JUNIPER NETWORKS | Engineering Simplicity

白皮书

通过瞻博网络 SESSION SMART SD-WAN 实现 SASE

为当今的云时代网络保驾护航

目录

执行摘要

Gartner 将安全接入服务边缘 (SASE) 定义为一种转型技术。这项技术将软件定义广域网 (SD-WAN) 和网络安全的元素整合到单一云托管套件中。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。

在认识到安全性必须完全整合到网络中之后，Juniper® Session Smart™ SD-WAN 解决方案开始提供作为架构固有组成部分的内置安全功能。此外，基于服务的路由可确保会话根据身份和环境按照实时策略交付给相关方。这样可以确保以云为中心的现代化数字业务能在任何地方为用户和设备提供安全接入，而这正是 SASE 的关键要求。

简介

随着企业对于云技术趋之若鹜、物联网 (IoT) 盛行、用户热衷于移动应用，加上各种应用需要更高级别的响应能力，指望在传统模式下将安全性固化在网络上的某些点来保障安全显然不切实际。

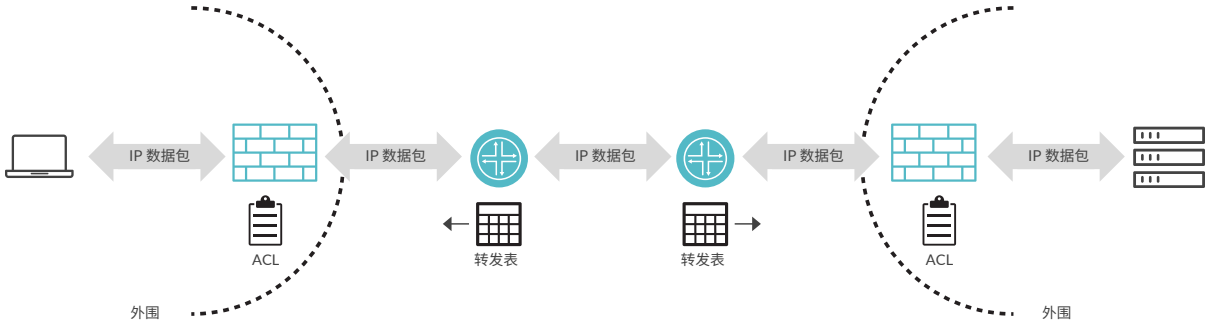


图 1：传统安全模式

独立分布式防火墙

保护用户和数据的传统做法是在外围设置防火墙。这就需要在所有位置部署防火墙，包括云端、数据中心和桌面等。然而，随着自带设备 (BYOD) 和云技术的盛行，边界变得越来越模糊，用户数据会驻留在软件即服务 (SaaS) 应用、手机、笔记本电脑和平板电脑中。这些设备没有固定的使用地点，因而无法定义其边界。无处不在的独立防火墙会阻碍为云端提供支持，并且已经不敷所需。虽然分散在各个位置的服务链防火墙虚拟化网络功能 (VNF) 无需使用单独的设备，但会遇到相同的问题。

集中式防火墙

另一种方法是将所有来自各种移动设备的流量通过 VPN 回传到数据中心，这种方法是在用户开始使用移动设备之后才流行起来的。在这里，流量在被发送到目的地之前可以经由大型集中式防火墙进行清理。这需要在数据中心部署昂贵的大型设备来管理所有流量。这种方式会增加延迟，进而造成用户体验不佳，而且还会阻碍云和 SaaS 模式的有效运行。

