

多核安全网关成功案例——营口港务集团公司

客户名称：营口港务集团公司

所属行业：运输物流型企业

客户需求：营口港公司内有几千人通过集团的宽带总出口访问Internet，需要做到安全防护和多出口负载均衡

产品型号：Hillstone SA-5050

实现功能：高性能NAT、内外网安全防护、基于IP的流量控制和会话数限制、SSL VPN

用户介绍

营口港是辽宁沿海经济带上的重要港口，也是东北地区及内蒙古东部地区最近的出海港。现辖营口、鲅鱼圈和仙人岛三个港区，陆域面积20多平方公里，共有包括集装箱、滚装汽车、煤炭、粮食、矿石、大件设备、成品油及液体化工品和原油8个专用码头在内的61个生产泊位，最大泊位为20万吨级矿石码头和30万吨级原油码头，集装箱码头可停靠第五代集装箱船。2007年，营口港吞吐量达到1.22亿吨，成为中国沿海第10个亿吨港口；2008年吞吐量超过1.5亿吨，2010年预计实现2亿吨。

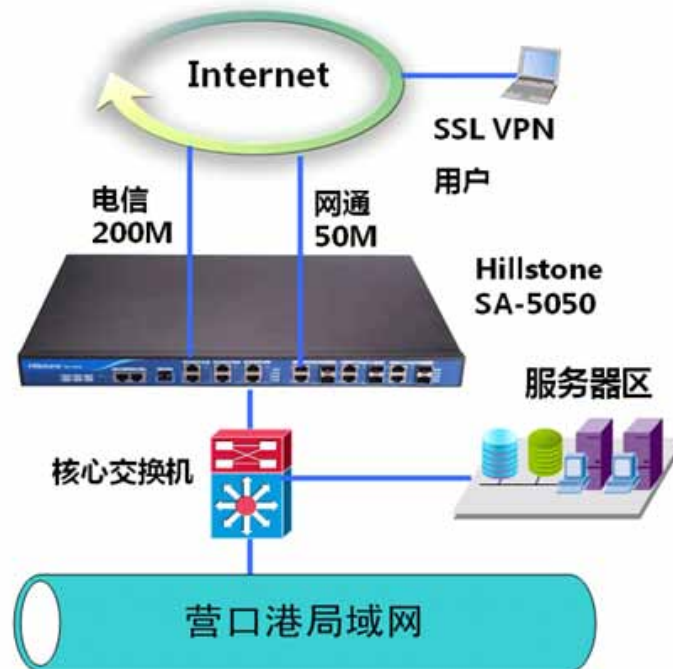
营口港的集装箱航线已覆盖沿海主要港口，并开通了日本、韩国和东南亚等国家和地区十几条国际班轮航线和多条可中转世界各地的内支线。2007年集装箱吞吐量完成137万标准箱；2008年超过200万标准箱；2010年预计实现300万标准箱。

目前，营口港已同50多个国家和地区140多个港口建立了航运业务关系。装卸的主要货种有：集装箱、汽车、粮食、钢材、矿石、煤炭、原油、成品油、液体化工品、化肥、木材、非矿、机械设备、水果、蔬菜等。其中，内贸集装箱、进口矿石、进口化肥、出口钢材、出口非矿的装卸量均为东北各港之首。

Hillstone SA-5050在营口港网络中的方案特点

营口港网络中心是整个集团内部几千人访问Internet的总出口，同时考虑到Internet上的互联网攻击众多，因此选购的安全产品的性能、安全性和稳定性是首要考虑的，而在此基础上构建可靠、可控的网络则同样重要。同样的，营口港网络中应用众多，因此应用层管理和访问控制等需求也应运而生。

针对营口港的特点，Hillstone山石网科给用户推荐了一套基于Hillstone SA-5050多核安全网关的解决方案。该方案从处理能力、扩展能力、安全性、应用的便利性等多个方面为用户考虑，很好的满足了本项目中用户对高性能、高安全性、高性价比和多功能的需求。整个项目解决方案的拓扑如下图所示。



营口港网络拓扑图

Hillstone SA-5050多核安全网关提供了一系列解决方案，在本项目中，SA-5050针对营口港网络安全防护上的主要特点如下：

SA-5050多核安全网关的抗攻击能力

在营口港网络中部署SA-5050之前，ARP病毒频繁、带宽滥用、潜在的信息泄露、资源间的随意访问及未知病毒的爆发严重影响着内网用户正常的网络应用。特别是项目开展之前，营口港网络中有多台重要的电子业务服务器被不明攻击者入侵过并留下了相应的痕迹。而安全防护和抗攻击并非网络服务器的专利防护，它也是普通PC在享受互联网便利性时必须考虑的。因此，安全防护和抗攻击是营口港本次项目的需求之一。

