



Network Behavior Control

1. Introduction

Popularity of internet changes the life and working environment of many people. At the same time, traffic from intranet that cause bandwidth clogging, reduce work efficiency, information leakage, legal risks and security issues are becoming a bigger problem. For example, on company time, an employee maybe playing online games, downloading music and video, engaging in lengthy IM chats, leak company secret to the outside. They may also browse inappropriate web sites, make inappropriate posts or otherwise engage in illegal activities.

StoneOS provides license based Network Behavior Control to help administrator deal with this problem. Administrator can now control and manage network behavior of each user, and optimize the usage of network resource, effectively solve the issues that arises with internet usage.

2. Product Functionality

StoneOS Network Behavior Control (NBC) offers full management of user actions such as online game, IM, stock trading, P2P download, web surfing, outbound email and web posting. And based on different user, different actions and time period, offer flexible control and logging functionality. Working with Hillstone Security Management (HSM) system, user activity logs can be searched and audited, forming the bases for network administrators to manage the network.

NBC Policy

StoneOS NBC functions are implemented using policies. Administrator can have different NBC Policies for different set of users. The system will manage and control internet traffic based on the policies that has been set.

NBC Policy rules can be classified into three categories: Application Control Policy, Web Content Control Policy and Outbound Content Control Policy. Each category in turn have several different subcategories.

Network Behavior Control

Policy rule name, priority, user/user group/role, time schedule, network behavior and control action forms the basic elements of each NBC Policy. Configuring NBC Policy from WebUI, the following elements needs to be defined:

- Policy name – the name of a NBC policy
- Priority – determine the priority of the NBC policy. When a flow matches multiple NBC policy, the one with highest priority will be used.
- User – the user related to the NBC policy. This is the party initiating the network behavior, can be an user, user group, role, IP address etc.
- Time schedule – the effective time of the NBC policy. Can have different behavior control for different users at different time.
- Network Behavior – user activity that will be managed, for example, IM, web surfing, outbound email, BBS posting etc.
- Control Action – action taken for the network activity, for example, permit or deny, or log and audit the content of the network activity.

In above elements, user, time schedule and network behavior forms the condition of the policy, only the network activity that matches this condition will be controlled by this policy. The Control action is the action performed on the network activity that matches the condition.

Application Control Policy

Application Control Policy controls access of network applications. StoneOS categorize application into categories, such as online game, IM, stock trading, P2P, online video, etc. Each category contains specific application that can be controlled. Application control policy also includes rules that do fine grain control on FTP and HTTP protocol. Based on needs, administrator can do control based on category or individual application, assign different profile to different user at different times.

Web Content Control Policy

Web content control policy control user' s web access based on content. These policies can be divided into URL filtering policy and keyword filtering policy. URL filtering policy can be based on predefined URL categories or user defined categories, filtering user access to these web sites. Keyword filtering policy is based on user defined keyword and keyword category, filtering user access to web sites with matching content. This function can work with SSL decryption to filter HTTPS web sites that contain certain keyword.



Network Behavior Control

Outbound Content Control Policy

Outbound content control policy consists of Email control policy and BBS posting policy, and controls outbound information from the intranet. Email control policy can control outbound SMTP email or Webmail, based on email recipient, sender, content keyword, attachment, attachment size etc. Work together with SSL, this functionality can decrypt and control webmail that is HTTPS based. BBS posting policy can control outbound HTTP Post which match certain keyword, for example, block certain user from posting to a BBS that contain a certain keyword.

Exception Settings

For object that does not need to be controlled by NBC, administrators can setup exception lists. These exception lists can be users, black and white lists, and bypass domain names.

Exception Users

These are special users that will not be controlled by NBC policies. For example, administrators can put company executives or special departments into this group. StoneOS support IP subnets, IP range, user, user group, role or address book entry as exception users.

White List and Black List

White and Black List can setup special URL, when user visits these URLs, NBC policies can be bypassed. The visit can be permitted or denied unconditionally. There are following types of black and white lists:

- Black List: contains URLs that are not allowed. Each platform has a different limit on maximum number of URLs in this list.
- White List: contains URLs that are allowed. Each platform has a different limit on maximum number of URLs in this list.
- Keyword List: If URL contains keyword from keyword list, then visit to the URL is not allowed. Each platform has a different limit on maximum number of keywords in this list.
- Domain name Only Option: if this option is turned on, user can only browse internet using domain names. URLs that is based on IP addresses will be denied access.



Network Behavior Control

- White List Only Option: if this option is turned on, user can only access URLs in the white list, all other sites will be denied access.

Bypass Domains

Administrators can setup special domain names that will bypass NBC control, visit to these domain names will be allowed unconditionally.

Network Behavior Database

StoneOS network behavior databases include predefined URL database, user define URL database and keyword database. The predefined and user-defined URL databases provide URL categories for NBC policy to use. Administrators can filter and or specific categories of URL to be visited. Keyword database provide keyword category for NBC policy. Administrator can, through setting up proper NBC policy, perform keyword filtering of web browsing, outbound email and BBS posting.

Predefined URL Database

StoneOS contains a license controlled predefined URL database. Only after a license is installed, a platform that supports predefine URL database can start using it.

StoneOS predefined URL database are divided into 39 category, with a total number of URL exceeding 20,000,000 domains.

URL Database Update

By default, StoneOS will update predefined URL database every day. Administrators can change the update parameters if needed. Hillstone provides 2 default update servers: update1.hillstonenet.com and update2.hillstonenet.com. StoneOS also provide means to do online update or manual update if administrator so choose.

User Defined URL Database

Besides categories in predefined URL database, Administrators can also define user-defined URL category. User-defined URL category will also be displayed in system URL category list.



Network Behavior Control

Keyword Database

Administrators can define keyword categories, used for web page content filtering, outbound email keyword filtering and BBS posting keyword filtering.

Logging

StoneOS maintains full logs for NBC activities, including logs for online games, IM with chat content, stock trading, FTP/HTTP usage, P2P download, online video, web surfing, outbound email with content and attachment, BBS posting etc. These logs provide the complete information for data mining. HSM (Hillstone Security Management) system can search, analyze and audit based on this information.

3. Product Characteristics

URL Category Control

- 39 URL Categories
- Over 20 million URLs, updated in real time

Application Identification and Control

- Closely follow application characteristics and application evolution. Application database is published periodically
- Cross inspection of application data, enhanced accuracy of identification
- Multiple ways of control, better than simple blocking of IP address

Device Independent Logging Facility

- Alleviate performance impact of log analysis to the gateway
- Pluggable storage support

Network Behavior Control

4. Deployment Scenario

Network behavior control, as a part of Hillstone UTM Plus, works in concert with access control, QoS, IPS etc to provide a security barrier at the network access point. It can defend against attacks and illegal access from the outside. And at the same time, it can audit and control web access, applications such as P2P and IM. All this help improve the security of the network by provide visibility into network traffic, application and user behavior.

