vSRX 虚拟防火墙

产品概述

vSRX 虚拟防火墙提供全面的虚拟防火墙解决方案，包括适用于服务提供商和企业的高级安全功能、强大的网络和自动化虚拟机生命周期管理功能。借助 vSRX，安全专业人员能够在高度动态的环境中部署和扩展防火墙保护。

要下载 vSRX 试用版本，包括 IPS、AppSecure 和 UTM 等高级安全服务，请访问 www.juniper.net/cn/zh/dm/free-vsrx-trial/。

产品说明

为了更快、更高效地提供服务，数据中心越来越依赖服务器虚拟化。然而，虚拟化数据中心带来了新的难题 — 除了确保实物资产的安全，还有一些额外的安全事项需要考虑。

在虚拟化数据中心，虚拟机 (VM) 可以频繁地增加、移动和更改，呈现高度动态和弹性趋势。这会导致以下能力变得复杂：向 VM 实例化附加安全策略，并随 VM 移动跟踪安全策略，以确保持续的监管合规。简而言之，虚拟化带来的动态和灵活特性很容易导致失去在实体世界被视作理所当然该具有的可见性和控制能力。

网络和安全专业人员必须采取审慎的平衡做法，既向组织提供虚拟化和云技术的益处，同时又不削弱组织的安全。为了解决这种挑战，我们需要一个新的解决方案 — 既要能密切关注并应对不断发展演变的威胁，同时又要能适应虚拟化环境和云环境的灵活性和可扩展性，而且不能牺牲可靠性、可见性和控制能力。

瞻博网络利用 vSRX 虚拟防火墙，将屡获殊荣的瞻博网络® SRX 系列服务网关的功能扩展到虚拟世界，很好地解决了这些难题。vSRX 由 Juniper Networks Junos® 操作系统提供支持，提供一个完整的一体化虚拟安全解决方案，包括适用于服务提供商和企业等组织的 L4-L7 高级安全服务、强大的联网以及自动化生命周期管理能力。

借助 vSRX 的自动化调配能力，网络管理员和安全管理员可以快速高效地调配和扩展防火墙保护，以满足虚拟化环境和云环境的动态需要。通过将 vSRX 与 Junos Space® Security Director 的强大功能相结合，管理员可以从一个集中式公共平台大幅改进实体资产和虚拟资产的策略配置、管理及可见性。

对于那些在软件中部署以服务为导向的应用程序的服务提供商和组织而言，vSRX 的虚拟化网络和安全服务组合支持各种网络功能虚拟化 (NFV) 用例。vSRX 还支持 Juniper Networks Contrail、OpenContrail 和其他第三方解决方案，并且可以直接或通过富 API 与诸如 OpenStack 等其他新一代云编排工具进行集成。

表 1： vSRX UTM 的功能与优势

功能	功能说明	优势
防病毒	• 声誉良好的基于云的防病毒功能，可检测并拦截通过 POP3、HTTP、SMTP 和 FTP 协议传播的间谍软件、广告软件、病毒、键盘记录器和其他恶意软件。 • 与反恶意软件技术领域内的领导者 Sophos Labs 合作提供服务	• 由权威的防病毒专家提供复杂的恶意软件攻击防护。恶意软件攻击可能导致代价高昂的数据泄露和生产力下降
Web 过滤	• 增强的 Web 过滤功能，包括与领先的 Web 安全提供商 Forcepoint 合作提供的广泛的类别选项（90 多个类别）和一个实时评分卡	• 防范生产力下降和恶意 URL 的影响，并帮助维护业务必要信息流的网络带宽
内容过滤	• 根据 MIME 类型、文件扩展名和协议命令，有效过滤入站内容和出站内容	• 防范网络上无意或恶意的文件传输及恶意内容，最大限度地减少数据破坏或数据泄露的风险
反垃圾邮件	• 与 Sophos Labs 合作提供的多层垃圾邮件防护、最新的网络钓鱼 URL 检测、基于标准的 S/MIME、Open PGP 和 TLS 加密、MIME 类型以及扩展名拦截器	• 使用复杂的电子邮件过滤和内容拦截器，防范通过社交网络攻击所实施的高级持续威胁，以及最新的网络钓鱼诈骗

