Hillstone
山 石 网 科

山石网科
全分布式架构技术白皮书

概述

当今快速增长的网络和数据通信发展，对安全产品提出了更高的要求。传统架构下的设备性能和扩展性都会存在瓶颈。山石网科的全分布式架构打破了这些限制，通过智能流量分配算法实现流量的分布式处理，并基于资源管理算法的专利技术实现实时动态信息的完全分布式处理，使安全设备可以在提供丰富的应用安全服务的同时具备极高的性能、可扩展性及可靠性。

数据中心网络安全的挑战

快速的网络发展和数据中心的业务集中，为数据中心安全设备的性能要求提出了全新挑战。一方面，随着高清视频、流媒体和P2P等高带宽应用的增多，网络流量激增；宽带的普及和移动互联网的发展带来海量用户同时在线，这就要求数据中心防火墙具备处理大流量和海量网络访问的能力。同时，网络实时业务的推广和网络焦点事件的增多也使海量用户突发大规模同时访问的频率越来越高。因此，数据中心安全产品还需具备高新建连接速率。

面对这些种种挑战，对于数据中心安全设备提出了超高的吞吐量、并发连接数和每秒新建连接数的全面性能要求，并且安全性能可以按需进行线性扩展，应用安全处理能力也需具备高性能与高扩展性。

现有安全产品的架构限制

业界典型的传统安全产品架构中，有单CPU架构和多CPU架构之分。很明显，在高端安全产品上只使用一个单CPU的系统是无法满足用户要求的。多CPU架构中的堆叠式架构和现有的分布式架构也都存在着各自的问题与瓶颈，无法使安全产品性能做到全面有效的线性增长。

• 堆叠式架构的限制

堆叠式架构是将多个系统模块在一个大的系统中叠加起来，以此来提升整机的数据处理能力。但是这样一个系统叠加多个模块的问题是子系统模块之间的性能与容量不能相互支援，跨模块之间的性能利用率比较低且无法实现相互冗余。同时，对于整个系统中资源的管理和对实时动态信息(RTO)的管理都会比较困难。因此，堆叠式架构无法使数据中心防火墙的资源得到有效利用。

实时动态信息(RTO)是指在进行数据包处理中动态创建的信息，这些信息既包含数据包处理过程中所需的信息，又包含进行攻击防护和系统监控所需的计数器和状态信息等。实时动态信息的处理机制是决定整个安全设备性能和可扩展性的关键因素之一。存储RTO信息的数据库即RTO-DB。

• 分布式架构的限制

现有常见的分布式架构是将业务流量在各个模块上进行分布式的处理，而对于实时动态信息(RTO)的处理方式是决定分布式架构性能的关键因素。现有的分布式架构中，有共享型分布式和复制型分布式两种。但是这两种分布式都存在着性能瓶颈和问题。

◇ 共享型分布式架构

共享型分布式架构是在多CPU的系统架构中采用集中的RTO-DB管理方式。如下图所示：

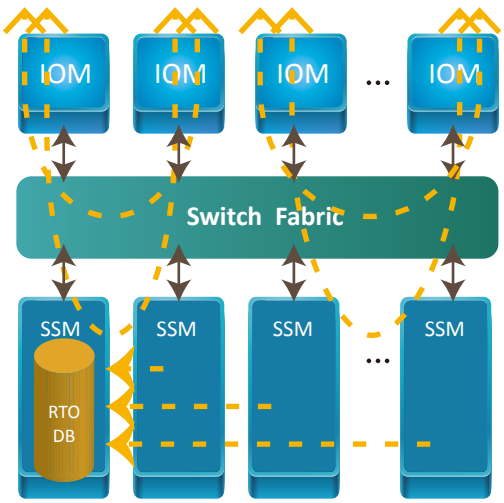

图1：共享型分布式架构处理机制

在共享型分布式架构中，RTO-DB是一个全局的集中式数据库，所有的RTO信息都存储在这个RTO-DB中，所有对于RTO的操作都通过远程调用来实现。这样系统的性能会受限于单一的数据库，尤其是在CPU数量不断增加的情况下，这种一对多的模式将会对性能提升有更大的限制。同时，一旦这个集中式数据库出现问题将影响整个系统。因此，共享型分布式架构不仅会带来性能瓶颈，还存在单点故障的问题。

◇ 复制型分布式架构

复制型分布式架构是在多CPU系统中采用所有CPU上完全复制RTO信息的方式。如下图所示：

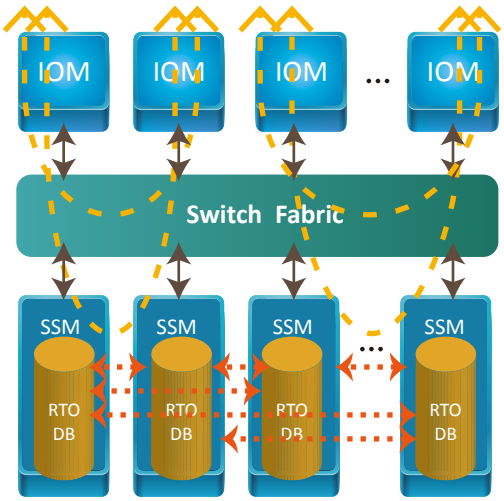

图2：复制型分布式架构处理机制

在复制型分布式架构中，RTO-DB存储全部RTO信息，并且每一个CPU上都有相同的RTO-DB的复制信息。虽然这样可以避免单点故障问题，但是当CPU数量增加时，对于CPU之间RTO-DB的信息同步复杂度却是在不断增加的，会造成系统资源的内耗，如CPU资源的更多占用等，这也将成为系统性能扩展的瓶颈。

