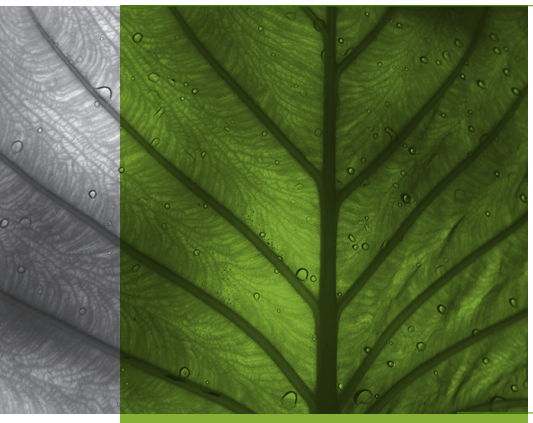

通过 SESSION SMART SD-BRANCH 连接数以千计的分支机构

SASE 架构融合了 WAN 和网络安全功能，可在边缘控制访问并管理流量

挑战

为支持传统企业应用和流量模式而设计的旧有中心辐射型分支机构网络无法适应主导现代企业的动态工作负载和多样化数据流。但新的云优先 IT 模式会引发各种性能、安全性和可用性方面的挑战。

解决方案

Session Smart SD-Branch 是以服务为中心的高级网络解决方案，可将 SD-WAN 提升到全新水平。这款完全基于软件的解决方案可以降低成本和复杂性，从而消除困扰传统 WAN 和老旧 SD-WAN 解决方案的中间设备和 VNF 蔓延。

优势

- 支持 WAN 优化和智能路由功能，确保为不同的应用和服务提供优异性能和高品质服务
- 降低成本和复杂性，消除中间设备和 VNF 蔓延
- 随附 SASE 功能，例如基于会话和以服务为中心的路由、动态全局发现以及基于身份的接入和管理控制
- 在云或数据中心资源之间自动分配分支机构工作负载

数字化转型从根本上重塑了企业流量，并且为分支机构的网络规划者带来了性能、安全性和服务质量方面的挑战。在全球范围内，很多企业都在采用基于云的应用和服务来降低基础架构的成本和复杂性，从而提升企业敏捷性，并推进数字化转型。根据 RightScale 2019 年的行业调查，目前有 79% 的企业工作负载在云端运行，其中 46% 在私有云中，33% 在公共云中。

为支持传统企业应用和服务而设计的旧有分支机构网络并不适合云优先 IT 环境。现代企业需要现代化的企业网络——一种采用全新设计、适应性强的应用感知型网络，能够处理当今多样化的工作负载和动态数据流。

Juniper® Session Smart™ SD-Branch 是一款以服务为中心的先进解决方案，其消除了传统分支机构网络和旧有 SD-WAN 解决方案固有的效率不彰和成本限制问题。这款解决方案将 SD-WAN 的优势扩展到分支机构 LAN，并将集中管理、可编程性和控制与即插即用安装相结合，从而支持新的软件定义分支机构。这为当今的数字业务提供了快速、安全、可靠的分支机构连接，可以产生突破性的经济效益，实施起来也十分简便。

挑战

数字化转型改变了企业提供应用和服务的方式，并从根本上重塑了企业的流量。一直以来，大多数企业都将应用托管在位于核心位置的企业数据中心。企业通过 MPLS 网络或专用 WAN 来连接各分支机构，从而实现对这些分支机构的严密监控。大多数关键业务应用流量被局限在企业网络内部，而外部流量（Web、电子邮件、VoIP 等）通常会通过企业网络回传并安全移至互联网。

在新的云优先 IT 模式下，应用和服务都托管在公共云和私有云（以及企业数据中心）中，而且大多数分支机构流量不再局限于企业内部。相反，大量的关键业务应用流量会通过最佳公共互联网连接进行流动，这会让企业缺乏有效的可见性和控制力。

为支持传统企业应用和流量模式而设计的旧有中心辐射型分支机构网络无法适应主导现代企业的动态工作负载和多样化数据流。但新的云优先 IT 模式会给企业网络架构师带来各种性能、安全性和可用性方面的挑战。

