

# Executive Summary for Arbor/Cisco Clean Pipes 2.0 Solution Functional and Performance Test Results

## Objective

To test and certify Cisco/Arbor Clean Pipes v2.0 and demonstrate on-demand mitigation capability, empowered by timely and accurate attack detection, classification and trace back.

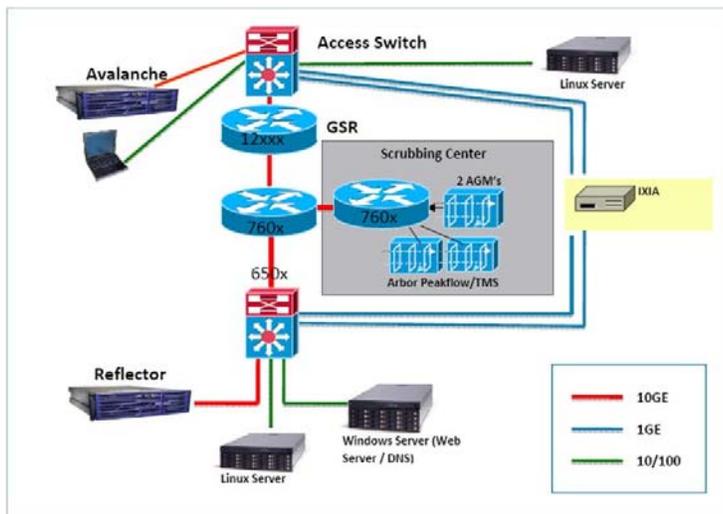
## Products Tested

The Arbor Networks® Peakflow® SP and Peakflow SP Threat Management System products (“Peakflow SP”) (“Peakflow SP TMS”) were tested.

## Summary of Functional and Performance Tests

- Detection and mitigation of attacks from spoofed and non-spoofed source IP addresses.
- Detection and mitigation of TCP connection-based attacks.
- Packets-per-second (pps) performance measurements.

## Test Bed



## Conclusions (Please refer to actual document for individual test results.)

- “Results have shown that the Peakflow SP and Peakflow SP TMS solutions have the capability to detect and mitigate a wide variety of distributed denial of Service (DDoS) threats representative of those seen on the Internet today.”
- “Results of the functional and performance tests validate that the Peakflow SP/TMS solution is a recommended migration path for customers with Cisco Guard deployments.”

# HTTP Attack Tests

## Spoofed:

Attack Type	Counter Measure
SYN Flood	TCP SynAuth
SYN-ACK Flood	TCP SynAuth
FIN Flood	TCP SynAuth
ICMP Flood	Black/White List
ICMP-Frag Flood	Invalid Packets
UDP-Frag Flood	Invalid Packets
TCP-Frag Flood	Invalid Packets
DNS Flood	Zombie Detection or Payload Regular Expression
SYN Flood	TCP SynAuth

## Non-Spoofed:

Attack Type	Counter Measure
SYN Flood	TCP SynAuth
SYN-ACK Flood	TCP SynAuth
FIN Flood	TCP SynAuth
ICMP Flood	Black/White List
ICMP-Frag Flood	Invalid Packets
UDP-Frag Flood	Invalid Packets
TCP-Frag Flood	Invalid Packets
DNS Flood	Zombie Detection or Payload Regular Expression
SYN Flood	TCP SynAuth

## Attack Environment:

• Legitimate HTTP traffic consisting of 50 connections per second (cps), with 10 KB of response per connection. Overall 70 Kpps of uplink (client to server) traffic.

• For spoofed attacks, the attack traffic consisted of: 200 Kpps packet flood, 64 bytes per packet, 16.7 million source IP addresses

