

Hillstone山石网科上网行为管理白皮书

概述

互联网的兴起与普及为人们的工作和生活提供了极大的便利，与此同时，经由内部访问互联网导致的带宽滥用、效率下降、信息泄漏、法律风险、安全隐患等问题日益凸显。例如，在企业内部，部分员工利用工作时间在线炒股、玩在线游戏、欣赏音乐和视频、通过P2P工具下载、使用即时通讯工具无节制地网络聊天、通过网络外泄公司机密；在网吧等一些公共上网场所，人们可以随意浏览不健康网站、发表不负责任的言论、甚至参与非法网络活动……

针对互联网所带来的上述问题，StoneOS提供许可证控制的上网行为管理功能。该功能通过对用户的网络访问行为进行控制和管理，有效解决因接入互联网而可能引发的各种问题，优化对互联网资源的应用。

产品功能

StoneOS上网行为管理功能对网络游戏、在线聊天、在线炒股、P2P下载、网页访问、邮件外发及论坛发帖等各种网络行为进行全面控制管理，并可以根据需要针对不同用户、不同网络行为、不同时间进行灵活的管理策略设置和日志记录，同时能够配合Hillstone山石网科集中网络安全管理系统（HSM）对网络行为日志进行查询统计与审计分析，从而为网络管理者的决策和管理提供重要的数据依据。

上网行为管理策略

StoneOS上网行为管理功能主要通过策略机制实现，网络管理者可以针对不同用户制定适合的上网行为管理策略规则，系统则会根据策略规则对网络应用流量进行行为控制和管理。

上网行为管理策略规则共分为三类：网络应用控制策略规则、网页内容控制策略规则和外发信息控制策略规则，每类中又包含若干子控制策略规则。

策略规则名称、优先级、用户、时间表、网络行为以及控制动作构成上网行为管理策略规则的基本元素。通过WebUI配置上网行为管理策略规则，需要进行下列基本元素的配置：

Hillstone山石网科上网行为管理白皮书

- 策略规则名称 - 上网行为管理策略规则的名称。
- 优先级 - 上网行为管理策略规则的优先级。当有多条匹配策略规则的时候，优先级高的策略规则会被优先使用。
- 用户 - 上网行为管理策略规则的用户，即发起网络行为的主体，比如某个用户、用户组、角色、IP地址等。
- 时间表 - 上网行为管理策略规则的生效时间，可以针对不同用户控制其在特定时间段内的网络行为。
- 网络行为 - 具体的网络应用行为，比如MSN聊天、网页访问、邮件发送、论坛发帖等。
- 控制动作 - 针对用户的网络行为所采取的控制动作，比如允许、拒绝某网络行为或者对该行为或者内容进行日志记录等。

上述四部分中，用户表、时间及网络行为构成策略规则的控制条件，只有符合这些条件的网络应用流量才称为与策略规则相匹配的流量；控制动作即为对满足控制条件的网络应用流量（也即与策略规则相匹配的流量）所采取的控制动作。

网络应用控制策略规则

网络应用控制策略规则对网络应用的使用进行控制。StoneOS根据不同的协议及应用领域将网络应用分为网络游戏、即时通讯、在线炒股、P2P协议、流媒体协议、其他协议、FTP控制以及HTTP控制等等大类，每一大类中又包含若干具体的子应用和协议。网络管理者可以根据需要，对各种应用和协议制定基于用户和时间表的策略规则，以实现对用户上网行为的控制。

网页内容控制策略规则

网页内容控制策略规则包括URL过滤策略规则和关键字过滤策略规则。网页内容控制策略规则能够对用户访问的网页进行控制。URL过滤策略规则可以基于系统预定义的URL类别和用户自定义的URL类别，对用户所访问的网页进行过滤。关键字过滤策略规则可以基于用户自定义的关键字类别，对用户所访问的网页进行过滤，同时，能够通过SSL代理功能对用户所访问的含有某特定关键字的HTTPS加密网页进行过滤。

外发信息控制策略规则

外发信息控制策略规则包括Email控制策略规则和论坛发帖控制策略规则，能够对用户的外发信息进行控制。Email控制策略规则能够对通过SMTP协议发送的邮件和Webmail外发邮件进行控制，可以根据邮件的收件人、发件人、内容关键字、附件名称和附件大小对邮件的发送进行限制。同时，能够通过SSL代理功能控制Gmail加密邮件

Hillstone山石网科上网行为管理白皮书

的发送。论坛发帖控制策略规则能够对通过HTTP Post方法上传的含有某关键字的内容进行控制，如阻断内网用户在论坛发布含有指定关键字的帖子。

例外设置

对于特殊情况下不需要上网行为管理策略规则进行控制的对象，可以通过例外设置实现。例外设置包括免监督用户、黑白名单和Bypass域名。

免监督用户

免监督用户中可以设置一些特殊用户，这些用户的所有网络行为将不受上网行为管理策略规则的控制，比如将公司领导层或者某些特殊部门设置为免监督用户。StoneOS支持IP子网、IP范围、用户、用户组、角色和地址簿条目类型的免监督用户。