性能

当今的企业会利用各种基于云的应用和服务，而这些应用和服务具有不同的特征和服务质量 (QoS) 要求。统一通信、协同解决方案和 Web 会议服务等部分应用对带宽要求很高，对延迟也很敏感。客户关系管理 (CRM) 和供应链管理 (SCM) 解决方案等其他应用对数据包丢失和延迟的容忍度会稍高一些。网络架构师必须找到对流量进行优先级排序、规划和高效路由的方法，以便为正确的应用提供正确的服务级别协议 (SLA)。

安全性

网络犯罪分子和恶意的内部攻击者可能会利用公共和私人数据网络来窃取机密信息或破坏关键的 IT 系统和服务。网络规划者必须引入强大的安全系统和实践来保护数据隐私，还要保护企业和云基础架构免受拒绝服务 (DoS) 攻击和其他威胁，同时确保不会降低性能、损害用户体验或使操作复杂化。

可用性

分支机构连接故障会扰乱关键业务应用，降低工作人员的工作效率，并影响最终效益。规划者必须确保在发生链路故障或 ISP 中断的情况下能够持续访问任务关键型应用和服务。

成本

传统的分支机构网络产品和旧有 SD-WAN 解决方案本身就十分昂贵、复杂，无法满足数字时代日益增长的性价比和敏捷性要求。旧有 SD-WAN 解决方案使用服务链来路由流经多个虚拟网络功能（防火墙、IPS/IDS、WAN 优化器等）的流量，但每个虚拟网络元素都会被实例化为独特的虚拟化网络功能 (VNF)，这会消耗 CPU 和内存资源。因此，旧有 SD-WAN 解决方案需要高密度的多核系统，而对于大多数分支机构而言，这类系统的价格过于昂贵。

中间设备蔓延

许多企业依赖于一系列专用的分支机构网络和安全解决方案（路由器、防火墙、IPS/IDS 设备、VPN 设备等）来提供安全可靠的连接。大量中间设备会产生各种令人头疼的问题，包括：

- 漫长、拖沓的部署流程 — 每个中间设备都需要经过独立安装、配置和部署，这是一种耗时的资源密集型工作方式，需要具备现场专业知识。
- 效率低下的“转椅式”管理 — 每个设备都具有独特的管理界面和 API。引入新的应用、扩大容量或排除故障可能需要大量人工操作，不仅易于出错，而且涉及多个不同的 CLI 或元素管理系统。

