

用SRX系列业务网关构建安全的数据中心

目 录

介绍.....	1
应用范围	1
设计理念	1
性能要求.....	1
安全	2
路由	3
虚拟	3
高可靠性 (HA)	1
管理	4
SRX系列在数据中心的应用	4
硬件设计	4
可扩展的性能	4
路由集成.....	5
虚拟化.....	5
安全	6
高可靠性 (HA)	6
管理	6
应用场景描述和部署.....	7
数据中心核心	7
数据中心边缘	7
数据中心汇聚	7
小结.....	8
关于瞻博网络.....	8

介绍

在一个网络中数据中心是至关重要的，需要精心部署。通常一个大的数据中心要包含上千台服务器，每天都有数以万计的客户端到此访问。这会造成非常可观的数据流，而要从海量数据流中阻断某些特定流，几乎是不可能实现的。那么如何部署防火墙，以及多大规模的数据中心需要部署多大容量的防火墙会令用户很难抉择。最后用户会发现，大多数数据中心部署的防火墙基本只是开启了非常有限的功能。

瞻博网络已经拥有一套全新的安全产品来应对这些挑战。瞻博网络的SRX系列业务网关可以提供前所未有的高性能和高可扩展性。瞻博网络将JUNOS?软件设计精髓以及早已成熟的硬件体系结构应用于新产品的的设计，并开发了SRX系列家族产品。SRX产品就是为了满足今天的数据中心对安全产品的需求而设计，并充分考虑到产品自身的可扩展能力，以应对将来客户对网络扩展的需求。

应用范围

本文的编写有几个目的。首先，本文讨论了在数据中心部署防火墙的设计思路，让读者对数据中心面临的挑战有一个很好的理解。其次，本文描述了SRX系列业务网关的具体容量，并揭示其如何满足当今数据中心一些特定的需求。另外，还对防火墙部署方式做了分析，告诉读者在什么情况下部署SRX比较恰当。最后，对于那些想深入了解该产品的读者，还可以从本文中找到一些如何进行产品配置的细节描述。

设计理念

任何一个数据中心都会提供一系列的业务，允许其他数据中心设备或最终用户与其互访。这些业务的应用如果少的话是几种，多的可到上千种。不同种类的数据中心环境都会将承载数据流的重担放到其状态检测设备上，因为数据流是混杂在一起的，很难说清楚网络中某一种应用的数据流占整个负载的比例是多少。即使可以人为定义出一个比率，但实际情况是应用程序的使用具有突发性，任何时候都可能超过设定的值。考虑到这个复杂性，防火墙的性能需要具备根据不同的应用进行相应扩展的能力。因此说能够做到自己的网络准确定位一款设备是非常困难的。

传统数据中心业务典型的模式就是每台服务器上跑一到两个应用。而如今是虚拟技术盛行的时代，这个模式也会相应的变化。通常单一服务器可以跑几十个应用，每个应用都可以拥有一个其专属的虚拟系统进程。这就增加了数据中心网络设计的复杂性，因为每个虚拟服务器都需要接入特定的VLAN。这种状况也就使得物理连接变得极为复杂。另外就是数据中心的安全问题，每个数据中心都要连接几十个不同的网络，服务器之间需要互相传输大量混杂在一起的数据流，要想让这些数据流不会对彼此的网络造成安全威胁也是非常困难的。

以下几章节讨论在做防火墙实施部署时，需要考虑哪些不同的方面。看完这几部分读者应该对在数据中心部署防火墙所面临的挑战有了一定的认识和了解。

性能要求

提到数据中心，大家可能会联想到如下的画面：在一个房间里，眼睛所能看到的地方纵横交错地摆满了服务器。这种情况通常会发生在现在的大型企业。一个数据中心拥有几千台主机也是很常见的。根据数据中心的客户需求，这些主机会分到不同的组里代表不同的组织机构类别。各组织机构的安全策略会有所不同，决定了组与组之间的互访权限：允许访问或限制访问。通常这是很难做到的，因为主机之间会有无数的连接通道。防火墙必须做到维护主机之间的每一个连接状态，由于几个主要变化因素的存在，此工作将会给防火墙带来巨大的负担。