架构和关键组件

高级安全服务

目前实施的非集成的传统系统都是围绕传统防火墙以及各个单独的设备和软件构建的，已不足以防范现今高深复杂的攻击。利用瞻博网络的高级安全套件，用户能够部署多种技术，以满足现代组织既独特又不断发展变化的需要并应对不断变化的威胁格局。实时更新确保技术、策略和其他安全措施始终保持最新。

vSRX 提供一套用途广泛且功能强大的高级安全服务，包括统一威胁管理 (UTM)、入侵检测与防御 (IDP) 以及通过瞻博网络 AppSecure 提供的应用程序控制和可见性服务。

统一威胁管理 (UTM)

vSRX 包括全面的内容安全功能，通过同类最佳的防病毒、反垃圾邮件、Web 过滤和内容过滤等功能来抵御恶意软件、病毒、钓鱼攻击、入侵、垃圾邮件和其他威胁。

入侵防御系统 (IPS)

vSRX 的 IPS 通过检查数据并采取行动，如：在攻击发展形成过程中以及在它们成功前拦截它们，或者在防火墙中创建一系列规则，来控制对 IT 网络的访问，由此保护系统免遭攻击。IPS 将瞻博网络的应用程序安全功能紧密集成到网络基础架构中，可以进一步减少威胁并增强对名目繁多的攻击和漏洞的防范。

表 2：vSRX IPS 的功能与优势

功能	功能说明	优势
有状态签名检查	仅对适当协议上下文所确定的网络信息流的相关部分应用签名。	最大限度地减少误报并提供灵活的签名开发。
协议解码	支持超过 65 种的协议解码以及 500 多个上下文以确保协议使用恰当。	通过精准的协议上下文来提高签名的准确性。
签名	提供 15,000 多个签名，可用于识别异常、攻击、间谍软件和应用程序。	准确识别攻击并且检测那些企图利用已知漏洞的行为。
信息流规范化	提供数据包重组、规范化以及协议解码。	系统通过使用混淆方法，击败那些企图绕过其他 IPS 检测的行为。
“零”日防护	为新发现的漏洞提供协议异常检测和当日防护。	网络已获得妥善保护，能够抵御任何新的攻击行动。
推荐策略	攻击签名被瞻博网络安全团队确定为一般企业要防范的关键点。	在确保最高级网络安全的同时简化安装和维护。
主动/主动的信息流监控	IPS 监控包括主动/主动 vSRX 机箱群集。	包括对主动/主动 IPS 监控的支持。
数据包捕获	IIPS 策略支持按规则进行数据包捕获日志记录。	用户可以对周围的信息流进行进一步分析并为保护目标而确定随后的步骤。

表 3：适用于 vSRX 的 AppSecure 的功能与优势

功能	说明	优势
AppTrack	按风险级别、区域、源地址和目标地址，对应用程序数据进行分析和分类。	跟踪应用程序使用情况，以辨识高风险的应用程序并分析信息流模式，由此改进网络管理和控制。
AppFW	创建应用程序控制策略，由此依据动态应用程序名称或组名来允许或拒绝信息流。	基于应用程序而非传统端口和协议分析，来增强安全策略的创建和执行。
AppQoS	根据管理员所设置的应用程序安全策略，来计量信息流并在信息流上加注标记。	根据应用程序信息和上下文，确定信息流的优先顺序并限制和决定带宽，由此提高整体性能。

AppSecure 所提供的应用程序可见性和控制

AppSecure 是适用于 vSRX 和 SRX 系列服务网关的下一代应用程序安全套件，它提供威胁可见性、保护、执行和控制。

无论是需要了解每日有多少用户访问诸如 Facebook 等基于云的应用程序，还是需要了解哪些应用程序在使用大部分带宽，AppSecure 均可提供强大的可见性和持续的应用程序跟踪。通过使用开放式签名，它可以监控、测量和控制独特的应用程序集，使它们与组织的业务优先事项紧密相联。

瞻博网络高级威胁防御

瞻博网络高级威胁防御 与 vSRX 集成，针对已知恶意软件和高级零日威胁提供动态的自动防御，几乎可以即时响应威胁（参见表 4）。

安全策略确定一个会话是否可以在一个区域发起并转发到另一个区域。vSRX 接收数据包并追踪每个会话、每个应用程序和每个用户。当 VM 在虚拟化环境或云环境内移动时，它仍将向 vSRX 发送数据包供处理，在安全模式中持续地进行通讯。