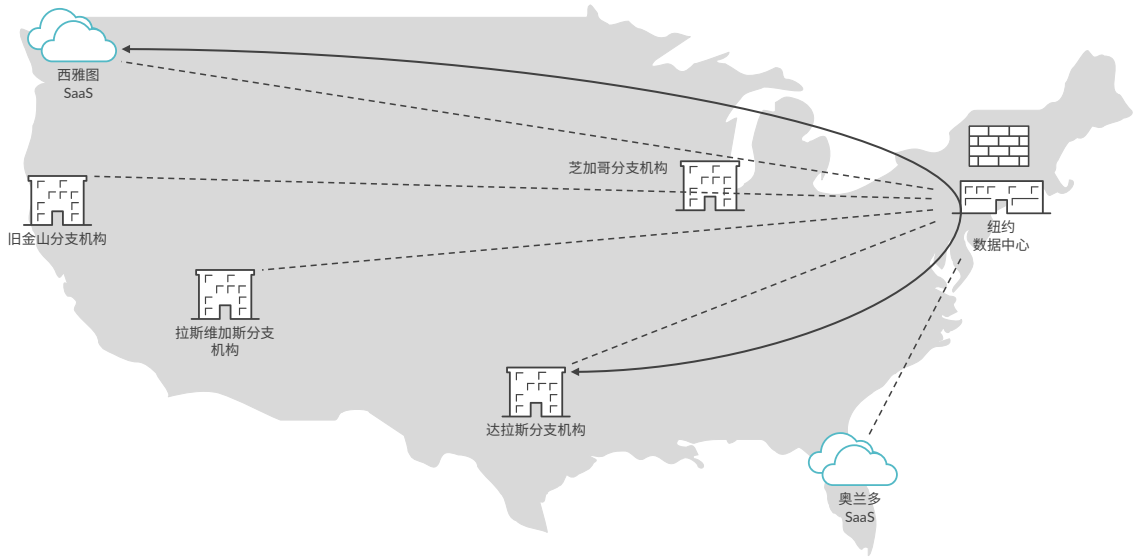


图 2：通过 VPN 将流量回传到数据中心会损害用户体验

基于云的防火墙

提供网络安全的一种主流方法是将来自各种设备的所有流量发送到由基于云的网络安全提供商托管的防火墙。这样用户便可将自己设备上的数据发送到最近的云提供商托管位置，而不是中央数据中心。虽然这种方法可以缩短靠近用户出行地区之托管设施所在地的延迟，但要向云提供商支付高昂的数据清理费用。此外，这种方法无法采用动态策略，因为用户或设备的任何变化都需要与云提供商协调。

Gartner 在其《云环境网络安全的未来》报告中指出，“我们需要转变思路，将检测引擎和算法部署在最靠近实体的位置，而不是将各种实体的流量强制（通过‘往返流动’）传送到数据中心设备内置的检测引擎中。”

除了传统安全模式引发的问题外，攻击者变得越来越老练，数据加密强度也越来越高，使之难以清理。隧道可以绕过安全解决方案 [RFC 6169]，而用户需要更好的响应能力。临时性的修补程序、协议扩展、调整和应对措施会造成系统环境错综复杂，导致大量服务中断，使企业成本不断攀升 [IETF 102]。