简要总结，传统的安全产品架构方案中，系统的性能、线性扩展性以及可靠性都有很大的限制，无法满足新一代数据中心的发展趋势。

山石网科全分布式架构

山石网科创新的全分布式架构，是通过基于会话的智能流量分配算法，实现海量业务流量在业务模块（SSM）和接口模块（IOM）上的分布式高速处理；并基于拥有专利技术的独特的资源分布管理算法，突破了多CPU下的资源高效分配的技术壁垒，实现RTO信息在多CPU上分布式存储与同步。全分布式架构为性能的全面线性扩展提供架构基础，使包括吞吐量、并发连接数、每秒新建连接数在内的防火墙性能可以随着CPU的增加而全面的线性增长，并且为数据中心应用层安全提供强大的支撑。

• 分布式业务流量处理

从硬件架构上看，全分布式架构的硬件构成是由多个IO接口模块(IOM)和安全业务模块(SSM)组成的，它们由高速交换通道进行相互联接。下图显示出典型的硬件架构：

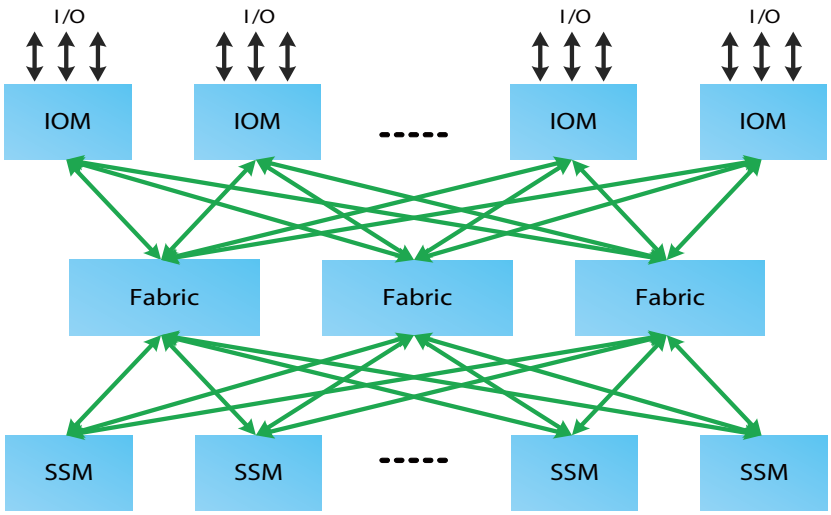

图3：全分布式架构硬件构成

全分布式架构的数据包处理是在IOM和SSM上完全分布式进行的。当数据包由IOM进入防火墙后，数据包既可以通过IOM直接独立进行快速转发，也可以在SSM上进行分布式处理后，再由IOM送出。这样的分布式处理方式提高了各模块CPU的利用率，也使系统整体性能得到大幅提升。

• 全分布式实时动态信息(RTO)处理

对比现有的两种共享型和复制型分布式架构，山石网科全分布式架构采用了创新的专利技术实现对于RTO-DB的全分布式处理机制。

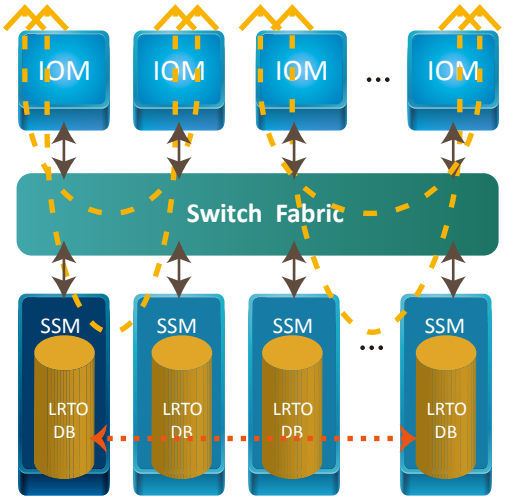

图4：全分布式架构RTO-DB处理机制

全分布式架构的RTO-DB是在SSM的CPU上完全分布式部署的。每一个CPU负责一个本地的RTO-DB（LRTO-DB本地实时动态信息库），整个RTO-DB的信息完全分布式存储在各个LRTO-DB中。同时，采用拥有专利技术的独特的资源分布管理算法，保证对于RTO-DB的定位和检索。

与之前的方式相比，全分布式RTO-DB处理方式可以使系统间通信复杂度恒定，即使是增加系统中CPU的数量，对于RTO-DB的管理和操作也同样可以保持高性能与高效运行。采用全分布式架构可以实现系统性能的全面线性扩展，保证系统的高吞吐、高并发、高新建，并可支持应用层安全处理能力的大幅度提升。同时，在可靠性方面也可以避免单点故障问题。

结论：

山石网科的全分布式架构打破了传统架构的限制。它采用了创新的资源管理算法实现全分布式实时动态信息的管理机制，采用了基于会话的全分布式处理流程实现业务流量在SSM与IOM上的分布式处理。由此带来的是，整个系统的性能和可扩展性可以随着CPU数量的增加而全面线性的增长。

基于这种创新分布式架构的数据平面软件也可以很容易的扩展应用到虚拟机中，因此非常适合于满足数据中心的安全应用和服务的需求。