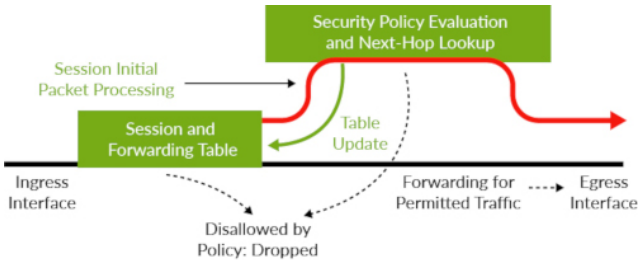

图 1：vSRX 基于会话的转发算法

高可用性 (HA)

vSRX 提供任务关键型可靠性，支持主动/主动和主动/被动模式均实现机箱群集。HA 功能为任何正在处理的连接以及横跨虚拟机管理程序的群集成员提供完全的状态故障转移。在群集中配置 vSRX VM 时，VM 将同步连接/会话状态和流量信息、IPsec 安全关联、网络地址转换 (NAT) 信息流、通讯簿信息、配置变更和其他项目。因此，在故障转移过程中不仅保存会话，而且安全性也保持完好无损。在一个不稳定的网络中，vSRX 还可减少链路摆动。

表 4：适用于 vSRX 的瞻博网络 ATP 的功能与优势

功能	优势
深度检测和分析	提取遭到入侵的文件并发送至云，以快速识别已知威胁，或者深度分析文件以查找深度隐匿的恶意软件。
即时识别以阻止攻击	即时识别恶意软件，并将检测到的恶意软件通报至 SRX 系列防火墙以阻止攻击。
具有丰富报告和分析工具的基于 Web 的门户	提供基于 Web 的界面，用于执行配置和产品更新等管理任务。还提供了一套丰富的报告和分析工具，用于了解威胁和遭到入侵的主机。
隔离系统和主机	分析功能使管理员和安全人员可分析和关联数据，从而识别遭到入侵的系统，并将信息发送到 SRX 系列防火墙以隔离这些系统。
Spotlight Secure 集成	与 Spotlight Secure 威胁情报服务相集成，将威胁信息级联到 SRX 系列防火墙，以便立即采取措施。
命令与控制 (C&C) 数据	向 SRX 系列防火墙提供 C&C 数据，防止遭到入侵的内部系统与这些设备进行通信。
电子邮件分析和补救	隔离恶意软件，避免电子邮件被用作攻击媒介。机器学习算法分析电子邮件流量，检测恶意附件，并在防火墙阻止文件。
威胁情报	使用强大的开放式 API 与第三方供应商无缝集成，为您提供多个威胁情报源，减少您的攻击面。

表 5：vSRX 服务网关的关键性能指标

性能和容量 [1]	VMware				KVM			
vCPU 数	2	5	9	17	2	5	9	17
内存	4 GB	8 GB	16 GB	32/64 GB	4 GB	8 GB	16 GB	32/64 GB
防火墙吞吐量，大数据包 (1514B)	9.5 Gbps	14 Gbps	73 Gbps	81 Gbps	14 Gbps	39 Gbps	68 Gbps	98 Gbps
防火墙吞吐量，IMIX	2.4 Gbps	4.1 Gbps	17 Gbps	27 Gbps	3.2 Gbps	14 Gbps	16 Gbps	27 Gbps
AES+GCM IPSec VPN 吞吐量 (1420B)	22 Gbps	4.2 Gbps	12 Gbps	13 Gbps	1.1 Gbps	7 Gbps	10 Gbps	16 Gbps
应用程序可见性和控制 [2]	2.4 Gbps	7.2 Gbps	21 Gbps	39 Gbps	3.3 Gbps	10 Gbps	1.9 Gbps	38 Gbps
IPS 建议的签名	2.3 Gbps	7.1 Gbps	18 Gbps	39 Gbps	3 Gbps	10 Gbps	1.9 Gbps	36 Gbps
每秒 TCP 连接数	55,000	166,250	351,250	537,660	69,000	239,380	360,000	612,660
最大并发会话数 [3]	512000	2M	4M	12/24M	512000	1M	1.5M	12/24M

[1] 全部性能数字都是"最多"，具体性能将取决于底层硬件配置（一些服务器配置可能会提供更优性能）。列出的性能、容量和功能均基于在 Junos OS 19.2R1 版本上运行 vSRX 且在理想测试条件下测得。实际结果可能因 Junos OS 版本和部署而异

[2] 吞吐量数字基于事务大小为 44KB 的 HTTP 流量测得。

[3] 最大并发会话数可能会增加，具体取决于 vSRX 的内存分配。有关详细信息，请访问 https://www.juniper.net/documentation/en_US/vsrx/information-products/topic-collections/release-notes/19.2/ topic-98044.html#jd0e107。

