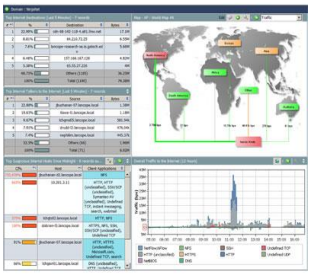
GAMBIT COMMUNICATIONS CASE STUDY

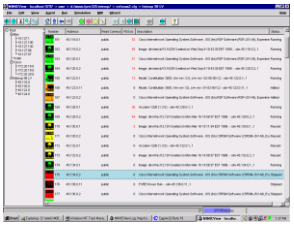
Lancope®

"MIMIC is an excellent resource for us. It helps ensure that the StealthWatch System is thoroughly tested against the most commonly used NetFlow-capable networking devices."

Byron Turner, Director of QA, Lancope,



StealthWatch System showing various traffic patterns of a large network using MIMIC Simulator.



***MIMIC NetFlow Simulator** creating a virtual lab with hundreds of devices.*

Lancope leverages MIMIC® NetFlow Simulator for StealthWatch® System testing, demonstrations and training

Lancope is a leading provider of network visibility and security intelligence to protect enterprises against today's top threats. By analyzing NetFlow, IPFIX and other types of network telemetry, Lancope's StealthWatch® System delivers Context-Aware Security Analytics to quickly detect a wide range of attacks from APTs and DDoS to zero-day malware and insider threats. Combining continuous lateral monitoring across enterprise networks with user, device and application awareness, Lancope accelerates incident response, improves forensic investigations and reduces enterprise risk.

Challenges:

Lancope engineers are continuously working to ensure that the StealthWatch System is thoroughly tested against the most commonly used NetFlow-capable networking devices. In the past the company used NetFlow generators and physical devices to gather various kinds of network traffic, but found it challenging to generate predictable traffic from a physical device. NetFlow generators allow generation from only one exporter at a time, and are difficult to configure for the variety of scenarios needed for testing. Lancope decided to use MIMIC NetFlow Simulator from Gambit, because it allowed them to easily create very predictable traffic from multiple flow sources.

Solution:

The MIMIC NetFlow Simulator generates a variety of flows and enables organizations to fully test their applications. Lancope currently uses multiple MIMIC copies for testing, customer support, training and demonstrations. Recently, Lancope's QA group started using MIMIC for regression, performance, scalability and feature testing.

The MIMIC NetFlow/SNMP Simulator immediately provided high performance and scalability for generating NetFlow, IPFIX, sFlow and SNMP traffic. Engineers can simulate hundreds of Cisco switches and other devices (exporters), each generating thousands of flows per second. It is easy to create predictable traffic with MIMIC and compare the results with previous tests. MIMIC's user-friendly GUI makes it easy to generate a wide variety of flows with configurable source and destination addresses, time intervals, protocols and custom template fields. Along with NetFlow traffic, the StealthWatch System is also tested for polling of simulated device interfaces (ifIndex, interface name, interface speed, etc.) using SNMP.

Using the MIMIC Flow Simulator, Lancope can simulate network and security "issues" such as asymmetric routing, flooding, bad flags generation, creating single IP with multiple user name (like a proxy server), address or port scan. These features help in testing the support for the detection of various Botnets, DDoS attacks, insider threats and spread of malware.

The StealthWatch System handles hundreds of thousands of flows per second and analyzes threats from multiple exporters. MIMIC made it much easier to test that scalability with a fraction of their lab budget.

For more information:
Please contact **Gambit Communications**: info@gambitcomm.com **www.gambitcomm.com**