

打造可靠网络边界 ——红云红河集团红河卷烟厂成功案例

客户名称：红云红河集团红河卷烟厂

所属行业：大型烟草企业

客户需求：高可靠的防火墙功能，以及未来3-5年在功能和性能上的扩展能力

产品型号：Hillstone SA-5020

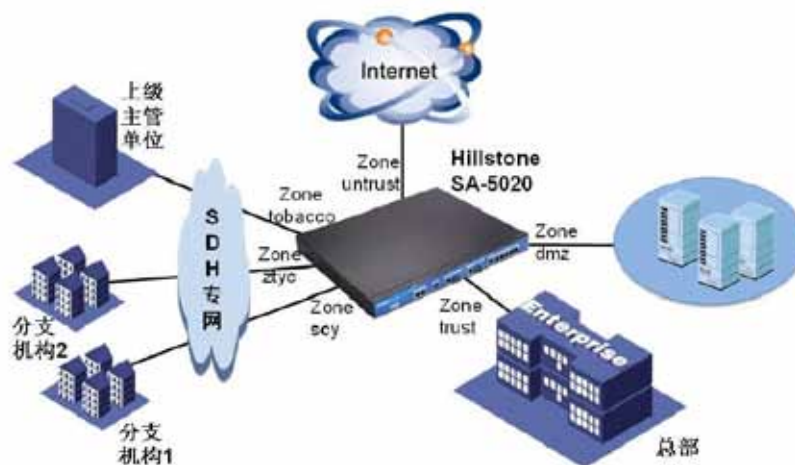
实现功能：防火墙、NAT、攻击防护、会话限制、日志记录及详尽的监控统计功能

客户需求

红云红河烟草（集团）有限责任公司（简称红云红河集团）是世界第四大烟草集团公司。下辖红河卷烟厂、昆明卷烟厂、曲靖卷烟厂等六个生产厂和其他企业。作为集团中重要成员的红河卷烟厂，是全国唯一生产单一品牌的烟草工业企业。2007年品牌产量161.5万箱，品牌销售收入160.2亿元，实现税利99.8亿元。

红河卷烟厂网络边界原有防火墙使用年限已久，基本无力承载当前业务及性能的需要。为了避免出现防火墙阻塞宕机的事故，同时兼顾未来边界设备功能扩展的需要，于2008年底通过组织多方论证和近1个月时间的企业网边界出口区域真实环境的设备在线测试，最终选择了Hillstone的SA-5020高性能多核安全网关，来满足红河卷烟厂未来3-5年左右出口扩容的需要。

Hillstone SA-5020在红河卷烟厂对其网络边界进行安全防护的应用特点



SA-5020高效的策略控制

在红河卷烟厂的企业园区网与外界网络边界出口处，包括 Internet/WAN（分支机构和上级主管单位），同时公共服务器对外部提供 WWW/E-MAIL 等服务。

所有的外部出口及DMZ服务器群交换机，都直挂到SA-5020。SA-5020可以提供6个千兆电口、2个千兆Combo口（电口+光口）的物理接口，同时还支持子接口、VSwitch 接口、VLAN 接口、回环接口、隧道接口、集聚接口和冗余接口等逻辑接口。

和传统防火墙基于接口的策略配置方式不同，Hillstone SA-5020多核安全网关可以支持通过安全域 Zone来配置防火墙的安全策略，即支持域间的访问控制策略。通常将拥有相同安全级别的接口划分在同一个安全域中，然后对各域进行安全策略的配置和安全管理。如图所示，按照实际需要，红河卷烟厂的SA-5020的各个接口分别被划分到了trust、untrust、dmz、tobacco、zytc和scy等6个安全域。通过对各域之间配置防火墙安全策略，对各域之间的所有连接进行传输层协议以及应用层协议状态的检测，从而实现域间的访问控制以及应用状态监控。

Hillstone SA-5020多核安全网关的安全策略数最高可达30,000条，并且具有优化的规则匹配算法，规则的查询、匹配时间不随配置的策略规则数目线性增长！

