1） 发送端识别业务报文，进行 FEC 编码处理后发送。

2） 在广域网中传输报文，编码块中的原始报文和冗余包都可能出现丢包。

3） 接收端识别业务报文，进行 FEC 解码后发送给目的端。

4） 接收端在执行步骤 3 的同时会计算每个编码块的丢包率，按周期对编码块的丢包率采样，并将采样的丢包率反馈给发送端。

5） 发送端根据收到的丢包率计算平均值，动态调整平均抗丢包率，并从下一次编码开始，使用调整后的平均抗丢包率进行 FEC 编码。

本 SDWAN 方案中设备集成支持 A-FEC 前向纠错，在最高丢包 30% 的情况下，视频会议不花屏，拒绝视频会议马赛克，优化视频会议体验。

（3）网站缓存加速

网站缓存功能将用户访问过的 Web 页面内容缓存在本地用于直接响应后续相同请求。

- 用户通过 HTTP/HTTPS 协议请求指定服务器的 Web 页面内容时，网站缓存将服务器响应的内容缓存在本地文件中。
- 后续用户访问该服务器时，网站缓存获取报文的统一资源定位（uniform resource locator，URL）系统，依据 URL 在本地缓存文件中进行查找。
- 网站缓存使用查找到的本地缓存文件中的内容直接响应用户。

通过 WAAS、FEC 和网站缓存等广域网优化技术，视频会议等业务质量得到保障，解决了带宽不足、丢包等因素导致的业务响应速度慢、视频会议马赛克等业务质量问题，极大提升了省生态环境厅的生产工作效率。

2.3　安全防护设计

本方案通过 SDWAN 控制器来深度融合安全控制器[14]，基于统一数字底盘来做统一界面呈现，对外提供统一的页面和丰富的安全能力。SDWAN 安全防护设计如图 4 所示，2 个控制器各司其职又互相配合。

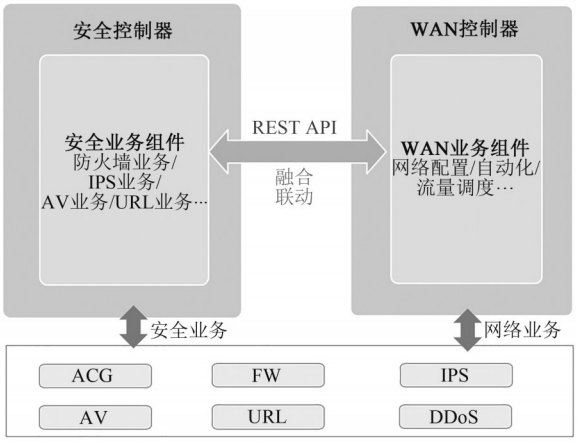


图4　SDWAN 安全防护设计

- SDWAN 控制器提供设备上线、基础网络部署能力。
- 安全控制器提供安全域和安全策略自动化部署能力。
- 安全控制器提供分支 CPE 设备上的安全功能自动化部署和统一管理能力。

安全自动化部署如图 5 所示，具体包括如下策略。

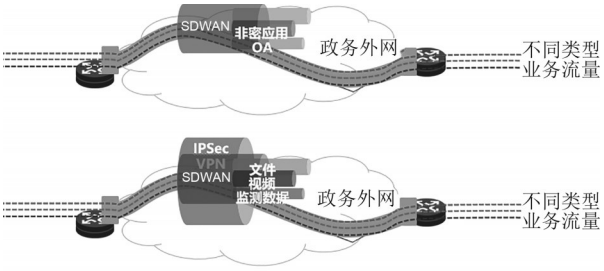


图5　安全自动化部署

（1）防火墙安全策略

将安全需求相同的接口进行分类，并划分到不同的安全域（security zone），能够实现域间策

略的统一管理。

（2）入侵防御系统（intrusion prevention system，IPS）防御技术

trust安全域和untrust安全域与局域网和Internet相连，使用IPS策略对用户数据报文进行IPS防御。通过应用层检测引擎对报文进行特征匹配来实时检测入侵行为，并基于IPS策略对报文进行处理。IPS策略中定义了对哪些IPS特征进行匹配，以及对匹配成功的报文执行的动作。

（3）URL过滤

URL过滤通过将报文中识别出的URL与过滤规则进行匹配，判断对报文执行的动作。首先，URL过滤模块向应用层检测引擎下发过滤规则；其次，引擎在识别出报文中的URL后，将URL与过滤规则进行匹配，并向URL过滤模块返回匹配结果；最后，URL过滤模块根据匹配结果判断对报文执行的动作。

（4）防病毒（anti-virus，AV）策略

隔离内网和外网的网关设备上部署防病毒策略来保证内部网络安全。

- 内网用户需要访问外网资源，且经常需要从外网下载各种应用数据。
- 内网的服务器需要经常接收外网用户上传的数据。

部署防病毒策略后，正常的用户数据可以进入内部网络，携带病毒的报文会被检测出来，并被采取阻断、重定向或生成告警信息等动作。

（5）安全日志审计

设备在运行时会产生日志，按模块和日志等级将设备产生的日志信息发送到日志主机，用于日志分析审计。

2.4 网络管理设计

本方案SDWAN控制器提供网络运维管理能力，提供iNQA随流探测、可视化运维报表、一键巡检、故障设备替换等运维管理能力。

（1）iNQA随流探测

iNQA目前支持丢包测量，可测量正向、反向以及双向的丢包情况（包括丢失的报文数、报文的丢失率、丢失的字节数、字节的丢失率），利用测量结果可快速定位丢包时间、丢包位置、丢包严重程度。