当部署数据中心防火墙时必须将以下因素考虑在内。对于数据中心防火墙最主要的挑战就是跟踪每秒新建连接数。在真正部署防火墙之前，这个数字很难确定下来。在没有状态防火墙的环境中，其他设备都不具备跟踪测算每秒新建连接数的能力。而且，每秒连接数的计算是要通过多种取样而得出的一个平均值，因此我们可以给出防火墙平均支持的每秒连接数。然而，如果每秒新建连接数发生突发状况，那么防火墙的吞吐能力将被迅速消耗，如果流量过载就会导致宕机。放置于数据中心的任何一台防火墙需要具备有效处理每秒连接数处于平均值的状况，更重要的是，还要具备能够支撑2-10次突发状态的能力。

当一个新的连接完成，防火墙必须要马上考虑会话的建立。最大并发会话数对于数据中心的部署是第二个非常重要的参数。数据中心里数量巨大的服务器，还有与之关联的客户端，需要不停地进行数据交换，这会导致庞大的并发会话数。由此将带给防火墙两大考验：第一，要确保现有会话的安全，第二，要保证有资源可以分配给新建的会话。如果在确保现有会话的同时无法建立新的会话，意味着无法建立新的连接，业务会中断。因此数据中心防火墙支持的最大并发连接数应该是平均值的2-4倍，这就保证了在突发情况下，会话不会丢失。

当会话建好之后，最关键的是要保证数据流能顺利地通过防火墙。数据流的测量可用两种方法：每秒转发数据包的数量，即PPS值；另一个是所有会话的总吞吐量。PPS值可以说明一台防火墙的大包转发能力，举例来说：由1500字节/包组成的一个流对比由64字节/包组成的流，要达到同样的吞吐，后者需要转发的数据包总数是前者的23倍还要多。这里要说明的是一台防火墙的能力不能只通过包转发值的大小来判断，还需要配合其吞吐能力的指标。尤其在数据中心部署的防火墙，需要特别注意其真实的性能，既要看PPS值，又要看吞吐。

安全

数据中心的安全是至关重要的，因为这里存储的数据往往是一个企业最重要的信息。数据中心提供的业务要达到不中断，并且是安全的。理想的数据中心的业务目标是，将类似业务或可信任业务分成一组，而非安全的业务在另一组。例如：将企业的应用分层部署，Web服务器，应用服务器和数据库服务器，通常都会把相似的业务类型部署在一个网段。

要做到服务器访问的安全第一步就是部署一台状态防火墙。它可以限制访问服务器的连接，将连接数控制在最少，不必要的访问就会被阻挡在防火墙之外。这就降低了一台主机与服务器进行未经授权连接的可能性。大范围地部署这种类型的安全配置是比较困难的，在下边章节会讨论虚拟技术，可以有效地解决这个问题。

要保证多种应用之间的安全连接，首先需要限制服务器之间的连接通道。下一步就是要保证内部安全，需要用到入侵防御系统，即IPS技术。IPS允许设备检查内网连接中是否包含恶意攻击行为。这对于数据中心来讲尤为重要，因为内网的恶意攻击行为很有可能造成服务中断或丢失数据等重大事件。为了避免这些风险，一定要在数据中心部署IPS设备。

IPS的两大局限性体现在设备本身的扩展性和IPS的部署位置。首先，用传统的IPS应用来满足现在数据中心的的需求是极为困难的，这不仅仅是IPS本身的容量问题，还涉及到IPS部署的能力问题。例如，如果你对IPS的部署没有经验，可能会把IPS放在所有应用服务器设备的前端。IPS也没有足够大的性能可以在数据中心的的核心位置大规模部署。基于以上考虑，典型的IPS设备只可以处理特定数量的数据流。所以当部署IPS时，无法指定其选择哪种数据流处理，而且IPS设备在性能扩展方面是有局限性的，正如我们前边所讲。所以理想状态是：在部署IPS时，可以有选择地处理一些数据流，对于那些不需要处理的流就不允许通过，以此来减少整体通过IPS的吞吐量，这样IPS就有足够的处理能力了。

