Evergreen Application Protocols: Validate Network Equipment With Always-Current Application Traffic

BreakingPoint Research Team Provides Constant Updates for Applications That Are Critical in Validating Lawful Intercept, Data Loss Prevention, and Deep Packet Inspection Devices

In today's rapidly evolving networks, popular application protocols change on a daily basis. Meanwhile, content-aware networking equipment makes decisions about traffic by looking deeper into it than ever before. Devices that handle the most popular application protocols are at a severe disadvantage if they are not tested using the most up-to-date versions of the protocols.

The BreakingPoint Evergreen Applications program addresses this need by providing ever-current versions of popular Web and network applications. It expands upon BreakingPoint's Application and Threat Intelligence (ATI) repository of 150+ application protocols and 30,000+ security attacks. With BreakingPoint Evergreen Applications, customers focused on advancing the capabilities of deep packet inspection (DPI), Lawful Intercept (LI), and Data Loss Prevention (DLP) products can now do so using the most current application and attack traffic.

Maintaining Currency for the Most Popular Mail and Messaging Protocols

Each week, an ATI engineer reviews the Evergreen Application Protocols for changes to their attributes. These protocols were chosen based on specific requests from BreakingPoint's DPI, LI, and DLP customers Each significant change to one of these protocols initiates a protocol update that is then distributed to customers through an ATI release. These are the Evergreen

Application Protocols supported:
- AOL Messaging
- AOL Webmail
- Google Mail (Gmail)
- Google Talk
- ICQ
- Jabber (XMPP)
- MSN Messaging
- Windows Live Mail
- Yahoo! Mail
- Yahoo! Messaging

Contact NextGig Systems, Inc. 805-277-2400 www.NextGigSystems.com

Flexible Product Architecture and Dedicated Research Team Deliver Unprecedented Testing Capabilities

Evergreen Application Protocols are just part of BreakingPoint's commitment to enabling customers to test the resiliency of applications, devices, networks, and data centers under the most authentic conditions possible. Because of their exclusive design, BreakingPoint CTMs evolve along with the frequent changes in the landscape for applications, attacks, telecommunication standards, and more.

BreakingPoint ATI releases are provided on a nearly weekly basis and contain updates responding to customer requests, the latest advances in application protocol technology, and emerging network threats. These updates also often contain entirely new features and performance enhancements for the BreakingPoint CTM. As a result, each BreakingPoint CTM enables you to:

- Validate device capabilities by re-creating more than 150 application protocols, including FIX, IBM DB2, VMware® Vmotion™, HTTP, Microsoft® CIFS/SMB, MAPI, Oracle, Encrypted BitTorrent™, RTSP, RTP, SSL, Facebook®, Twitter Mobile, YouTube®, MSN® Nexus, RADIUS, SIP, Skype™, World of Warcraft®, and many other enterprise, social, and gaming protocols—with multicast support.
- Stress network and security devices with constantly updated libraries of more than 4,500 security attacks and 28,000 pieces of malware— including mobile malware—plus obfuscations and evasions.
- Employ built-in network traffic profiles created by BreakingPoint engineers using data collected from top global telecom carriers and other enterprises, or easily customize these profiles to fit your own network's unique conditions.
- Validate LI, DLP, and DPI solutions with scenarios that deliver "needle" phrases via multiple communications protocols in a massive digital "haystack" of content in various languages.

- Employ the optional Custom Application Toolkit for even more customization of application traffic and testing scenarios.

Ensure the accuracy and validity of network device evaluations, security testing, and more with Evergreen Application Protocols and the BreakingPoint ATI Program.

BreakingPoint FireStorm CTM Specifications

A single BreakingPoint FireStorm CTM provides the equivalent performance of many racks of servers from a 4U chassis, including:
- 120 gigabits per second of blended stateful application traffic
- 90 million concurrent TCP sessions
- 4 million TCP sessions per second
- 1.5 million steady-state complete TCP sessions per second
- 120,000+ SSL sessions per second
- 150+ stateful application protocols
- 4,500+ live security attacks
- 1 Gigabit Ethernet and 10 Gigabit Ethernet interfaces

Set up a demonstration contact

NextGig Systems, Inc.
805-277-2400
www.NextGigSystems.com

BreakingPoint Research Center
- Network surveillance
- In-house research
- Vendor advisories
- Independent Researchers
- Strategic operating system vendors
- Service provider feeds

Application and Threat Intelligence updates
- New Applications
- New Attacks
- New Features

BreakingPoint
Find it before they do.™

Contact NextGig Systems, Inc. 805-277-2400 www.NextGigSystems.com