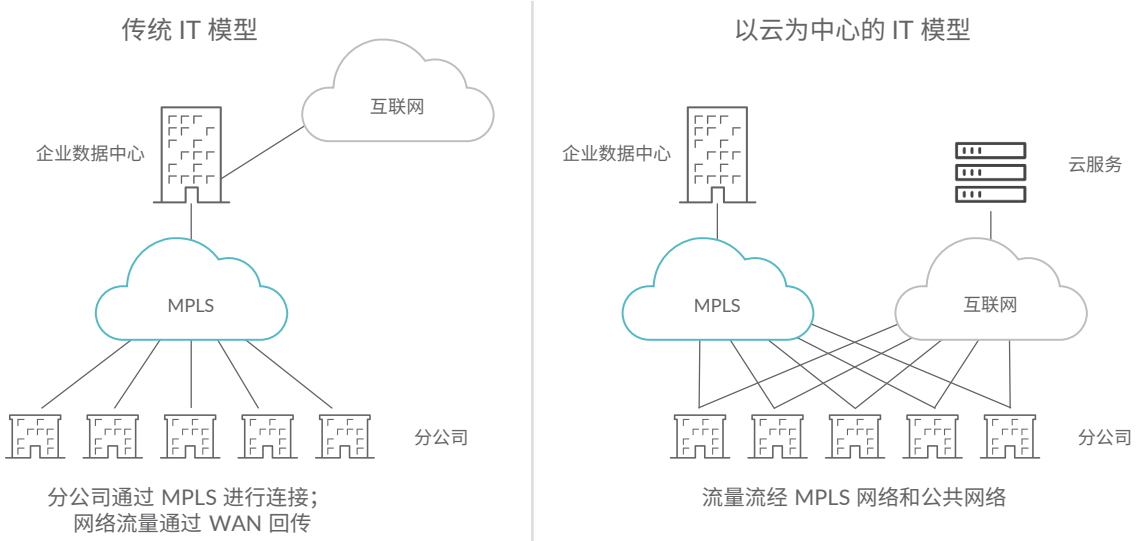

图 1：传统分支机构模型与云优先分支机构模型对比

- 复杂的后勤工作 — IT 团队经常被迫与多个供应商合作，才能完成产品采购、技术支持和软件升级工作。每个供应商都有各自的服务计划和软件维护时间表。而且，产品互操作性问题和兼容性问题会导致供应商之间发生争吵，相互指责。

瞻博网络 Session Smart SD-Branch 解决方案支持以身份为中心的安全接入服务边缘

Session Smart SD-Branch 是以服务为中心的高级网络解决方案，可将 SD-WAN 提升到全新水平。这款完全基于软件的解决方案可以降低成本和复杂性，从而消除困扰传统 WAN 和老旧 SD-WAN 解决方案的中间设备和 VNF 蔓延。这款解决方案还可以将软件定义 WAN 的优势一直扩展到分支机构 LAN，形成一个新的 SD-Branch。

正如 IDC 所指出的那样，“SD-WAN 是 SD-Branch 的基础组件。支持 SD-WAN 的虚拟化路由器是部署在 SD-Branch 环境中的最常见功能。当企业将其他虚拟网络功能与 SD-WAN 搭配使用时，便会形成 SD-Branch。”

Session Smart SD-Branch 解决方案将多种网络功能整合到单一 VNF 实例上，该 VNF 实例会在低成本的现成商用 (COTS) 平台上运行。企业可以基于策略在边缘和/或云端执行网络功能，以满足多样化的业务要求或应用需求。例如，来自一家企业组织的流量可以通过边缘的有状态防火墙进行引导，而来自另一家企业组织的流量可以通过运行在 Azure 或 AWS 上的新一代防火墙 (NGFW) 进行路由。

Session Smart SD-Branch 提供 Gartner 称之为“以身份为中心的安全接入服务边缘 (SASE) 架构”的网络组件。这款解决方案在靠近用户和连接端点的网络边缘监管流量，可以实现卓绝的速度、效率和经济性。

SASE 的基本功能包括：

- 基于会话的路由 — 瞻博网络 Session Smart 路由器可以像防火墙一样执行针对会话（而非个别数据包）的操作。
- 以服务为中心的路由 — Session Smart 路由器是围绕用户使用的应用进行建模而设计的。以服务为中心的网络是一种自上而下配置路由基础架构的方法。管理员不是使用内部网关协议 (IGP) 进行路由交换，也不使用访问控制列表 (ACL) 来限制访问，而是描述网络内的服务和网络内允许访问每个服务的组。动态全局发现 — 要想让 SASE 真正取得成功，网络必须能够动态检测服务所在的位置，以便向这些服务提供有效的会话。服务和拓扑交换协议 (STEP) 使 Session Smart 路由器能够与这些服务交换服务和连接信息。
- 基于身份的接入和管理控制 — Session Smart SD-Branch 可以在中央策略服务器的指示下，在边缘建立精细的、基于身份的接入和管理控制。