路由

数据中心会包含很多分离的子网，用来区分不同的应用组。这就需要路由功能满足不同子网之间的数据交换或位于数据中心之外的主机对内的访问需求。子网之间或数据中心出口就是部署防火墙最好的地方，防火墙可以做为连接内外网或不同子网之间的通道，数据流要想进出子网或数据中心出口均需要通过防火墙的安全检查。但这样也给防火墙带来麻烦，它需要具备路由的能力，要支持各种路由协议。

防火墙最基本的功能单元就是一台路由器，它需要将一个网段的数据流路由到另外一个网段。但是路由器默认时是允许数据在不同网段传送，而防火墙在默认情况下是阻断数据流。而且，路由器的设计是让数据流以尽可能快的速度转发出去，而防火墙的目的则是在放行数据流之前要先保证其安全性。基于以上的原因，路由器在数据处理和转发等特性方面都是要优于防火墙的。其中一个主要的特性就是路由协议，动态路由协议是路由器支持的一个主要功能。一个复杂的数据中心一定会运行动态路由协议以支持不同网段之间的业务连接。因此数据中心内置的防火墙也需要支持动态路由协议。只不过防火墙上的路由功能是其次，安全功能是主要的。正因为防火墙在动态路由支持方面比较弱，怎样更好地将其集成在数据中心里也会是一个挑战。一般的防火墙，我们都是尽量避免在其上开启动态路由协议。而用于数据中心的防火墙需要具备与路由器同样强大的动态路由功能才可以做到更好与数据中心集成。

虚拟

如今人们都在致力于减少数据中心设备的投资成本，虚拟技术成为关键。“绿色”概念的引入使得减少数据中心设备占用空间变为现实。最简单的做法就是提高每台服务器的利用率，减少总的服务器数量。更少的服务器不仅减少了对环境的破坏，同时节约了能源。虚拟技术带来如此多好处的同时，也给网络的设计带来了新的挑战。

通常每台服务器都会与网络有两条连接，在过去，这就表示与一个或两个子网有访问。现在如果是虚拟服务器，可能会和几十个可更多的VLANs连接，可以扩展网络中的子网数量。这大大增加了数据中心可达网络的数量，由于这个原因，更增加了动态路由协议的重要性。有了虚拟技术，我们看到网络设备的物理空间变小了，而逻辑上的网络密度反而增加了。

由于逻辑网络大规模扩展，对防火墙的需求也增加了。为了使单个设备更加稳固，需要更大容量的防火墙。虚拟防火墙的概念和虚拟服务器类似，同样是为了减少机房的物理空间，增加逻辑密度以提高利用率。保证不同网络之间的安全隔离与设备的容量同等重要。

高可靠性 (HA)

数据中心中的每个设备需要具备高可靠性，要保持业务的不间断性和业务的可达性。很多数据中心经营者在业务中断时都会用美金来计算每秒的损失。一个数据中心从应用服务到网络到安全部署，每个环节都至关重要，需要设备非常的可靠。每个环节都会面临其独有的问题，这其中，安全部署环节面临最大的挑战。

对于一个高可靠性安全部署的环境，用一个词可以描述其面临的巨大挑战，那就是：状态。大多数的高级设备都会检测并跟踪进出数据流的状态。当两台处于工作状态的安全设备任何一台失效，两台设备都要知道这个状态。如果状态不是共享的，那么备用防火墙不知道发生了什么情况，它便会采取行动断掉当前会话。当部署任何状态检测设备时，最重要的就是要保持业务的连续性，任何状态都要在两台设备间共享。