SA-5020内外网的攻击防护功能

作为网络安全设备的安全网关，必须具备攻击防护功能来检测各种类型的网络攻击，从而采取相应的措施保护内外部网络免受恶意攻击，保证内部网络及系统正常运行。Hillstone多核安全网关提供基于域的攻击防护功能。

如上所述，用户有选择性地在trust、untrust、dmz等安全域上启用了攻击防范功能，以识别并阻断主流网络攻击包括：IP 地址扫描攻击、端口扫描攻击、IP 地址欺骗攻击、SYN Flood 攻击、ICMP Flood 攻击、UDP Flood 攻击、Huge ICMP 包攻击、WinNuke 攻击、Ping of Death 攻击、Teardrop 攻击、IP Option 攻击、TCP 异常攻击、Land 攻击、IP 碎片攻击、Smurf 和Fraggle 攻击等。并且可以查看开启攻击防范功能之后，设备所检测到的每种攻击次数和丢包次数。

SA-5020强大的会话控制

SA 系列多核安全网关支持基于安全域的会话限制功能，以防止单一用户如果在短时间内发起大量的连接，就会导致系统资源迅速消耗，挤占其它合法用户的资源。

红河卷烟厂用户有选择性地在SA-5020的trust、untrust、dmz等重点安全域上启用了会话限制功能。传统防火墙的会话限制功能，一般只能够实现到限制单一用户发起的连接总数这样的程度。Hillstone SA-5020多核安全网关具备业界最强的会话(连接)控制功能，可以对安全域内的源IP 地址、目的IP地址、指

定的IP 地址或服务进行会话数量或者建立会话速率控制，从而保护连接表不被DoS 攻击填满，并且能够有效限制和管控一些应用的带宽，如IM 或者P2P 等。

SA-5020针对企业用户上网行为的日志、网络分析监控功能

为加强对整个企业网络资源应用情况的了解，Hillstone SA-5020多核安全网关还可以提供内容详尽、分析透彻、功能强大的日志报表及统计系统。这点尤其受到红河卷烟厂用户的青睐。

a,提供基于企业网内部每个用户的最完整的互联网访问记录，避免法律风险

b,通过直观的、图象化的方式了解网络带宽的利用情况，以及企业网用户的网络访问状态，统计出网络访问的趋势，以帮助系统管理员更好地维护和管理网络，为企业网络管理者提供清晰的管理和决策依据。

例如:企业网内部每个用户的IP上下行带宽，每个用户的各种上网应用及其带宽占用情况，每用户(IP)的TCP/UDP会话数量，整个企业网出口整体接口上下行带宽，各种上网应用的带宽分布，TCP/UDP会话数量等。

用户评价

Hillstone SA-5020多核安全网关自2008年底投入使用后运行稳定，性能优秀，成为红河卷烟厂Internet/WAN网络边界的可靠支撑平台，大幅度提高了企业网信息服务保障能力，并为后期的系统升级和扩展提供了全面投资保护。

北京总部

海淀区上地七街1号
汇众大厦3层
邮编: 100085
电话: 010-8289 7229
传真: 010-8289 9814

上海办事处

陕西北路1388号
银座企业中心1715室
邮编: 200060
电话: 021-6149 8205
传真: 021-6149 8001

广州办事处

天河体育东路122号羊城国际
商贸中心东塔15层1510-1511
邮编: 510620
电话: 020-3825 4309
传真: 020-3825 4311

成都办事处

总府路2号时代广场A
座26层2625
邮编: 610016
电话: 028-6606 7115
传真: 028-6606 7199

南京办事处

中山东路300号
长发中心A栋1602室
邮编: 210002
电话: 025-8682 9916
传真: 025-8682 9916-606

西安办事处

高新技术开发区科技路33号
高新国际商务中心7层704B
邮编: 710075
电话: 029-8833 7347
传真: 029-8833 7347

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)。