提供 SASE

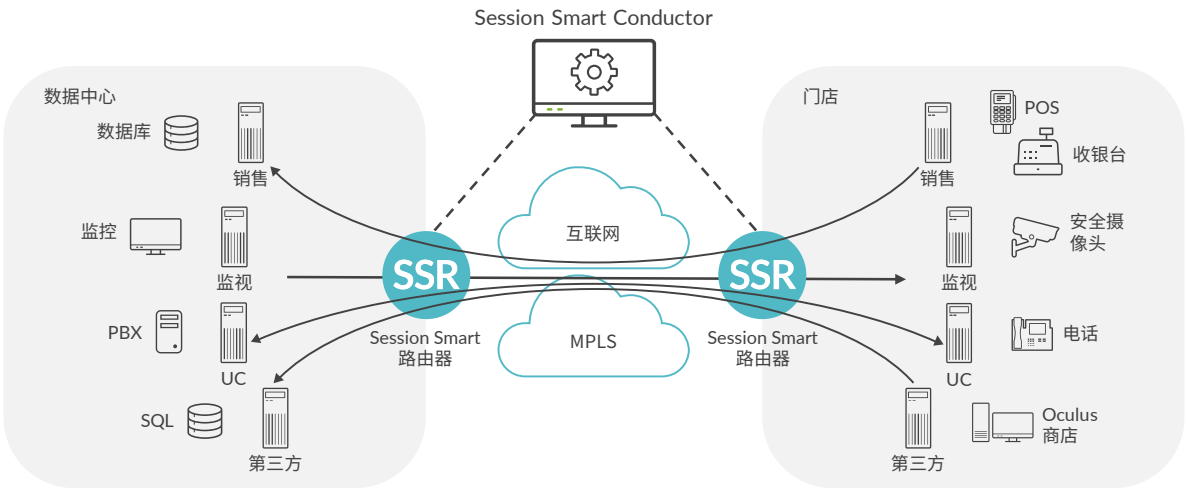
真正的 SASE 要求最靠近用户及用户设备的网络设备能够发现端点、端点权限并保护流量，从而提供动态安全服务。瞻博网络 Session Smart SD-WAN 解决方案的内置功能可在网络中的每台路由器上提供这些安全服务。

基于会话的路由

瞻博网络 Session Smart 路由器采用基于会话的技术，这意味着它可以像防火墙一样执行针对会话（而非个别数据包）的操作。这项技术具有与生俱来的方向性，使路由器能够判断会话发起者及数据传输方向。管理员可以根据任何给定的身份验证标准指定允许哪些会话。一旦路由器确认来源有效，系统便会将会话放置在一个允许租户根据权限访问特定目标的租户位置。与安全性、加密、身份验证、服务质量 (QoS)、负载或其他标准相关的会话相关联的策略也是在每个会话的基础上单独决定的。这就实现了精细化的超分段，而且可以确保安全访问，因为任何未经授权的会话只要通过网络中的第一个路由器便会被丢弃。Session Smart 路由器还可以自动识别会话，并将会话放在不同的类别或租户中，从而根据管理员的需求给予不同的处理。

以服务为中心的路由

Session Smart SD-WAN 解决方案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。这样可以让网络将会话路由到服务而不是 IP 地址。在路由器判断出会话有效之后，便会将这些会话定向到打算使用的目标服务。这可以确保仅将有效会话发送到可根据负载和流量状况使用这些会话的服务。在服务不明的情况下，路由器不需要判断用户或设备的身份，只需转发数据包，并将这些数据包与目标 IP 地址关联起来。