黑白名单

黑白名单中可以设置一些特殊URL，用户对这些URL的访问会跳过已定义好的上网行为管理策略规则，无条件地允许或者禁止。黑白名单包括以下部分：

- 黑名单：包含不可以访问的URL。不同平台黑名单包含的最大URL条数不同。
- 白名单：包含允许访问URL。不同平台白名单包含的最大URL条数不同。
- 关键字列表：如果URL中包含有关键字列表中的关键字，则PC不可以访问该URL。不同平台关键字列表包含的关键字条目数不同。
- 只允许通过域名访问：如果开启该功能，用户只可以通过域名访问Internet，IP地址类型的URL将被拒绝访问。
- 禁止访问白名单以外的所有网站：如果开启该功能，用户只可以访问白名单中的URL，其它地址都会被拒绝。

Bypass域名

Bypass域名中可以设置一些特殊域名，用户对这些域名的访问将无条件地允许。

上网行为库

StoneOS上网行为库包括预定义URL数据库、自定义URL数据库和关键字数据库。预定义URL数据库和自定义URL数据库能够为上网行为管理策略规则配置提供URL类别，网络管理者可以通过设置上网行为管理策略规则，对特定的URL类别进行过滤，从而控制用户的URL访问行为；关键字数据库能够为上网行为管理策略规则配置提供关键字类别，网络管理者可以通过设置上网行为管理策略规则，对用户进行访问网页内容关键字过滤、外发邮件关键字控制和论坛发帖关键字控制。

Hillstone山石网科上网行为管理白皮书

预定义URL数据库

StoneOS内置许可证控制的预定义URL数据库，即为支持预定义URL数据库的StoneOS系统安装URL数据库许可证后，预定义URL数据库才能使用。

预定义URL数据库中的URL按照中国的文化背景、伦理道德、法律法规、应用领域、上网习惯等进行分类。目前，StoneOS预定义URL数据库共提供几千万条的URL。

URL数据库更新

默认情况下，StoneOS会每日自动更新预定义URL数据库，用户可以根据需要更改数据库更新配置。Hillstone山石网科提供两个默认数据库更新服务器，分别是update1.hillstonenet.com和update2.hillstonenet.com。StoneOS支持在线更新和本地更新两种方式供用户进行选择。

自定义URL数据库

除了预定义URL数据库中的URL类别外，用户还可以根据需要自定义URL类别。自定义的URL类别将显示在系统URL类别列表中。

关键字数据库

用户可以定义关键字类别，用于网页内容关键字过滤、外发邮件关键字控制和论坛发帖关键字控制。

日志管理

StoneOS上网行为管理日志信息可以对用户的上网行为进行全面记录，包括网络游戏记录、IM行为及聊天内容记录、在线炒股记录、FTP/HTTP使用记录、P2P下载记录、在线视频访问记录、Web访问记录、外发邮件行为、内容及附件记录以及论坛发帖记录等等，这些记录为HSM（Hillstone Security Management™，Hillstone山石网科集中网络安全管理系统）的上网行为管理日志查询统计与审计分析提供完整的数据信息。

产品特点

URL内容分类访问控制

- 结合中国地区内容访问的政策、法规和习惯量身定制
- 具有数千万条域名的分类web页面库，实时同步更新

Hillstone山石网科上网行为管理白皮书

基于深度应用特征的行为控制

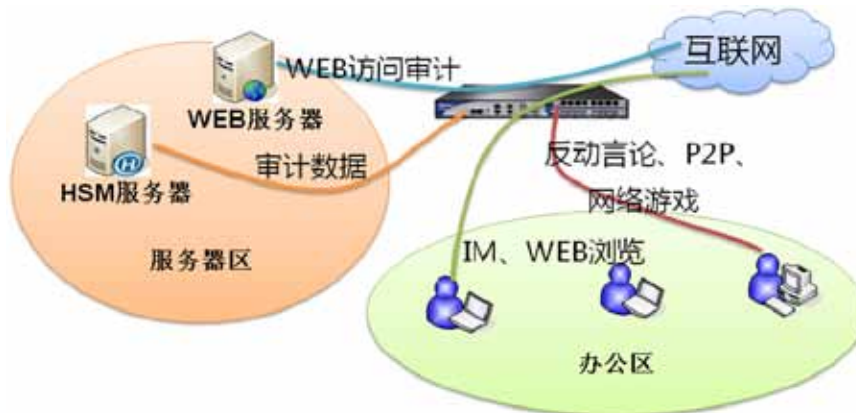
- 及时跟踪应用特征变化，定期分类更新
- 深度数据流识别，确保识别的精准度
- 先于NAT进行数据流特征识别，不受透传影响
- 手段多样性，优于简单的服务器地址阻断

日志审计独立于网关设备

- 降低日志数据分析对网关性能的影响
- 可插卡式存储支持

典型案例

上网行为管理作为山石网科UTM中一部分，与访问控制、Qos、IPS等模块构成企业网络出口的安全屏障。对外可进行入侵防护和非法访问阻断，对内可进行WEB访问、P2P、IM等应用进行审计。从而使网络的安全性得到提高，使应用和用户的行为能够可视化。部署图如下：



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

上海市闸北区广中西路777弄
88号华清大厦406室
邮编: 200072
电话: 021-6631 8601/02/03
传真: 021-6631 8601-800

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

成都市顺城大街308号
冠城广场7楼S座
邮编: 610017
电话: 028-8652 8597
传真: 028-8652 8306

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)。