防火墙在保证可靠性方面有几种不同的方法。最基本的方法就是一主一备，工作原理就是主防火墙工作时，另一台作备用，只有当主防火墙失效，备用设备才会接管。这是一个简单的方法，在需要高可靠性的环境，这样部署可减小问题的出现。

另一种常用的方法就是主/主方式。工作原理是：两台防火墙都处于工作状态，数据流同时流过两台设备。这样部署除了防火墙自身，还带来了一些其他问题，例如动态路由协议的处理，相邻路由器和交换机如何配置等。要保证所有周围的设备可以协调工作是很困难的。如果这些问题可以解决，那么这种方式最大的好处就是两台设备同时工作。网络管理员可以清楚地知道设备是否处于工作状态。

管理

数据中心里的所有设备都需要被管理起来，管理问题通常也是关系到网络是否具有扩展性。如果只有十几台设备需要管理，那么最直接的办法就是单独管理他们。然而，如果有几十台上百台设备需要管理，那么分开管理就是件麻烦事了。通常每个设备都有一个通用管理接口用来和外界通信，那么采用通用管理结构就是最好的选择。

在使用通用管理平台时，被管理的网元只需做好一次配置即可被其他需要管理的设备共享，这样的好处是减少了网络管理所需要的步骤。最后达到节省设备管理的成本，提高效率。通用管理平台也可以提供监控所有核心设备的能力。这使得网络管理员可以一目了然地看到网络中发生的任何事件。

如果要更详尽地了解某台设备发生的问题需要花一些时间，这就需要强大的CLI命令行方式做为重要的管理方式来备份中央管理平台。网络管理员需要根据设备状况或硬件情况进行故障排除。有了CLI，网管员就可以通过设备最直接地发现问题。

SRX系列在数据中心的应用

瞻博网络开发的SRX系列业务网关以应对数据中心的各种挑战。在本章中，我们将讨论SRX系列的各种特性，并显示其如何解决上述章节中涉及的挑战。我们也将更深入的分析SRX系列的功能，并讨论如何使用以发挥其最大优势。

硬件设计

SRX系列的硬件平台汲取了瞻博网络超过10年的各种产品设计经验。特别的是，SRX系列的设计，采用了与瞻博网络MX系列以太业务路由器相似的架构。MX系列与SRX系列的不同在于SRX系列需要实现安全业务服务。为实现该服务，瞻博网络在SRX系列上开发了业务处理卡SPC这一强大的模块化、高速、高密度计算卡，可在一个机箱中安装多块。增加更多的业务卡实现了性能的自动扩展。

SRX系列实现了真正的控制和转发平面的分离。控制平面实现全部的管理和动态路由交互，与数据平面处理分离。数据平面是高性能交换背板，实现SPCs和接口卡之间业务的线速转发。这确保了机箱能以SPCs处理业务的最快速度进行转发。其接口卡也与MX系列平台使用的接口卡相似。接口卡支持线速性能，确保了接口上无阻塞的业务输入和输出。

SRX5000系列作为防火墙，具有非常高的接口密度。支持在高达10个槽位中部署4端口万兆以太网接口卡模块和40个千兆以太网接口卡模块的混插。其余的槽位可用于业务处理卡。

可扩展的性能

如上述章节所讨论，性能的扩展性是非常困难的。为解决该问题，SRX系列的设计基于可扩展的硬件架构。

这使得用户可从使用少量的安全处理卡开始，然后随着需求的提升，增加更多的SPC处理卡以扩展性能。每个新增的SPC处理卡所带来的性能的增加是可以计算出来的，这使得企业可根据需求的增长来规划所需的SPC处理卡的数量。

在SRX5000系列中，每个SPC处理卡包含两个业务处理单元（SPUs），每个SPU都是高密度处理器。第一个被安装的SPC使用其中一个SPU作为总控中心。总控中心和其他SPUs一样处理业务，不同之处是它需要对会话是否存在进行判断。也就是说由总控中心来判断会话是否已经创建。当数据流进入SRX系列，但此时并没有会话创建，总控中心就会依据负载均衡算法将数据流转发到下一个可用的SPU。SPU实现了SRX系列业务网关的大多安全服务。这是设备最重的工作。所有的防火墙、入侵防护（IPS）和会话状态维护都在SPU上实现。