性能

客户历来需要在可扩展性与性能之间进行取舍和权衡。vSRX 解决方案经过优化，能够充分利用多个虚拟的 CPU，使虚拟环境中的数据包处理和整个吞吐量达到最大化。每个 vSRX VM 也有多个虚拟网络接口卡 (vNIC)，可以连接到各种虚拟网络，以同时保护多个网段。从虚拟结构内运作，vSRX 提供最佳的安全和性能—向虚拟化环境或云环境提供支持时所需的性能强大的安全性。

通过利用纵向扩展模式，vSRX 为客户提供升级其虚拟安全容量的灵活性，只需将最少两个以上 vCPU 的额外核心* 添加到同一实例即可升级，无需认证新实例映像。通过使用单个插槽中的 17 个 vCPU，vSRX 可实现高达 100 Gbps 的性能。

*核心数应为 2 的幂 + 1（即 2n + 1）

表 6：vSRX 系统要求

组件	规格			
CPU 核心	2	5	9	17
内存	4 GB	8 GB	16 GB	32 GB
磁盘空间	16 GB			
网络驱动程序 - VMware ESXi	Intel X710/XL710 或 X520/X540 上的 VMXNET3、SR-IOV	VMXNET3	SR-IOV（Mellanox ConnectX-3/ ConnectX-3 Pro 和 Mellanox ConnectX-4 EN/ConnectX-4 Lx EN）	
网络驱动程序 KVM	Intel X710/XL710 或 X520/X540 上的 Virtio、SR-IOV	Intel X710/ XL710 上的 Virtio、SR-IOV	Intel X710/XL710 上的 Virtio、SR-IOV，带 PCI 直通 SR-IOV（Mellanox ConnectX-3/ ConnectX-3 Pro 和 Mellanox ConnectX-4 EN/ConnectX-4 Lx EN）	

Junos Space Security Director

Junos Space Security Director 通过一个基于网络的既直观又集中的界面（它实现跨各个新兴风险矢量和传统风险矢量的执行），提供安全策略管理。作为 Junos Space 平台上的一个应用程序，Security Director 在整个网络内提供广泛的安全规模、具体策略控制及策略宽度。它帮助管理员快速管理状态防火墙、UTM、IPS、AppFW、VPN 和 NAT 的安全策略生命周期的各个阶段。

统一管理

通过利用 Junos Space Security Director 的强大功能，管理员可以从一个集中式公共平台大幅改进实体资产和虚拟资产的策略配置、管理及可见性。

主要功能与优势

- 通过提供一个具有状态数据包处理和应用层网关功能（采用虚拟机形式）的完整防火墙，确保多租户私有云环境和公共云环境的安全。
- 充分利用 SRX 系列服务网关的相同、一致、高级的安全和联网功能（IPsec VPN、NAT、QoS 和全部路由能力）
- 通过为一个综合的威胁管理框架集成强大的 UTM、IPS 及应用程序可见性和控制能力，来抵御日益复杂的威胁态势
- 通过使用开放的 RESTful API 支持与第三方管理和云编排工具的集成，由此提高管理的灵活性
- 通过使用 Junos Space Security Director，扩大对跨虚拟环境和非虚拟环境的防火墙安全策略配置与管理的可见性和控制
- 通过与 Contrail、OpenContrail 和其他第三方解决方案的集成，支持 SDN 和 NFV

在 Amazon Web Services 市场中提供

vSRX 可在 Amazon Web Services (AWS) 市场上获得，该产品提供了高级网络、应用程序安全以及与 AWS VPC、私有云和内部资源的安全 IPsec VPN 连接。借助 vSRX 3.0，您可以利用 AWS 的自动扩展功能动态增加容量，同时以尽可能最低的成本保持稳定、可预测的性能。通过使用 Junos Space Security Director，客户可在跨内部和 AWS VPC 分布的 SRX 系列服务网关上维护和管理一致安全策略。使用 AWS 上的 vSRX 的客户可自带 vSRX 许可证，也可通过基于用量的定价付款（按需购买，渐进扩展；按小时或按年）。

在 Microsoft Azure 市场中提供

您可以从 Microsoft Azure Marketplace 和 Microsoft Azure Government 获取 vSRX，该产品可为 Azure 虚拟网络提供安全的 IPsec VPN 连接和高级新一代安全功能。通过使用 Junos Space Security Director，客户可在内部和 Azure 虚拟网络中部署的 SRX 系列下一代防火墙上保持和管理一致安全策略。vSRX 在 Microsoft Azure 市场和 Microsoft Azure Government 上以“自带许可证 (BYOL)”模式提供。

