

# 新一代防火墙服务

## 产品概述

瞻博网络提供了丰富多样的高性能新一代防火墙，通过整合应用程序可见性、用户识别和深度内容检测功能，可以为安全基础架构提供无与伦比的细粒度控制。

### 产品说明

应用程序使用、用户行为和网络基础架构的不断变化造成了一种危险的局面 — 组织持续暴露在广泛的攻击范围内。而用户由于要访问在各种各样的设备上运行、数量在不断增长的应用，根本无暇顾及企业安全，从而导致该问题越发严峻。

您期待有一种全新的安全模式，既能抵御这些威胁，又能保证用户访问不同设备上的各种新应用。Juniper Networks® SRX 系列服务网关提供具备应用程序感知、用户身份和内容检测的集成式新一代防火墙 (NGFW) 保护服务。除 NGFW 功能外，SRX 系列设备还提供入侵防御、SSL 检测、URL 过滤和未知威胁检测功能，可通过一个安全平台满足通用架构的各类安全要求。

### 架构和关键组件

SRX 系列 NGFW 服务架构中包括的多个关键组件提供了一个强大的平台，可以保护企业免受不断出现的网络攻击的威胁。

#### 应用程序识别和控制：AppSecure

现代应用程序不再依赖基于端口的传统通信。新型应用程序从一开始就采用了规避传统防火墙的设计，它们会动态地更改端口和协议，或者在常用的服务（如 Web 流量）中建立隧道。对于用户，这意味着可以随时随地使用应用程序。对于企业，这意味着要应对威胁不断变化的局面，而且这些威胁绕过了传统的网络层保护，直接以应用程序为目标。

瞻博网络的 NGFW 服务可提供功能齐全的强大安全平台应对此挑战。其核心是 AppSecure，它对网络上运行的应用程序具有稳健的可见性和控制能力。AppSecure 拥有一种强大的机制，这种识别技术可不考虑端口、协议或加密方法，精确确定网络中应用程序的确切身份，从而立即识别应用程序，即使是全新的应用程序。

AppSecure 具有深入的应用程序可见性和控制能力，能够在不考虑位置和设备的情况下，提供将应用程序使用情况与用户关联起来的上下文。此外，AppSecure 的设计旨在了解应用程序行为和识别漏洞，从而在造成任何损害之前，阻隔以应用程序为载体的安全威胁。

只要对网络流量进行了细致分类，就可以基于应用、内容和用户精确定义安全策略，以此缩小威胁的覆盖范围。主要用于个人通信、以用户为中心的应用（如即时通信、对等文件共享、网页邮件、社交网络以及 IP 语音/视频协作等）现在都可以明确区分开来，并按企业许可向每一个应用授予特定的访问权限。

#### 用户识别：UserFirewall

用户身份是新一代防火墙的核心要求，让管理员能够创建反映企业需求而非网络要求的安全策略。根据用户身份而非 IP 地址定义防火墙规则是定义、管理和完善安全策略的强大机制。有了瞻博网络的 UserFirewall 功能，SRX 系列设备可通过与目录服务（如 Active directory）集成，将网络流量与特定用户相关联。您可以定义策略以基于用户或组而允许使用应用，从而实现更强大却更简单的安全控制。通过 UserFirewall，安全策略可通过组表达，这样，在向组中增加用户或从组中删除用户后，安全策略依然能起作用。此外，UserFirewall 还提供了用户级别而非 IP 地址级别的应用程序可见性，让您能深入洞察网络中的应用程序流量。安全管理员可以调整安全策略，使应用程序使用与安全和业务实践保持一致，从而减小威胁范围。

## 攻击缓解：入侵防御系统

瞻博网络的入侵防御系统 (IPS) 已与瞻博网络的 NGFW 紧密集成，可减少威胁并防范各种攻击和漏洞。与瞻博网络 Sky™ Advanced Threat Prevention (Sky ATP) 结合后，IPS 可对已知和未知的威胁提供全面的防御，在零日攻击袭击网络之前就开始防范。该解决方案会持续监控对新近发现漏洞的新攻击，不断更新对新网络攻击方法的网络防护。经由网络，针对客户端和服务系统上的漏洞发起的攻击在造成任何损坏之前就会被阻止。

## 未知恶意软件：瞻博网络 Sky ATP

瞻博网络 Sky ATP 是基于云的服务，可以提供全面的高级恶意软件防护。通过与 SRX 系列防火墙集成，瞻博网络 Sky ATP 可提供动态反恶意软件解决方案来适应不断变化的威胁环境。该解决方案提供基于云的服务来通过强大的机器学习算法动态分析 Web 和电子邮件文件，从而迅速识别新的、未知的恶意软件。一旦得出结论，相关决策就会发送至 SRX 系列 NGFW，以供实施。瞻博网络 Sky ATP 支持所有主流文件类型，包括 Microsoft ( .docx、.xls 和 .ppt )、pdf 和 Android 应用程序 (APK)。