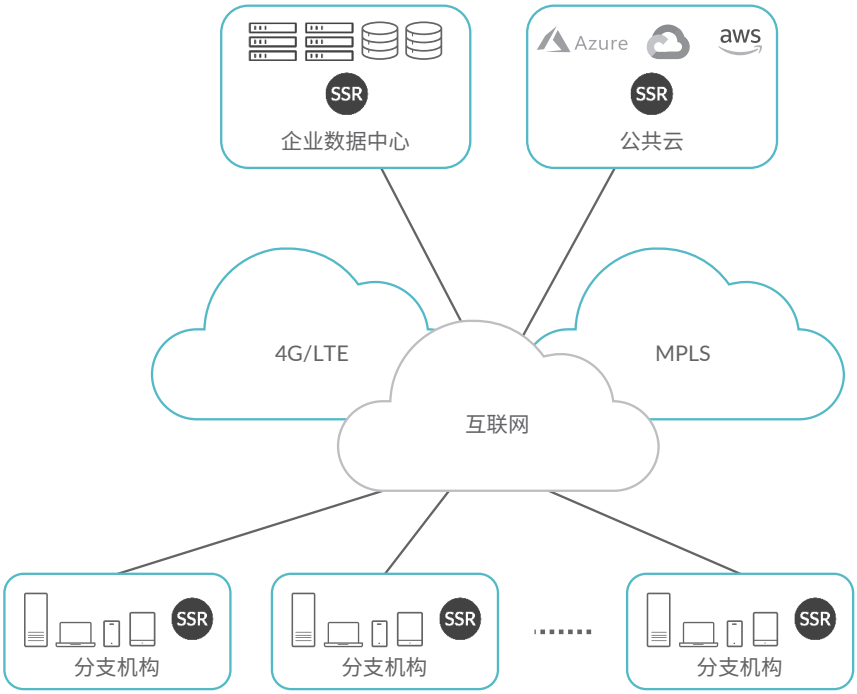

图 2：瞻博网络 Session Smart SD-Branch 连接

Session Smart SD-Branch 解决方案是当今分布式数字业务的理想选择，可为云优先 IT 模式提供敏捷、安全、有弹性的分支机构连接。这款解决方案能够消除旧有分支机构网络解决方案固有的效率不彰和成本限制等问题，提供具有应用感知能力的灵活网络交换矩阵，进而为以云为中心的关键业务应用和服务提供优异的性能、安全性和可用性。

功能与优势

性能

Session Smart SD-Branch 支持各种 WAN 优化和智能路由功能，可确保为不同应用和服务提供优异性能和高品质服务。精细化的 QoS 控制可让网络管理员有效率地进行流量规划和优先级安排，以便为不同的数据流执行不同的 SLA。创新的应用感知型路由可根据管理型定义的策略和实时网络状况，智能地引导流量，从而在正确的时间为适当的应用自动选择合适的网络路径（MPLS、4G、互联网）。服务器负载平衡功能可跨云端或数据中心资源自动分配分支机构的工作负载，进而优化应用性能。独特的无损应用交付功能可提高 WAN 的带宽利用率，助您提升低容量分支机构连接的性能。

安全性

Session Smart SD-Branch 可以保护应用和基础架构，防止数据丢失和恶意攻击。固有的安全功能包括“拒绝所有”（零信任）路由、第三层/第四层 DoS/DDoS 防御以及网络地址转换 (NAT) 和 VPN 功能。这种开创性的安全矢量路由 (SVR) 方法提供强大的数据安全性，而没有像 IPsec 这样的传统加密协议的开销（与 IPsec 相比，SVR 将协议开销减少了 30% 以上）。无隧道架构还为网络管理员提供对个别流量的全面可见性，可让他们高效监测端到端会话，评估服务质量并排除故障。

Session Smart SD-Branch 通过技术整合以及将网络和安全运维进行统一的集中化管理，从根本上简化了分支机构 LAN 的实施和安全性。这款解决方案与 Genians 和 PacketFence 等主流网络接入控制 (NAC) 解决方案相集成，可在中央策略服务器的指示下自动发现端点并在边缘实施基于身份的精细化接入和管理控制。该解决方案还能与 Palo Alto Networks、Zscaler、Seceon 和其他基于云的安全服务进行无缝服务功能链集成，从而提供卓绝的可扩展性和最终选择。

可用性

Session Smart SD-Branch 提供持续连接，而不像传统的分支机构网络解决方案那样需要昂贵的热备用隧道。在链路故障或网络中断时，这款解决方案会始终如一地将流量无缝重定向到备用路径上，而不会中断会话或降低应用性能。不仅如此，企业还能可以使用服务器负载平衡功能跨数据中心或可用性区域分配工作负载，为任务关键型服务提供业务连续性 (BC) 和灾难恢复 (DR)。