在 Google Cloud Platform Marketplace 中提供

您可以从 Google Cloud Platform Marketplace 和 Google Cloud Government 获取 vSRX，该产品可为 Google 虚拟网络提供安全的 IPsec VPN 连接以及高级新一代安全和 UTM 安全功能。使用 Junos Space Security Director，客户可在内部和 Google 虚拟网络中部署的 SRX 系列新一代防火墙上管理和维护一致的安全策略。Juniper 在 Google Cloud Platform 和 Google Cloud Government 上提供自带许可（BYOL）以及“按需购买，渐进扩展”（PAYG）许可选项。

瞻博网络服务与支持

瞻博网络是高性能服务支持领域的领导者，致力于提供帮助您加速、扩展和优化高性能网络的各种服务。我们的服务可让您最大程度地提高运维效率，同时降低成本和风险，并更快地实现网络价值。瞻博网络通过优化网络来保持所需级别的性能、可靠性和可用性，以此确保卓越运维。有关详细信息，请访问 www.juniper.net/cn/zh/products-services/。

规格

下表重点列出了一些关键规格。请参见产品文档以获取完整列表。

表 7：vSRX 虚拟防火墙规格

协议	IP 地址管理	安全	SLA、测量和监控	虚拟机管理程序
• IPv4、IPv6、MPLS、ISO 无连接网络服务 (CLNS) • 静态路由 • RIPv2 +v1 • OSPF/OSPFv3 • BGP • IS-IS • 多播（互联网组管理协议、PIM、会话描述协议） • MPLS • VPLS	• 静态 • 动态主机配置协议 (DHCP) • 互联网 DHCP 服务器、DHCP 中继 • 地址转换 • 带有端口地址转换 (PAT) 的源 NAT • 静态 NAT • 带有 PAT 的目标 NAT • 持续的 NAT、NAT64 • 封装 • 以太网 • 1q VLAN 支持	• 防火墙 • 防火墙、区域、屏幕、策略 • 状态防火墙、无状态过滤器 • 网络攻击检测 • 屏幕拒绝服务 (DoS) 及分布式 DoS (DDoS) 保护（基于异常） • 重播攻击防护；防重播 • 统一访问控制 (UAC) • 以分段数据包保护为目的的 TCP 数据包重组 • 减轻暴力攻击 • SYN cookie 防护 • 基于区域的 IP 欺骗 • 畸形数据包防护 • VPN • 隧道（通用路由封装、IP-IP） • IPsec、数据加密标准 (DES)（56 位）、三重数据加密标准 (3DES)（168 位）、高级加密标准 (AES)（128 位+）加密 • 消息摘要 5 (MD5)、SHA-1、SHA-128、SHA-256 身份验证 • IPv6	• 实时性能监控 (RPM) • 会话、数据包及带宽使用情况 • IP 监控 • 日志 • 系统日志 • Traceroute • 广泛的控制功能和数据平面的结构化及非结构化系统日志管理 • Junos Space Security Director 支持 • 瞻博网络安全分析 • 瞻博网络高级观点解决方案支持 • 外部管理员数据库（RADIUS、LDAP、SecureID） • 自动配置 • 配置回滚 • 带按钮的救援配置 • 提交更改确认 • 供诊断程序使用的自动记录 • 软件升级 • J-Web • CLI	• VMware ESXi 5.5、6.0、6.5；KVM/QEMU： - CentOS 7.1 - Ubuntu 14.04、16.04、16.10 - RHEL 7.3 • Hyper-V 2012、2012R2、2016

订购信息

有关瞻博网络 vSRX 虚拟防火墙的更多信息，请访问 www.juniper.net/cn/zh/products-services/security/srx-series/vsrx，或者联系最近的瞻博网络销售代表。要获取 vSRX 免费试用版，请访问 www.juniper.net/cn/zh/dm/free-vsrx-trial/。

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。

Corporate and Sales Headquarters
Juniper Networks, Inc. 1133 Innovation Way
Sunnyvale, CA 94089 USA
电话：888.JUNIPER (888.586.4737)
or +1.408.745.2000
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V. Boeing
Avenue 240 1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
电话：+31.0.207.125.700

Juniper Networks | Engineering Simplicity