无叠加网络 | 超分段 | 零信任安全性

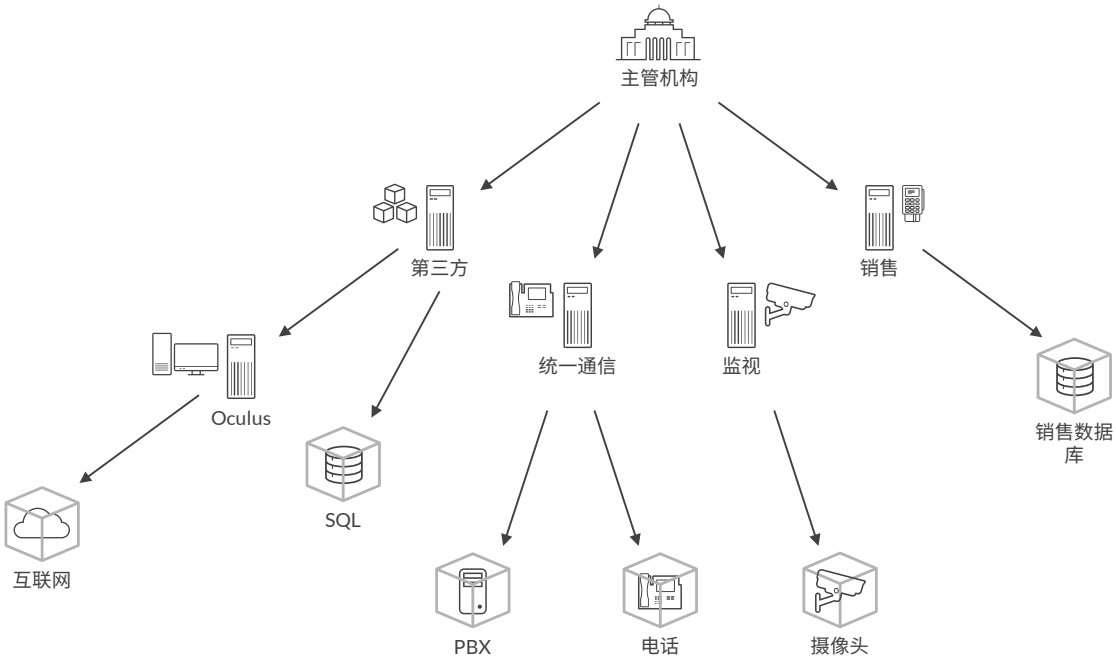


图 3：瞻博网络 Session Smart SD-WAN 以服务为中心的路由

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) 使用基于会话的服务导向型范例，使 Session Smart 路由器能够将服务和连接信息交换到相关服务。网络管理员通过定义服务来呈现专为消费者提供定制网络的功能。STEP 支持将此服务功能交换到所有路由器以及将可访问性和要连接的其他参数交换到这些服务。这使得网络管理员能够提供基于意图的应用导向型 SD-WAN 解决方案，确保解决方案遵循业务逻辑并使用实时信息来帮助路由器决定如何连接应用。动态服务发现使企业能够根据负载启动和关停现有服务的新位置、添加新服务以及删除或修改现有服务。这项功能可缩短上市时间并支持弹性增长。