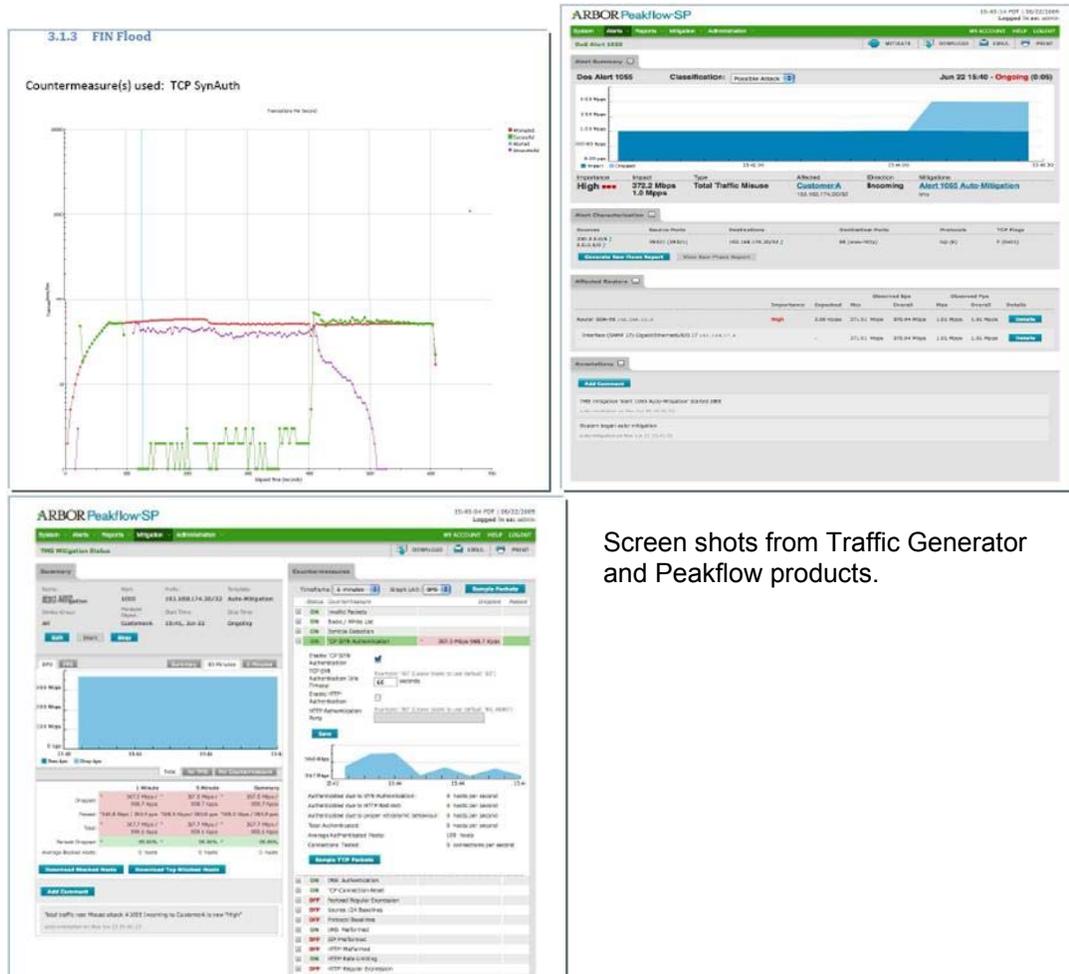
• Non-spoofed attack traffic consisted of: 200 Kpps packet flood, 64 bytes per packet, 100 source IP addresses.

• In parallel, a low rate of legitimate HTTP traffic was generated from the same 100 source IPs using http load on the Linux client. This legitimate traffic created host authentications to bypass the TCP SynAuth countermeasure.

• Peakflow SP detects the attack and automatically triggers the TMS to start mitigation.

• After the mitigation is started, Avalanche real-time graphs show that the legitimate traffic is restored.

Example of Test Results (refer to actual document for details).



Screen shots from Traffic Generator and Peakflow products.

## Performance Tests

Test: Attack	Countermeasure	Results
<b>Black List:</b> SYN flood, 64 bytes per packet, 16.7 million source IPs (randomized over /8)	Black/White List filter constructed to drop attack traffic by source IP subnet.	Maximum attack rate before impact on legitimate traffic: <b>~3.75 Mpps</b>
<b>Syn Authentication:</b> SYN flood, 64 bytes per packet, 16.7 million source IPs (randomized over /8)	TCP Syn Auth with HTTP Auth	Maximum attack rate before impact on legitimate traffic: <b>1.55-1.7 Mpps</b>
<b>Regular Payload Expression:</b> UDP flood containing the string "abcdefgh" in the payload. 16.7 million source IPs (randomized over /8)	Regex used for filtering: abc.*fgh	<p><b>Packet size: 72 bytes, regex hit &amp; miss.</b> Maximum attack rate before impact on legitimate traffic: <b>~2.8Mpps &amp; ~2.8Mpps</b></p> <p><b>Packet size: 256 bytes, regex hit &amp; miss.</b> Maximum attack rate before impact on legitimate traffic: <b>~2.8Mpps &amp; ~2.25Mpps</b></p> <p><b>Packet size: 512 bytes, regex hit &amp; miss.</b> Maximum attack rate before impact on legitimate traffic: <b>~2.28Mpps &amp; 1.5 Mpps</b></p>

*For more information regarding Arbor Peakflow solutions, please contact your Arbor representative or visit [www.arbornetworks.com](http://www.arbornetworks.com)*



#### Corporate Headquarters

6 Omni Way  
Chelmsford, Massachusetts 01824

Toll Free USA +1 866 212 7267

T +1 978 703 6600

F +1 978 250 1905

#### Europe

T +44 208 622 3108

#### Asia Pacific

T +65 6327 7152

[www.arbornetworks.com](http://www.arbornetworks.com)

Copyright © 1999-2009 Arbor Networks, Inc.  
All rights reserved. Arbor Networks, the  
Arbor Networks logo, Peakflow and ATLAS  
are all trademarks of Arbor Networks, Inc.  
All other brands may be the trademarks  
of their respective owners.

#### About Arbor Networks

Arbor Networks is a leading provider of secure service control solutions for global business networks. Its customers include a majority of the world's ISPs and many large enterprises. Arbor solutions deliver best-in-class network security and visibility, along with the power to improve profitability by deploying differentiated, revenue-generating services. By employing flow-based and deep packet inspection (DPI) technologies, Arbor solutions measure and protect the entire network—from the network core to the broadband edge. Arbor also maintains the world's first globally scoped threat analysis network—ATLAS—which uses technology embedded in the world's largest ISP networks to sense and report on comprehensive worldwide threat intelligence.