

# Hillstone山石网科HSM (Hillstone Security Management™) 白皮书

## 概述

HSM是为了使企业和服务提供商可以很容易地管理多个设备，最大程度地降低了配置，管理，监控及维护设备的投入成本。支持企业和服务提供商集中高效地完成和管理多台设备的需求。

结合山石网科上网行为管理，为企业提供了全方位基于用户和应用的审计。可针对Web访问、论坛发帖、P2P、IM（即时通讯）、游戏等等进行细粒度审计，能够满足公安部82号令要求，提供长期的审计数据保存和维护。

通过集中的对全网设备进行状态监控、流量监控、行为分析，总结出用户网络的安全威胁和安全漏洞，通过保持持续的安全定义和策略的应用提高了系统的安全，最终构成安全闭环，达到动态安全防护。

## 产品架构

HSM系统分为三部分，即HSM代理（Hillstone Security Management Agent）、HSM服务器（Hillstone Security Management Server）和HSM客户端（Hillstone Security Management Client）。将这三部分合理部署到网络中，并且实现安全连接后，用户可以通过客户端程序，查看被管理安全设备的日志信息、统计信息、设备属性等，监控被管理设备的运行状态和流量信息。

## HSM代理

HSM系统对Hillstone安全设备进行管理和控制，因此，每台Hillstone安全设备运行的StoneOS都包含HSM代理模块，通过对代理模块的配置，使Hillstone安全设备与服务器相连，从而实现管理和控制。

## HSM服务器

HSM服务器是网管系统的管理中心，完成信息及数据的存储、分析和转发，实时接收并监控所有被管理设备的运行信息，实时接收安全告警消息，实时接收各种日志消息，且可提供长达半年的日志信息多条件查询和过滤。



## Hillstone山石网科HSM白皮书

系统使用曲线图显示设备的CPU利用率、内存使用率、会话数、总流量、VPN隧道数、攻击数以及病毒数。曲线图显示从当前时间到前30分钟的统计数据，统计数据信息每5秒钟刷新一次。

### 设备配置

用户可以通过HSM客户端登录到被管理的Hillstone安全设备并对其进行配置。HSM客户端支持通过Telnet和WebUI两种方式登录设备。

### 设备监控

#### VPN监控

HSM系统可以实时监控被管理设备的IPSec VPN和SCVPN隧道流量，并在客户端通过饼状图或者柱状图直观显示。

#### 流量监控

HSM系统可以实时监控以下对象的流量，并在客户端通过饼状图或者柱状图直观显示：

- 设备接口 (TOP 10)
- 指定接口TOP 10 IP，进而可以查看指定IP的TOP 10应用的流量
- 指定接口TOP 10应用，进而可以查看指定应用的TOP 10 IP的流量

柱状图可分别按照上行流量、下行流量或者总流量进行排序；饼状图可分别根据上行流量、下行流量或者总流量显示不同的百分比。



## Hillstone山石网科HSM白皮书

### 攻击监控

HSM系统可以实时监控以下对象的攻击情况，并在客户端通过饼状图或者柱状图直观显示：

- 设备接口遭受攻击（TOP 10）
- 指定接口发起攻击TOP 10 IP，进而可以查看指定IP发起的TOP 10攻击类型
- 指定接口TOP 10攻击类型，进而可以查看发起指定攻击类型的TOP 10 IP

### 病毒监控

HSM系统可以实时监控被管理设备的受病毒攻击情况，并在客户端通过饼状图直观显示。

### 日志浏览

HSM系统接收设备发送的多种日志信息，经过系统处理后，用户可通过客户端进行多维度、多条件的浏览。HSM支持通过以下种类进行日志浏览：

- 系统日志
- 配置日志
- 会话日志
- 地址转换日志
- 上网日志

序号	时间	源地址	目的地址	协议	状态	日志内容
518210	2009-03-19 12:20	62.118.0.164	www	80/TCP	0/0	http://62.118.0.164:80/
518211	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518212	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518213	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518214	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518215	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518216	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518217	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518218	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518219	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518220	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518221	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518222	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518223	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518224	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518225	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518226	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518227	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518228	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518229	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/
518230	2009-03-19 12:21	62.118.0.164	engine	80	0/0	http://62.118.0.164:80/