这款解决方案支持全自动部署 (ZTP) 和单一管理平台 (SPOG) 集中管理，可简化安装、管理和维护工作，非常适合部署在无人值守的远程站点。

下表总结了 Session Smart SD-Branch 相对于其他解决方案在关键分支机构网络要求方面的一些优势。

表 1：Session Smart SD-Branch 与传统 WAN 和旧有 SD-WAN 对比

要求	传统 WAN 与旧有 SD-WAN	Session Smart SD-Branch
低成本分支机构平台	特殊用途的中间设备会增加成本和开销。旧有 SD-WAN 需要昂贵的服务器来支持多个专用 VNF。	Session Smart SD-Branch 将所有网络功能整合到单一的 VNF 上，该 VNF 可在成本较低的 COTS 或白盒服务器上运行。
易于启动和运维	每个中间设备都有不同的 CLI/EMS/API。添加/移动/更改和故障排除需要大量人工操作，不仅费时，而且容易出错。	统一管理、自动设备发现、ZTP 和升级简化了部署和管理。
高安全性	隧道叠加能够保障数据隐私，但会限制可见性和控制，而且会损害性能。	安全矢量路由可以在保护数据隐私的同时实现精细化流量管理和可见性。
特定于应用的服务保证	隧道叠加抑制了流量管理，并阻止了特定于应用的 SLA。	精细化的流量管理和应用感知路由可以实现特定于应用的、基于策略的 SLA。
持续连接	闲置的热备用隧道成本高、效率低。	多路径会话迁移提供具成本效益的保护，可防止链路故障和 ISP 中断。服务器负载平衡为关键应用提供业务连续性/灾难恢复。
通过低速链路实现最佳性能	高开销的隧道协议会浪费带宽，影响延迟敏感型应用的性能。	安全矢量路由可将协议的开销降到最低。无损应用交付优化了带宽利用率，提高了应用性能。

总结 — 适用于当今数字业务的敏捷、安全且有弹性的分支机构连接

企业必须重新设计分支机构网络的架构，充分支持当今基于云的应用和服务。传统的分支机构网络设备和旧有 SD-WAN 解决方案专为支持传统的企业 IT 架构和流量而设计，其高昂的成本与复杂性并不适合当今的数字时代。

瞻博网络 Session Smart SD-Branch 通过整合功能、消除技术无序蔓延及大幅简化运维来削减分支机构网络支出并降低复杂性。作为以身份为中心的 SASE 架构的一部分，这款解决方案融合了网络系统和网络安全功能，在靠近最终用户的网络边界实施策略。自动发现功能和 ZTP 可以轻松启用服务并推出新应用，无需上门服务或现场专业知识。

Session Smart SD-Branch 解决方案提供以服务为中心的灵活网络交换矩阵，可满足新的云优先 IT 模式对性能、敏捷性和弹性的更高要求。这款解决方案还为新一代分支机构应用奠定了基础，帮助企业提升自动化程度、提高生产力、改善业务绩效。

后续举措

如需了解 Session Smart SD-Branch 如何帮助贵组织简化分支机构网络、加速数字化转型并改善业务成果，请联系您的瞻博网络客户经理或访问 www.juniper.net。

关于瞻博网络

瞻博网络将简单性融入到全球互联的产品、解决方案和服务之中。通过工程创新，我们消除了云时代网络的限制和复杂性，可应对我们的客户和合作伙伴日常面临的严苛挑战。在瞻博网络，我们坚信，网络是分享知识和实现人类进步的资源，它将改变这个世界。我们致力于以开创性的方式提供安全、自动化且易于扩展的网络，从而满足业务发展的需求。

公司和销售总部
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
电话： 888.JUNIPER (888.586.4737)
或 +1.408.745.2000
传真： +1.408.745.2100
www.juniper.net

亚太地区及欧洲、中东和非洲地区总部
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
电话： +31.0.207.125.700
传真： +31.0.207.125.701

JUNIPER NETWORKS | Engineering Simplicity