

Hillstone Application Identification

Overview

People engage in a variety of activities online today, for example, online stock trading, online gaming, online multimedia, instant messaging, P2P download etc. Many programs and services emerge to support these activities and these are categorized as network applications. Over the years, network applications as a whole dramatically change ways that people conduct their business and daily lives.

What is the relationship between network applications and security? It is well known that Internet applications cannot be identified with ports and protocols alone. In another word, they cannot be controlled just by looking at layer 3 properties. One example is BitTorrent traffic can use multiple seemingly random ports at the same time. Traditional security technology, including stateful inspection and packet filtering, can no longer secure against these applications. Identification of these applications will involve layer 4 to 7 information, as well as behavior and traffic patterns.

Application Identification

Network applications may not all be well behaved, some hungry for network bandwidth, other may contain malware or otherwise carries illegal traffic. Normal business traffic such as office applications or video conferencing may not get enough bandwidth. Activities against company policies maybe engaged without the knowledge of the system administrators. How to maintain smooth operation of mission critical applications while controlling others.

Effective traffic control and security defense start with network visibility. How can you control something that can not be seen.

Network Visibility

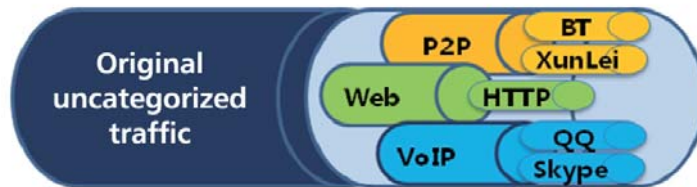
First, to achieve network visibility, packets through the device has to be categorized. Only after gaining knowledge about application and user traffic and utilization, can administrators start controlling the traffic and optimize the network.



Network visibility brings a new angle of security management. Before, the administrators need to know application as ports and protocols in order to exercise control. For applications that go through proxies, or those using dynamic ports, this old way does not work. Network visibility gives administrator a visual and intuitive way of managing the network.

Network Application Categorization

The number of network applications are in the thousands, and it would be a tremendous task to control them one by one. It would be much easier to control applications by categories, for example BT and Emule are different types of P2P downloading, QQ and MSN are instant messaging applications, and Youtube and Metacafe are online video sites.



There may exist a misconception that the more categories there are, the better the requirements can be satisfied. This is not true. In real life, understanding of the application is neither in the protocol level, such as TCP, UDP, nor the technical level, such as BT control vs data traffic. More reasonably, people focus on the functionalities of application, e.g., QQ contains the following functions: QQ text chat, QQ voice, QQ video, QQ file transfer, and so on. As long the applications are categorized properly, the management tasks are greatly reduced.

Network Application Updating

Everyday, some old network applications upgrade and some new applications emerges. Network application identification must be based on a dynamic updating service, just like anti-virus or intrusion prevention signatures. Continuous and frequent updating service is a must-have for effective application identification capability.

To keep track of a wide range of network applications and maintain accurate signatures, a local service and support team is required to follow the latest trends of applications, update identification engine, and release application signature updates periodically.

Hillstone Application Identification

Hillstone application identification adopts the state-of-the-art cross inspection engine, besides identifying based on application signatures, cross inspection can be performed within single packet, across multiple packets, across multiple sessions, and user history analysis. This multi-engine approach improves identification accuracy. Hillstone application identification cross inspection engine analyzes applications on three levels: packet level, session level, and user level.

Packet Level Inspection

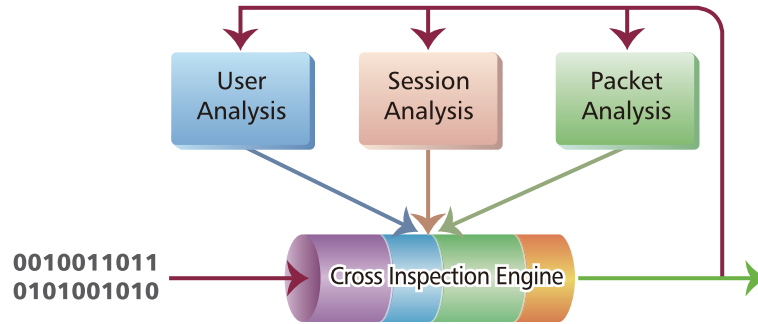
Hillstone cross inspection engine takes the following steps to identify applications: the engine extracts application signature vectors from the packets, and then matches the vectors with signatures in the database to perform application identification. In addition, the engine also performs statistical analysis according to the prevalence and hit rate of the signature. Based on the statistical result, the engine adjusts the identification priority dynamically to improve the identification accuracy.