## 阻止已知威胁：反恶意软件保护

来自多种攻击途径的恶意活动在持续激增，这种情况下，企业外围就成为了阻拦威胁进入网络的第一道防线。反恶意软件保护将基于云的声誉情报与 SRX 系列 NGFW 的本机处理相结合，提供轻便快捷的安全保护。其成果则是能够抵御众多已知威胁的高效外围防御，而且不会降低用户或业务的速度。

## 功能与优势

交付件	交付件说明	优势
AppSecure	无论使用何种端口或协议，都可使用精密的分类引擎来准确识别应用程序，包括使用逃避技术避免被识别的应用程序。	通过识别唯一应用程序而非 IP 地址来实施符合公司特定需求的安全策略，确保提供更精细的控制。
User-Firewall	与目录服务（如 Active Directory）集成，以便创建与特定用户或组相关联的防火墙策略，实施安全保护。	通过强大却简化的安全控制，设置更准确、更精细的安全策略。
入侵防御系统 (IPS)	提供抵御应用程序、数据库和操作系统中各种已知安全漏洞的全面防护。	持续监控对近期新发现漏洞的新攻击，以确保不断更新对最新网络攻击方法的网络防护。
瞻博网络 Sky ATP	基于云的沙盒服务，通过强大的机器学习算法提供精密的高级恶意软件检测，以便识别之前看不到的安全威胁。	准确识别避开传统方法的未知和前所未见的恶意软件，从而确保全面保护。
防恶意软件过滤	通过防病毒、防垃圾邮件以及 Web 过滤和内容过滤来防止遭受恶意软件、病毒、钓鱼式攻击、入侵、垃圾邮件及其他威胁的攻击。	实施实时安全防御，确保企业具有最新的签名，从而能够深入了解全球的威胁。
Junos Space Security Director	通过以单一管理平台集中管理所有 NGFW 来简化操作。	通过易于使用的 GUI 简化复杂的安全策略管理和实施，从而节省时间，提高生产力。

## 浏览防御：恶意 URL 过滤

钓鱼攻击是一种流行的攻击方法，通常会导致企业内部出现严重漏洞。毫无戒备的用户单击恶意 URL 后，就会安装利用漏洞的根程序病毒包，而此病毒包作为高级持续攻击的前导，为有价值的企业数据遭窃取创造了条件。攻击者通常会破坏热门网站，引诱用户无意中提供其用户密码。瞻博网络的 URL 过滤模块将持续地实时更新，提供全球不断发现的恶意 URL 的最新数据库，防止用户受到威胁。

## 加密保护：SSL 代理

SSL 已成为对网站进行身份认证和加密 Web 客户端与 Web 服务器之间流量的通用方法。但是，由于 SSL 内容是加密的，因此用户可以直接将恶意软件下载到其最终客户端。由于 SSL 连接的内容对组织不可见，因此看不到通过 HTTPS 传输到企业内部的任何威胁。

瞻博网络提供了一种功能强大的应用程序级 SSL 代理，它位于客户端和服务器之间，可拦截加密流量、终止会话以及重新启动与最终目标的连接。此代理可以用作 SSL“转发”代理，此时它位于企业 LAN 上的用户和用户 Internet 的访问之间，可以保护最终客户端。此代理还可充当企业外围的网关，拦截 HTTPS 流量，因而能够在加密流量进入企业之前终止加密流量。此时，未加密的流量会立即受到检查，以确定是否符合安全团队设置的安全策略。随后，主动恶意软件引擎会处理流量并立即阻止恶意软件，从而制止任何安全漏洞。

## SRX 系列平台支持

表 2 详细介绍了支持 NGFW 服务的 SRX 系列平台，并显示了需要的最低 Junos 版本。

表 2：新一代防火墙服务支持

平台	支持的 Junos 版本
SRX300 系列	15.1X49-D100 或更高版本
SRX550	15.1X49-D100 或更高版本
SRX1500	15.1X49-D100 或更高版本
SRX4000 系列	15.1X49-D100 或更高版本
SRX5000 系列	15.1X49-D100 或更高版本
vSRX	15.1X49-D100 或更高版本

## 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](http://www.juniper.net/cn/zh/products-services)。

## 订购信息

要订购瞻博网络 SRX 系列服务网关并获取软件许可信息，请访问[购买方法](http://www.juniper.net)页面，网址：[www.juniper.net](http://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](http://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** | Engineering  
NETWORKS | Simplicity