（2）可视化运维报表

网络可视。支持GIS地图展示组件， GIS地图支持在线模式；基于站点、链路的拓扑呈现，实时掌握站点设备性能及链路状态信息；全网设备链路故障实时告警，快速获取异常信息；自定义DashBoard，展示偏好信息。

（3）一键巡检

支持手动巡检和自动巡检；支持创建巡检任务，自由定制巡检项；支持下载和查看巡检结果。

（4）故障设备替换

支持故障设备替换，新设备上线后控制器自动部署原故障设备的全部业务配置。

3 结束语

江苏省生态环境厅业务专网以SDWAN技术为基础进行网络升级改造，本文详细阐述了SDWAN承载方案设计，充分体现了SDWAN技术在灵活组网、自动部署、安全防护、高效运维等方面的优势和能力[15]。同时，针对视频会议等业务质量差问题，重点介绍了智能选路、广域网优化等技术方案，满足客户的业务需求。最后在安全防护、网络管理方面也给出了解决方案，使业务专网在安全性、可管理性方面能力得到极大提升。

参考文献：

[1] 姜建民, 常海涛, 张文亮. SD-WAN: 企业互联网服务新趋势[J]. 山东通信技术, 2021, 41(3): 28-31.
JIANG J M, CHANG H T, ZHANG W L. SD-WAN: the new

trend of enterprise Internet service[J]. Shandong Communication Technology, 2021, 41(3): 28-31.

[2] 杨帅. 传统广域网向软件定义广域网(SD-WAN)架构转型浅析[J]. 中国信息化, 2019(5): 60-63.
YANG S. Analysis on the transformation from traditional WAN to software defined WAN (SD-WAN)[J]. Chinese informatization, 2019(5): 60-63.

[3] RISDIANTO A C, SHIN J, LING T C, et al. Leveraging onos sdn controllers for of@tein sd-wan experiments[J]. Proceedings of the Asia-Pacific Advanced Network, 2015, 40: 1.

[4] 穆琋博, 柴瑶琳, 宋平, 等. SD-WAN产业发展与关键技术研究[J]. 信息通信技术与政策, 2019(11): 73-78.
MU Y B, CHAI Y L, SONG P, et al. Research on industry developments and key technologies of SD-WAN[J]. Information and Communications Technology and Policy, 2019(11): 73-78.

[5] 王胜志, 章道勇. SD-WAN网络架构及产品应用探索[J]. 邮电设计技术, 2021(3): 71-76.
WANG S Z, ZHANG D Y. Network achitecture and product exploration of SD-WAN[J]. Designing Techniques of Posts and Telecommunications, 2021(3): 71-76.

[6] 颜永明, 左良, 许斌, 等. LSN DCI EVPN VxLAN组网架构研究及实现[J]. 电信科学, 2017, 33(6): 171-178.
YAN Y M, ZUO L, XU B, et al. Research and implementation of network architecture of LSN DCI EVPN VxLAN[J]. Telecommunications Science, 2017, 33(6): 171-178.

[7] 王霞. Openstack云平台多租户网络隔离证据收集研究与分析[D]. 北京: 北京工业大学, 2017.
WANG X. Research and analysis of forensic collection of multi-tenant network isolation in openstack cloud platform[D]. Beijing: Beijing University of Technology, 2017.

[8] 董炳泉. DWAN提供云网融合产品能力的研究及应用[J]. 信息通信, 2019(12): 2.
DONG B Q. DWAN provides research and application of cloud network convergence product capabilities[J]. Information and communications, 2019(12): 2.

[9] 牛佳, 颜永明, 林志华. SD-WAN隧道技术与组网模式[J]. 电信科学, 2021, 37(1): 137-146.
NIU J, YAN Y M, LIN Z H. SD-WAN tunnel technology and network constuction[J]. Telecommunications Science, 2021, 37(1): 137-146.

[10] 刘汉生. OTN技术及其在电信传送网中应用的研究[D]. 南京: 南京邮电大学, 2011.
LIU H S. Research on OTN technology and its application in telecom transmission network[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2011.

[11] 杨锋. SD-WAN应用场景和规模部署挑战浅析[J]. 通信世界, 2019(34): 47-48.
YANG F. Analysis of SD-WAN application scenarios and scale deployment challenges[J]. Communications World, 2019(34): 47-48.

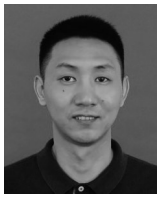
[12] 刘汉江, 欧亮, 陈文华, 等. 基于SDN的跨数据中心承载技术[J]. 电信科学, 2016, 32(3): 28-34.
LIU H J, OU L, CHEN W H, et al. Bearing technology across the data center based on SDN[J]. Telecommunications Science, 2016, 32(3): 28-34.

[13] 张朝昆, 崔摇勇, 唐嚣祎, 等. 软件定义网络(SDN)研究进展[J]. 软件学报, 2015, 26(1): 62-81.
ZHANG C K, CUI Y Y, TANG H Y, et al. State-of-the-art survey on software-defined networking (SDN)[J]. Journal of Software, 2015, 26(1): 62-81.

[14] 王茜, 王岩, 樊俊诚, 等. 安全SD-WAN的架构与应用实践[J]. 移动通信, 2019, 43(7).
WANG Q,WANG Y, FAN J C, et al. Infrastructure design and experiment of security SD-WAN[J]. Mobile communications, 2019, 43(7).

[15] 王瑾. 政企业务遇瓶颈 SD-WAN助运营商实现云网一体化[J]. 通信世界, 2017(16): 48-49.
WANG J. SD-WAN helps operators to realize the integration of cloud and network when government and enterprise business encounter bottlenecks[J]. Communications World, 2017(16): 48-49.

[作者简介]



徐益强（1982– ），男，江苏省生态环境监控中心高级工程师，主要研究方向为环境信息、网络安全。