Session Level Inspection

Hillstone cross inspection engine analyzes application signatures of multiple sessions and multiple packets inside one session. For encrypted SSL sessions, the engine can decrypt the packet before doing inspection.

User Level Inspection

Hillstone cross inspection engine also analyzes historical behavior of users and their use of application. This information is also used to identify future traffic flows of the same user.



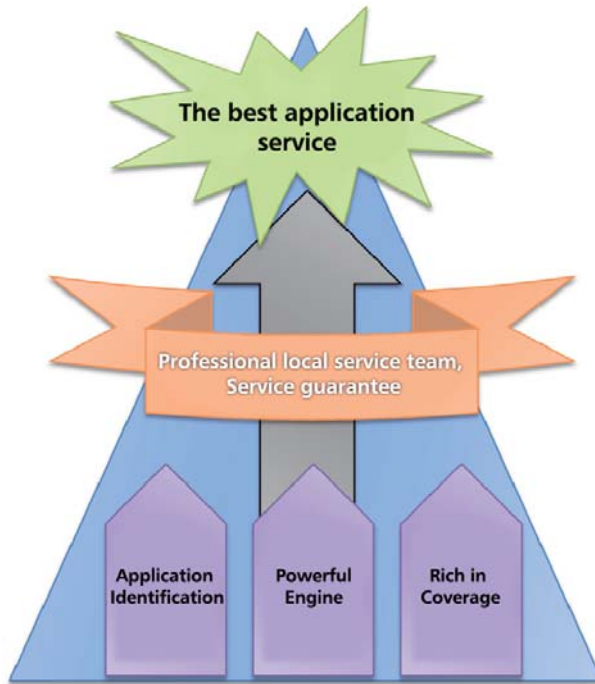
Hillstone Application Database

Hillstone application signature database includes about 7 main categories divided into 24 sub-categories. Nearly all commonly used applications are contained in the database. For detailed information about categories, see the table below:

Category	Sub-category
Communication	IM VoIP
Network software	Common network software P2P software Network tool File sharing Social network Anti-virus Stock software
Multi-media	Stream media P2P stream media
Business software	ERP Email Database
Game	Puzzle game Online game
Network protocol	Directory service Encrypted tunnel Routing protocol Network management Session

Hillstone Application Service

Hillstone has a dedicated professional network application service team, in which all the members are engineers experienced in the network application analysis.



Hillstone Networks, Inc.

US Office

239 West Hunter Lane
Fremont, CA 94539, USA
Tel: +1(510)856-5505
Fax: +1(510)279-5959

China Office

3F HuiZhong Plaza, No.1 ShangDi 7th Street
Haidian, Beijing, P.R. China 100085
Tel: +86(10)8289-7229
Fax: +86(10)8289-9814

Copyright © 2011 Hillstone Networks, Inc. All rights reserved.

Hillstone, Hillstone Networks, Hillstone logo, StoneOS, StoneManager, Hillstone PnPVPN, Multi-Core Plus, SG-6000-X6150, SG-6000-X5100, SG-6000-G6100, SG-6000-G5150, SG-6000-G3150, SG-6000-G2120, SG-6000-G2110, SG-6000-M6115, SG-6000-M6110, SG-6000-M3108, SG-6000-M3105, SG-6000-M3100, and SG-6000-M2105 are registered trademarks of Hillstone Networks. All other trademarks or registered marks are the property of their respective owners. Hillstone Networks assumes no responsibility for any inaccuracies in this document. Hillstone Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Hillstone Networks Website www.hillstonenet.com posts the latest information.