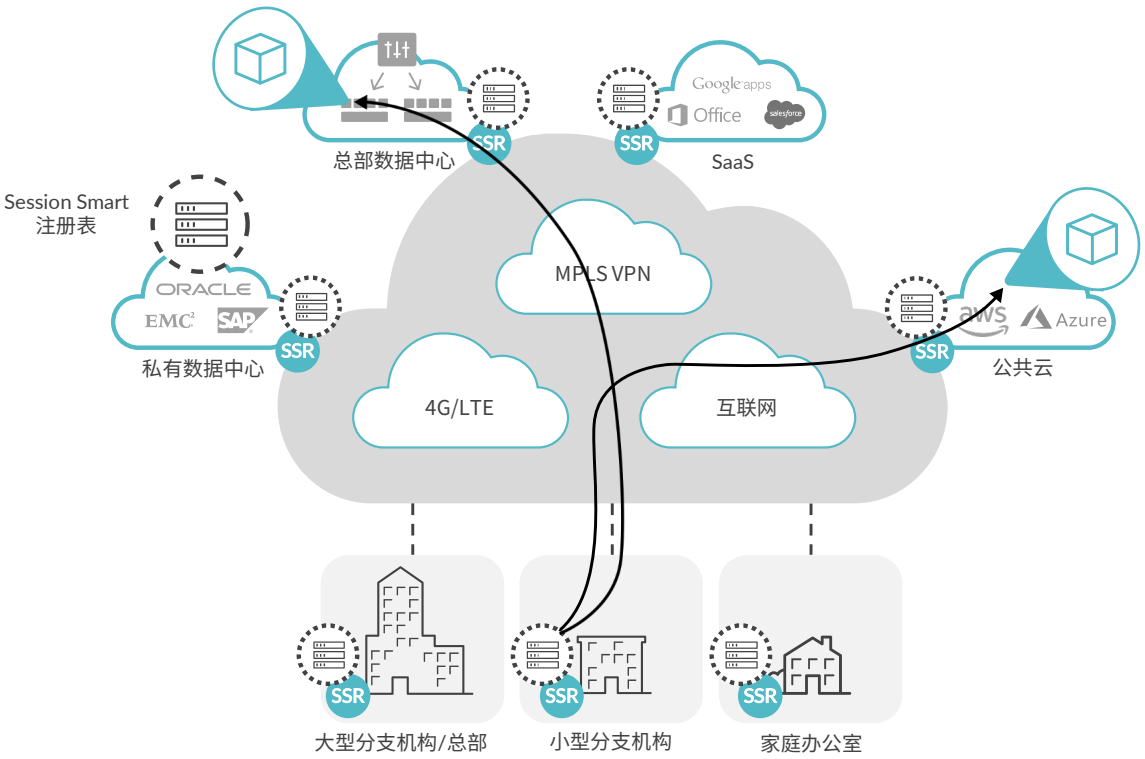


图 4：Session Smart 路由器支持动态服务发现

STEP 能够以任何其他协议都无法实现的独特方式来执行动态服务发现。这种协议可以使用前缀、协议和端口的精细度来定义服务。这意味着在当今的虚拟或容器化环境中，计算实例上的每个应用都可以有其自己的服务发现。如果无法访问应用，该服务将从 STEP 报告中退出，其他路由器将停止向相关服务器发送数据包。

当今网络中的路由器毫无保留地信任周围设备以及从这些设备收到的信息。网络无法隔离恶意用户或移除这种信任。STEP 则能通过区块链建立信任以共享密钥并验证所有权。

成为防火墙

防火墙的部署方式可能已经过时；然而，防火墙的功能不会过时。每一台 Session Smart 路由器都是一个经过 ICSA 认证的网络防火墙，并且具备支持 SASE 的其他功能。

这款路由器可以对通过的任何数据包进行加密/解密以及身份验证。它们支持自适应加密，可动态检测加密会话并防止双重加密，而且还通过了 FIPS-140-2 认证。这款路由器可以像防火墙一样，遵循默认拒绝模式。所以，如果某个会话未关联任何策略，便会被丢弃。这可以促使管理员明确地为有效会话定义策略。

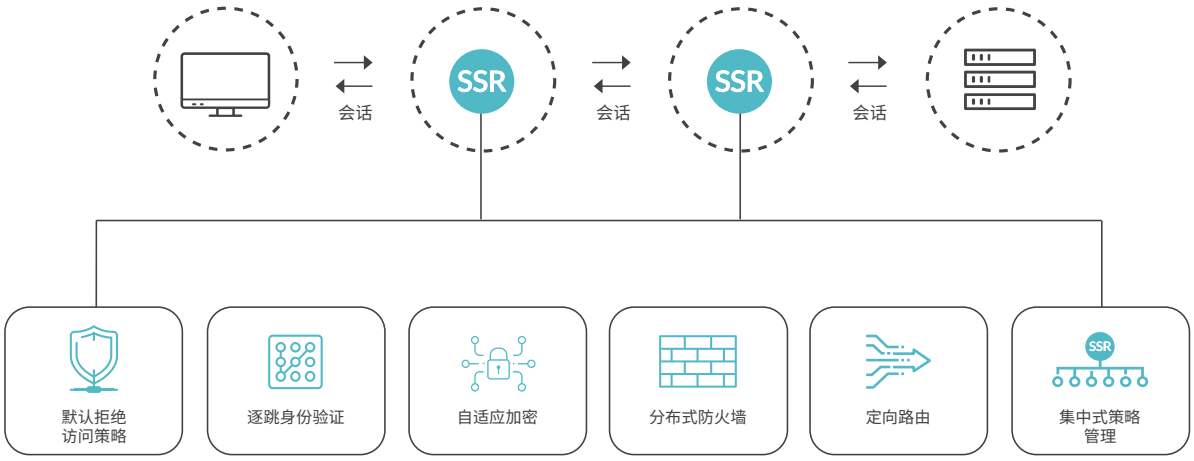


图 5：Session Smart SD-WAN 安全功能

Session Smart 路由器本身支持网络防火墙功能。不过，若有服务需要新一代防火墙 (NGFW) 来处理时，Session Smart 路由器仍可搭配瞻博网络 SRX 来满足这项要求。