在本项目中，营口港在防止外部攻击内部服务器的同时，也要防止网络内部的PC向外发起攻击，或是染毒后影响网关及对指定主机的攻击。对于营口港来说，管理一个近两千台PC的网络并非易事，因为网管人员不可能控制每台PC的行为，更不可能保障客户端PC不中病毒，唯一的解决办法就是在局域网出口处部署可以同时防御内外网攻击的安全网关设备。对此，部署的Hillstone SA-5050多核安全网关很好的解决了这方面问题。SA-5050多核安全网关具有强大的抗攻击能力，具有每秒20万TCP或50万UDP的新建

会话能力；在正常的使用下，能检测并防御800K包/s以上的SYN-FLOOD攻击；在极限背景流量情况下仍可以对攻击流进行识别和阻断，从而能有效的保障内外网安全。

SA-5050多核安全网关的会话控制能力

由于营口港公网地址有限，而且有大量的服务器需要对外做NAT映射，因此可给客户端PC用的NAT端口也是有限的。而客户端PC过多的占用会话及端口会影响到整个网络的访问效率，而且也会比较大的消耗出口网关有限的系统资源，因此即便在营口港这样的大型企业网络中，进行会话数限制也是很有必要的，这种解决方案能有效解决客户端上网打开网页过慢、FTP超时等待等问题。

Hillstone SA-5050多核安全网关具有强大的会话控制能力。通过启用会话控制功能，SA-5050能有效解决内网客户端PC过多的占用会话及端口，精确控制每台PC最大所能使用的会话数。同时，SA-5050也能够精确控制每个互联网上的IP地址对服务器发起的访问会话数以及访问会话速率，能在DoS/DDoS攻击发生前就将攻击控制在有限的范围内，这在最大程度上保护用户内网的服务器，一定程度上起到了对服务器的安全防护和抗攻击能力，而这都是通过SA-5050多核安全网关去实现的，内网的服务器就如同古城堡里受到城堡保护的平民一样免受外来的不良攻击。

SA-5050多核安全网关的带宽管理功能

对于Internet上的网络来说，只要能连到Internet，出口带宽就永远满足不了大型网络客户端的需求。营口港也同样存在这样的矛盾：个别用户大肆利用BT、迅雷、电驴等工具从Internet上疯狂下载各种电影、软件、音乐等，致使网络带宽被占满，影响其他用户上网；有的用户还会使用网络视频、在线视频、在线音乐也会占用过多的带宽资源；各种下载的泛滥和原有的应用带宽由于没有进行合理的分配，造成网络极度拥堵，导致企业的正常应用和关键业务经常无法使用或者经常掉线。因此，用户急需采取相应手段来对带宽进行精细、全面的管理从而提高网络带宽的有效利用率。Hillstone SA-5050很好的解决了用户此方面的困惑，本项目中主要通过以下几点进行精细化管理：

1、基于每个IP地址的最大带宽限制。在营口港的网络中，每个客户端IP上网的上下行带宽都限制到最大500Kbps，这样就可以防止某些个体大量独占带宽的情况发生。

2、基于每个IP地址的会话限制。在营口港的网络中，进行会话数限制后很好的解决了上网打开网页慢等问题。

3、基于服务的带宽管理：通过Hillstone多核安全网关，用户的网络管理人员能直观了解到各种协议占用网络的带宽，从而制定策略来保障关键流量带宽、抑制P2P等协议对网络带宽的占用。在对P2P服务的总带宽进行限制及将HTTP协议的带宽进行保障后总流量大幅下降，高峰时网页打开速度得到提升。

4、关键业务的带宽保障：针对用户的OA、ERP、电子邮件等关键业务进行了带宽保障，从而做到了如同北京2008年奥运会奥运专用道一样保证了关键应用的流畅运行。

SA-5050多核安全网关的NAT功能

由于用户公网地址数量有限，而且内部有众多的服务器需要对公网提供服务，因此用户在SA-5050上同时启用了源NAT和目的NAT。SA-5050提供了高性能的NAT功能能够满足用户的大量快速的地址翻译需要；而且SA-5050本身集成了服务器的负载均衡功能也很好的满足了用户对服务器访问流量分担的需要，避免了单台服务器出现负载过重的问题。

SA-5050多核安全网关的多出口负载均衡功能

营口港网络目前有2条Internet专线来实现连接Internet，后续还需要增加多条Internet专线来满足后续网络规模扩展的需要。而之前用户的网络中在每条Internet专线上都部署了一台路由器，这样也增加了用户的管理和维护的工作量。而本项目中，Hillstone SA-5050多核安全网关为用户的多出口问题提供了完美的解决方案。

1、实现了基于源/目的的智能选路。Hillstone SA多核安全网关，按照查找优先级排列分别是：策略路由、源接口路由、源路由、目的路由。即不仅可以实现基于srcIP的源路由、基于In-interface（源接口）+ srcIP的源接口路由、还可以按照srcIP + srcPort + dstIP + dstPort + Protocol五元组来完成智能选路的高级PBR功能，这点能很好满足用户在本项目中全方位的要求。