## Hillstone山石网科HSM白皮书

- 上网行为管理日志
  - ◆ 网页浏览日志
  - ◆ IM聊天日志
  - ◆ 文件传输日志
  - ◆ 论坛日志
  - ◆ 邮件日志

### 历史查询

HSM可查看历史监控信息，通过定义历史查询条件，包括指定查询参数和设置查询时间，进行历史数据统计和分析。历史数据统计包括以下几个方面：

- 监视数据趋势统计
- 流量统计
- 攻击统计
- 病毒统计
- VPN统计
- 上网行为统计



### 告警

#### 设备告警

HSM可以针对设备进行多层次监控，通过数据的采集和状态的监控，用户可根据各种需要定义告警条件，告警条件包括：

- 攻击次数、病毒数阈值

## Hillstone山石网科HSM白皮书

- 特征事件
- 关键字
- 日志级别

针对不同的告警条件，用户可定义不同的响应方式，目前响应方式包括：管理器显示提醒、声音告警等。

### 数据库告警

HSM的数据均存储在数据库中，数据库的正常与否决定了HSM系统的稳定性。因此系统针对数据库的进行了状态监控以及异常告警。用户可定义数据库空间百分比阈值，当数据库空间达到阈值时触发Email告警，用户也可以定义数据库空间百分比阈值清除旧数据，保障数据库可对最新的信息进行分析处理。

### 用户管理

HSM系统包含两种用户角色，分别是超级管理员和普通管理员，其权限说明如下：

- 超级管理员：超级管理员为最高权限管理员，可以通过客户端对所有设备做任何操作(添加、删除设备)，可以添加、删除以及编辑管理域，可以创建和删除普通管理员并为它们指定可管理域，可以修改普通管理员的权限。

- 普通管理员：普通管理员对其域内的设备的管理权限分为“只读”和“可编辑”两种(权限由超级管理员指定)。“只读”表示只可以查看域内设备的各类信息，例如设备属性和流量监控信息等；“可编辑”表示除“只读”权限外，还可以对设备进行编辑，例如设备分组等。

### 数据备份

HSM系统支持定期备份数据功能，用户可指定备份时间进行备份。备份的数据可进行查询，用户可以通过设置连接备份服务器查看已备份数据信息。

## 产品特点

### 可视化展现

- 基于设备面板状态监控
- 多维度图形化监控
- 设备集中状态监控

## Hillstone山石网科HSM白皮书

### 深层次审计分析

- 高性能数据处理能力
- 高容量数据存储
- 多应用数据挖掘和分析

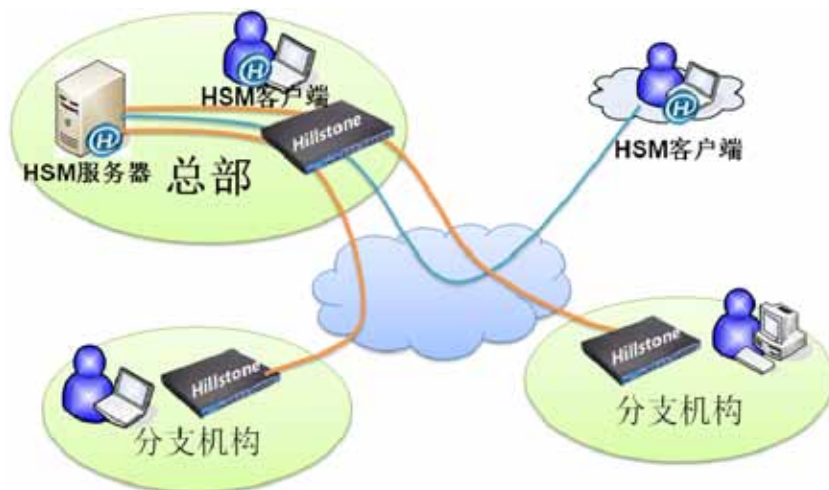
### 集中管理

- 多种协议方式管理
- 复杂网络环境应用

## 典型案例

### HSM应用场景

许多大中型企业在全国各地都建有分支机构或者办事处，当企业部署防火墙系统时会面临因分支机构众多而导致对整体安全系统的管理成本过高、整体监控难度过大的问题，集中管理方案的推出正是为了解决这一难题，具体的网络环境示意图如下。



### 软硬件环境

#### 硬件配置需求

HSM服务器对硬件的基本配置:

项目	参数
处理器	双核
内存	2GB
硬盘	240G

## Hillstone山石网科HSM白皮书

HSM客户端对硬件的基本配置:

项目	参数
处理器	双核
内存	1GB
硬盘	60G

### 软件配置需求

HSM服务器对软件的配置需求:

项目	参数
操作系统	32位Windows平台: 包括Windows 2003(推荐)、Windows XP或者Windows Vista
MySQL	mysql-5.1.33-win32.msi
JRE	jre1.6.0
Apache	apache_2.2.11-win32-x86-no_ssl.msi

HSM客户端对软件的配置需求:

项目	参数
操作系统	32位Windows平台: 包括Windows 2003(推荐)、Windows XP或者Windows Vista

#### 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)。