SRX3000系列具有相同的工作机制，但考虑到小规模部署的需求，以及价格因素，SRX3000上的每块SPC只包含一个单独的SPU。由于该原因，第一个SPU既要总控中心的工作，又要担当起数据处理的责任。当系统中仅安装有一块SPC时，SRX5000系列将采用与SRX3000系列相同的技术来使用该SPC，以最大限度地提高资源利用率。

这种类型的性能扩展正是数据中心所需要的。这使得可在数据中心放心地部署SRX系列业务网关，因其能够处理全部的、必要的会话。如果需要更高的性能，可增加新的SPC卡。这减少了对低性能设备进行昂贵升级的需求。

路由集成

如前讨论，SRX系列平台基于瞻博网络大量的已有的经验和现有技术来设计。其中包括了运行在分离的控制平面上的JUNOS?软件，这使得SRX系列可运行路由协议，并与现有的基于JUNOS?软件的平台一样强大。时间验证的JUNOS?软件已经运行在全世界成千上万的网络中，而实证优异的路由协议也被移植到SRX系列设备。路由协议的整个配置和任何其他基于JUNOS?软件的设备都相同。

所有的安全处理都在数据平面。由于是完全分离的，路由协议的收敛性能不受影响。这使得SRX系列平台在该类产品中具有出众性能。因此当SRX系列需要集成到动态路由环境中时，无需任何忧虑。

虚拟化

由于最初的成因，JUNOS?广泛部署在需要的网络中。尤其是在虚拟技术大规模应用的地方，JUNOS?便有了用武之地，足以应付变化多样的网络拓扑。需要支持不同的网络拓扑，使用多种虚拟技术。这就引出了虚拟路由器和路由进程的概念。JUNOS?采用路由进程的方式，因为路由进程能够实现多种不同的功能，虚拟路由器就是一个路由转发的进程。为配置一个虚拟路由器，网络管理员简单定义哪些接口运行在哪个虚拟路由器中即可。这会将该接口组与其他接口分离，实现不同接口设置之间的真正分离，以及一个物理设备上不同的业务处理流程。

SRX系列平台也汲取了ScreenOS软件的使用经验，在JUNOS?软件中实现了“域”的概念。域是一个逻辑的区域，可在其中配置接口。缺省下，仅在域内的业务可自由转发。而对于跨域的业务，需要进行安全策略的设置。这样做的好处是可以保证跨域业务的安全互访，并减少了创建安全策略时发生的错误数量。SRX系列产品很好地利用域和虚拟路由器技术，真正达到并行处理业务的要求，可成为替换任何数据中心现有防火墙的理想平台。

安全

SRX系列业务网关中的安全也利用了瞻博网络的技术优势，借助了ScreenOS软件中的防火墙功能以及瞻博网络IDP系列入侵检测和防护应用中的入侵防护系统（IPS）技术。这些都被移植到运行在SPCs上的JUNOS?软件中。防火墙功能和策略创建与ScreenOS中的配置是相似的。如前应用注释中的讨论，策略在域间创建，然后定义特定的主机和应用。这创建了管理员可配置的策略，以允许、拒绝或丢弃业务包。

当传统的状态防火墙不足时，可在业务经过防火墙时，通过标记为IPS检测的安全策略进行业务检测。一旦建立了会话，IPS引擎即可检测业务，并查询IPS策略以检查业务。IPS匹配熟知的源IP、目的IP和应用，也查询一组攻击设置。如果业务匹配任何一个攻击，攻击即被阻止。