2、Hillstone SA多核安全网关同时采用ECMP智能负载均衡技术，最大可以实现在40条路径之间作负载均衡。此外选择负载均衡的方式，有三种方式可供选择：基于源地址、基于源和目的地址、基于srcIP + srcPort + dstIP + dstPort + Protocol五元组，来迅速判断出流量的最佳路径，使整个网络出口的流量能够在这些不同的网络链路中智能的进行负载均衡，达到最大的网络效率。在本项目中，Hillstone SA-5050针对两条链路使用ECMP技术能很好的权重分担两条链路之间的负载。

3、Hillstone SA-5050多核安全网关完全替换了传统的路由器加防火墙的接入方式，简化了该用户的网络拓扑，减少了用户的管理维护工作量，同时降低了出口网关的投资。

SA-5050安全网关的SSL VPN功能

Hillstone SA-5050多核安全网关集成的SSL VPN为移动用户（出差员工、家庭办公人员等）和远程接入提供了完美的技术解决方案。通过使用Hillstone提供的SSL VPN技术，无论采用何种Internet接入方式，都能在用户快捷接入、数据传输以及内部资源访问等各方面安全性的前提下，确保VPN用户能方便、灵活、高效地通过该技术接入到用户总部的内网并访问相应的网络资源。SSL VPN系统的部署使得公司IT应用扩展到营口港企业网以外，充分提高了营口港的员工效率，强化了IT服务水平，提升了公司竞争力。

使用效果和用户评价

用户使用Hillstone SA-5050多核安全网关后，全面解决了用户面临的各方面安全问题，主要带来了以下效果：

1、关键业务流量得到保证：为关键数据业务流量设置了带宽保障，限制了网络中存在着大量的P2P软件（如BT、迅雷等）、P2P在线视频、大型网络游戏等应用流量，保障了正常业务的顺利进行，提高了网络资源的利用率。

2、保证系统免受攻击，正常运转：控制了网络中充斥着大量ARP攻击，保护企业网络免受来自

Internet上的控制，保障了网络的正常运转，保障了正常的网络应用系统。

- 3、很好的做到了多出口负载均衡，简化了用户网络拓扑架构，减少了用户的管理维护工作量。
- 4、会话控制的使用有效的控制了某些PC使用会话数过多的现象，更进一步的优化了网络。

Hillstone SA-5050部署在用户6个多月的使用过程中，用户评价：Hillstone SA-5050的确是一个性能高、功能强的一体化的多核安全网关，我们在本次项目中的使用对它有了一个全新的认识，我们对它这款一体化的设备很满意。使用它很好的解决了我们的多出口多设备连接问题；而且有很强大的抗攻击性能；还能提供SSL VPN功能以及强大的防火墙安全功能。以一台设备的价格买回多个设备的功能，感觉很有价值。通过使用这台SA-5050多核安全网关，强化了上网安全管理、节省了带宽的投资，把营口港网络的安全水平提高了一大截。

北京总部

地址：北京市海淀区上地七街1号
汇众大厦3层
邮编：100085
电话：+86(10)8289 7229
传真：+86(10)8289 9814

上海办事处

地址：上海陕西北路1388号
银座企业中心1715室
邮编：200060
电话：+86(21)6149 8205
传真：+86(21)6149 8001

广州办事处

地址：广州市天河区天河路208号
粤海天河城大厦13层1328室
邮编：510620
电话：+86(20)2826 1950
传真：+86(20)2826 1999

成都办事处

地址：中国成都市总府路2号
时代广场A座26层2625
邮编：610016
电话：+86(28)6606 7115
传真：+86(28)6606 7199

南京办事处

地址：南京市中山东路300号
长发中心A栋1602室
邮编：210002
电话：+86(25)8682 9916
传真：+86(25)8682 9916-606

销售与服务热线：400-650-0259

Copyright © 2009, Hillstone山石网科版权所有，保留所有权利。

Hillstone Networks、Hillstone Networks标识、Hillstone、Hillstone山石网科、Hillstone标识、StoneOS、StoneManager、Hillstone PnPVPN、多核Plus、Multi-Core Plus、Hillstone SA-2001A、Hillstone SA-2001、Hillstone SA-2001B、Hillstone SA-2003、Hillstone SA-2005、Hillstone SA-2010、Hillstone SA-5020、Hillstone SA-5040、Hillstone SA-5050、Hillstone SA-5180、Hillstone SR-320、Hillstone SR-330、Hillstone SR-530、Hillstone SR-550和Hillstone SR-560为Hillstone山石网科公司所属商标。所有其他商标和注册商标均为其各自公司的财产。
本文所包含信息可能会有所修改，恕不另行通知，如需最新信息请浏览Hillstone山石网科网站(www.hillstonenet.com)。