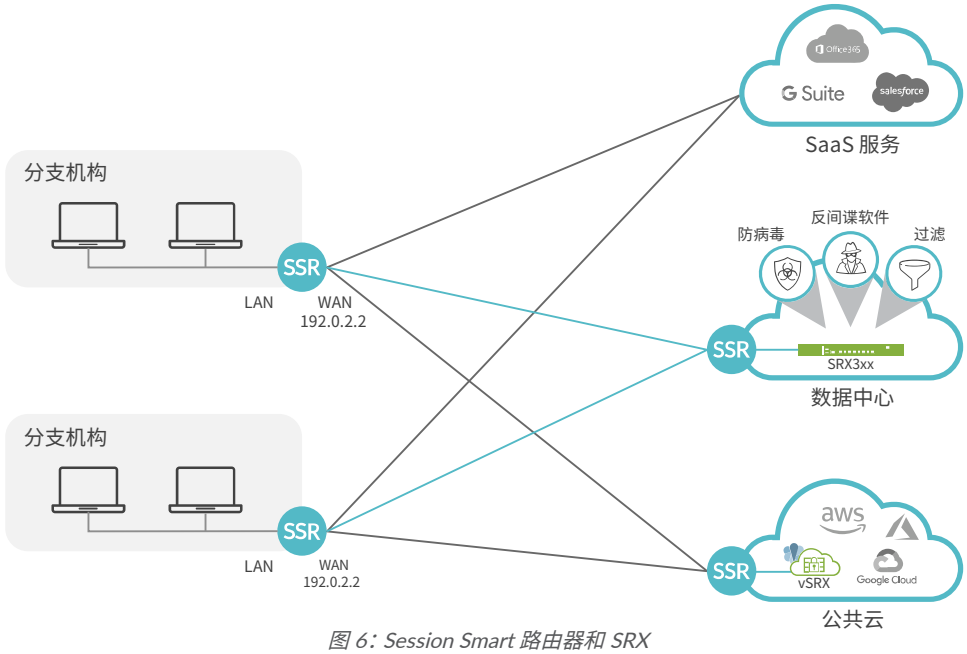


图 6：Session Smart 路由器和 SRX

在这种模式下，若分支机构中的某项服务需要新一代防火墙来处理时，分支机构中的 SSR 便会将数据包路由到数据中心内的 SSR 或云中的 SSR。将数据中心/云中的 SSR 与 SRX 相结合的服务将具备所需的新一代防火墙处理能力。

总结

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。真正的 SASE 要求网络中的每台设备都能够识别访问策略，可以发现身份的变化，对会话进行加密和身份验证，抵抗攻击并实现安全性。

在服务不明的情况下，路由器不需要判断用户或设备的身份，只需转发数据包，并将这些数据包与目标 IP 地址关联起来。支持 STEP 的 Session Smart 路由器使网络管理员能够提供基于意图的应用导向型网络解决方案，确保解决方案遵循业务逻辑并使用实时信息来帮助路由器决定如何连接应用。动态服务发现使企业能够信心十足地根据负载启动和关停现有服务的新位置、添加新服务以及删除或修改现有服务，从而缩短上市时间并支持弹性增长。

瞻博网络 Session Smart SD-WAN 解决方案打造出一种兼具默认拒绝路由、基于策略的转发、监管以及内置企业网络防火墙功能的 SASE 网络。瞻博网络 Session Smart 路由器以服务为中心，基于会话且具备与生俱来的方向性。Session Smart SD-WAN 解决方案支持端到端分段和零信任安全性，使企业能够对每种流量流进行隔离并提供差异化的安全功能和服务，从而将 SASE 的愿景变为现实。

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。我们致力于开创具有突破性的方式，提供自动化、可扩展且安全的网络，以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