这种结合的方法非常适合数据中心。SRX系列平台的性能使其可部署在支持高速业务流和大量动态路由环境的位置。

高可靠性（HA）

在数据中心，确保可靠性是一个关键设计原则。主要目标是确保SRX系列业务网关在数据或者控制平面失效的情况下，仍能继续工作。SRX系列在高可用设计中引入新的理念。SRX系列可在机箱之间进行控制平面和/或数据平面的故障切换。这一全新的混合设计使得两个独立的设备如在一个大的机箱中工作。通过该方法，使得两个不同的系统可扩展至两个单元。这一应用场景不同于传统的主/备方式——一台设备完成全部任务而另一台设备空闲。

控制平面部分是路由引擎（RE: Routing Engine）。路由引擎可在两个机箱之间进行切换，第一个节点转发业务，而第二个节点维护主路由引擎。当发生故障时，在失效机箱中运行的系统切换到第二个机箱。通过设备的全部业务在“状态”模式下处理。唯一丢失的业务是故障机箱或线路中的部分。在数据中心中，这实现了高度灵活的、简便的主/备部署，并且第二个机箱可提供部分备份服务。

管理

如整篇文档所讨论，SRX系列运行JUNOS?软件。实现和配置JUNOS?软件的最常用方法是通过CLI（command-line interface）。CLI是非常强大的配置工具。在JUNOS?软件后台，配置由可扩展的编辑语言（XML）处理，这对终端用户是透明的，并以层次化配置显示。这使得管理员可在他们认为最相关的配置之间切换，并使其关注于手头的特定任务。用户可在层次化系统的任何地方，进行任何操作命令，并查看所需配置的其余部分。只要用户使用过JUNOS?软件几分钟，他们就会快速适应这种方式。

当用户编辑一个JUNOS?软件配置的同时，一个备选的配置也在编辑，确保了每个运行的新配置命令与设备上运行的配置不冲突。变更需提交到设备并做确认。如果新配置有某种问题，系统可自动回退。这给数据中心提供了非常完美的方案——如果发生错误，变更需要非常快速的回退。JUNOS?软件存储了最近的50个配置，可以非常容易的与当前配置进行比较，以准确判定错误发生在何处。

CLI配置也可通过动态生成的Web管理接口—J-Web来支持。J-Web接口下载当前配置并以Web格式显示。这为经常使用CLI的用户提供了熟悉的视图，也为不熟悉CLI的用户提供了简便的用户接口。所有相同的配置选项以及易用向导在J-Web中都可用。这些向导简化了复杂的配置，并将其分解为一系列步骤。

为了给数据中心提供经常需要的、更大的视图，瞻博网络提供了网络和安全管理器软件--NSM。NSM支持全部的瞻博网络防火墙产品。NSM设计用于同时管理上千台设备。其提供了设备的可见性及健康检查。

通过NSM，管理员可以创建一个配置然后应用到多台设备。当整个数据中心实施相同的防火墙策略时，这是非常有用的。安全策略中的地址对象和服务在不同设备上都可使用。也可以创建模板，在多台设备应用相同的配置，如DNS（Domain Name System）和NTP（Network Time Protocol）。这减少了数据中心的维护工作量和大量的成本。

如果在报告中需要更深入的分析，可以部署瞻博网络STRM系列安全攻击响应管理器。STRM系列从NSM中提取log信息并进行关联。STRM系统在简单易用的console中显示了数据中心发生的全部各种安全攻击。了解整个架构中正发生的事情，是减少攻击和标记潜在问题区域的强大工具。

应用场景描述和部署

在数据中心部署SRX系列业务网关，有三个位置具有重要的意义。每一部署位置都有其特定的优势，在本章节将讨论每一位置，并提供SRX系列在数据中心的应用案例。

数据中心核心

数据中心的中心是核心—通过数据中心的大多数业务都经过该位置。这是部署SRX系列的理想位置，因其赋予防火墙检查数据中心全部业务的机会。SRX系列可以部署在数据中心的中心或者放置在核心路由器之外。

SRX5000系列非常适合于作为中等到大规模网络的核心设备，而SRX3000系列更适用于小到中等规模的网络。如果以防火墙功能评价，SRX系列非常快；如果作为核心路由器，即使SRX5800也远不及瞻博网络T1600核心路由器——其可以处理超过SRX5800 10倍的业务量。

SRX系列在最大型数据中心的理想部署方式是以HA模式、旁挂在核心设备上。这类数据中心的中心设备可能是T系列核心路由器、MX系列以太网业务路由器或EX8200以太网交换机。这些设备将提供高密度以太网端口和极高的包交换容量。SRX系列通过虚拟路由器和动态路由协议，将业务直接转发到核心设备。

数据中心边缘

数据中心边缘也是部署SRX系列防火墙的最佳位置。如果部署环境的广域网连接是以太网，SRX系列可以代替现有的路由器和防火墙。也可将几个防火墙整合到一个SRX系列组中。

大型企业部署称作“共享服务核心”的边缘方案。该设计提供了强大的、多个部门或企业共享的边缘。“共享服务核心”为企业提供了高速防火墙和路由。其也增强了通用安全策略并通过IPS技术消除了攻击。

数据中心汇聚

在数据中心的汇聚层部署SRX系列业务网关是值得关注的地方。SRX系列将位于核心和接入层之间。在该方案中，接入交换机应包括配置“集群交换 (virtual chassis)”技术的EX4200以太网交换机。“集群交换 (virtual chassis)”包含自身的二层区域。而交换机和SRX系列之间的链路为三层连接。服务器将SRX系列设置为缺省网关。这实现了“集群交换(virtual chassis)”所有主机之间的安全连接。

如果“集群交换 (virtual chassis)”中的主机需要与数据中心外部或者数据中心内部的另一台服务器通信，业务流首先发送到核心，然后转发出数据中心，或者经过相应服务器之前的SRX系列设备。这一设计确保了数据中心所有业务的安全性，安全处理也扩展到几台SRX系列防火墙。

小结

在本文中，回顾了数据中心部署防火墙的挑战。这给了读者良好的启发：当评估数据中心防火墙部署方案时，应提出何种问题。这些挑战的核心命题是，几乎全部现有防火墙无法扩展以满足高速数据中心的需求，或减小以满足不同位置的灵活性的需求。

这些问题也是瞻博网络在分析数据中心客户的关键需求时所考虑的。SRX系列是从瞻博网络现有产品线中选择真正的技术并通过新理念整合到一起。防火墙在今天的数据中心中以有限的方式部署。但通过使用现有SRX系列产品线，现在就可能满足大多数据中心的安全和性能需求。

关于瞻博网络公司

瞻博网络公司是高性能网络的领导者。Juniper提供的高性能网络架构，具备快速响应和安全实施的能力，可以加快用户部署单一网络上业务和应用的时间以满足高性能业务模式的需求。更多信息，敬请查询www.juniper.net。

北京代表处

北京市东城区东长安街1号
东方经贸城西三办公楼15层1508室
邮政编码：100738
电话：8610-6528-8800
传真：8610-8518-2626

上海代表处

上海市淮海中路333号
瑞安广场1102-1104室
邮政编码：200021
电话：8621-6141-5000
传真：8621-6141-5090

广州代表处

广州市天河区天河路228号
广晟大厦28楼03-05单元
邮政编码：510620
电话：8620-8511-5900
传真：8620-8511-5901

Copyright©2009, Juniper Networks, Inc. 版权所有，保留所有权利。Juniper Networks, Juniper Networks标识，NetScreen和ScreenOS是瞻博网络在美国和其他国家的注册商标。JUNOS和JUNOSe是瞻博网络所属商标。所有其他的商标、服务标记、注册商标或注册的服务标记均为其各自公司的财产。瞻博网络不承担由本资料中的任何不准确性而引起的任何责任，瞻博网络保留不做另行通知的情况下对本资料进行变更、修改、转换或以其他方式修订的权利。