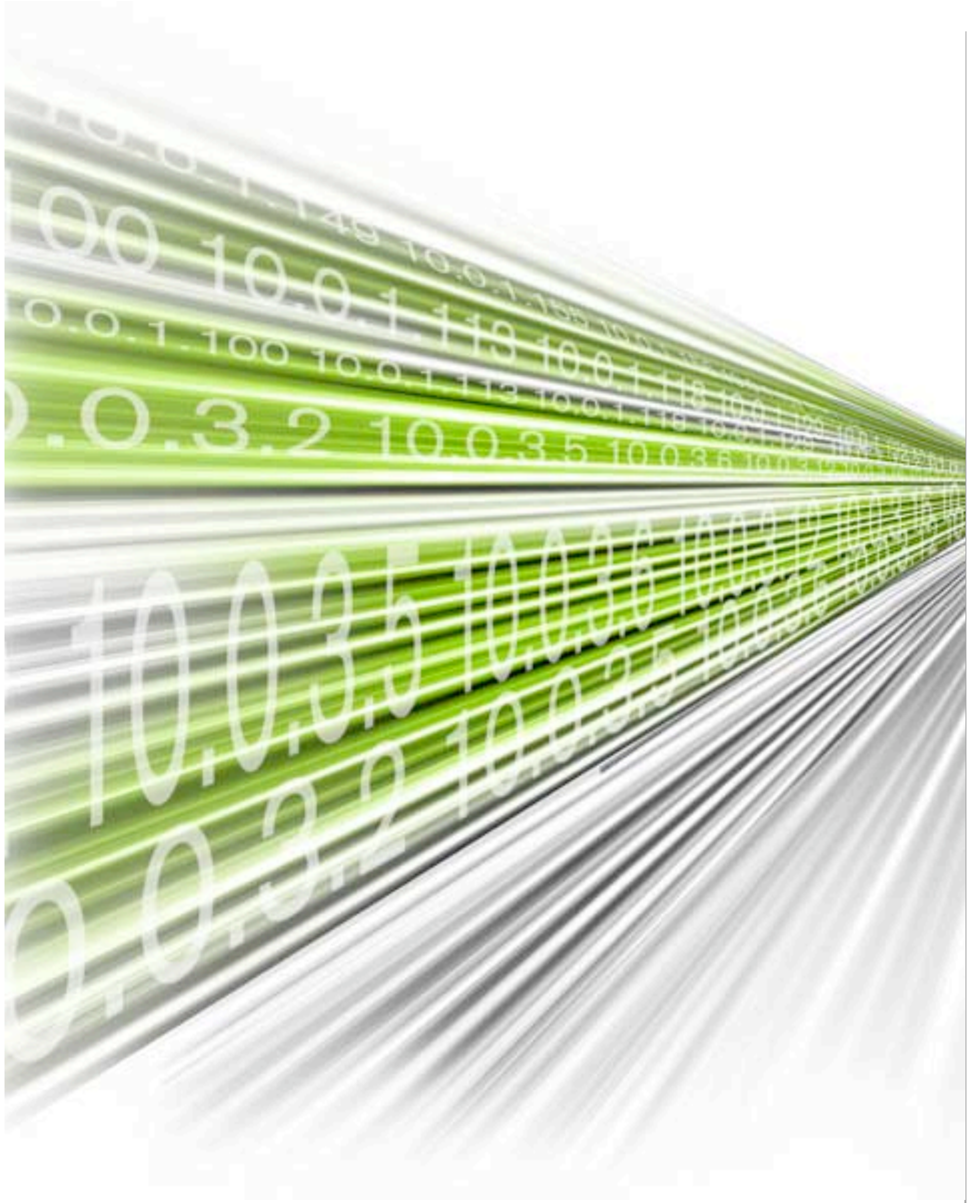


Threads in the Public Internet

Gerhard Schmid

Sales Director C&EE,ME

Agenda

- Introduction to Arbor Networks
  - Our unique ability to conduct this survey
- Worldwide Infrastructure Security Report v5
  - Overview of Report
  - Key Findings
  - Conclusions
- Questions?

Arbor Networks

ARBOR® NETWORKS

How networks grow™

- Founded in 2000
- 270 employees in 20+ countries
- 300+ customers
  - 90%+ of Tier1 providers, 60%+ of Tier2 providers, 11 of 13 of NA MSOs

Arbor's Vision:

Ensure the security, availability and profitability of the 21st century IP network.

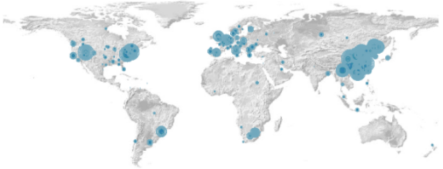
ARBOR® NETWORKS

Industry Thought-Leaders

- **Trusted Advisors on Internet Management, Security & Trends**
  - In December 2009, Arbor testified at House of Lords Select Committee of the European Union (EU) for an inquiry into EU policy to protect Europe from large-scale cyber-attacks
  - Active members of industry standard groups (i.e., IETF, IAB), regional operations groups (i.e. NANOG, RIPE, APRICOT) and other security forums (ICANN/SSAC)

- **Privileged Relationships with Majority of World's ISP**
  - 100+ ISPs sharing statistics, real time attack, routing and dark IP data.
  - Annual Worldwide Infrastructure Security Report.

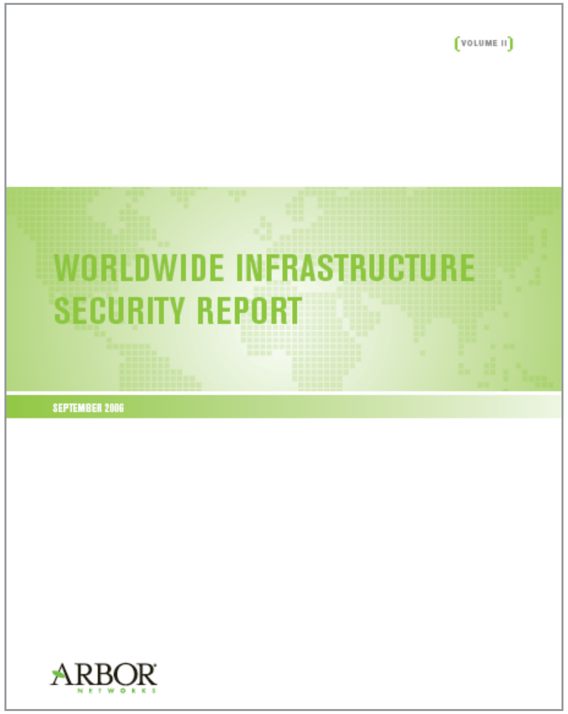
- **Arbor's Security Engineering & Research Team (ASERT)**
  - Active Threat Feed, Fingerprint Sharing Alliance
  - ATLAS – Global Threat Analysis: atlas.arbornetworks.com
  - Blog: asert.arbornetworks.com



ARBOR® NETWORKS

5th Annual Report: 3Q 2008 – 3Q 2009

- **Demographics:**
  - 132 self-classified IP network operators from Americas, Europe, Africa and Asia.
  - ***Double the participation vs. last year*** (66 respondents)
  - All participants are directly involved in operational security .
  - Major demographic expansion to include Tier-1 and Tier-2/3
- **Focus:**
  - Daily operational network security issues in commercial networks.
  - More accurate representation of real-world concerns vs. theoretical and speculated emerging trends.



(VOLUME II)

WORLDWIDE INFRASTRUCTURE SECURITY REPORT

SEPTEMBER 2006

ARBOR NETWORKS

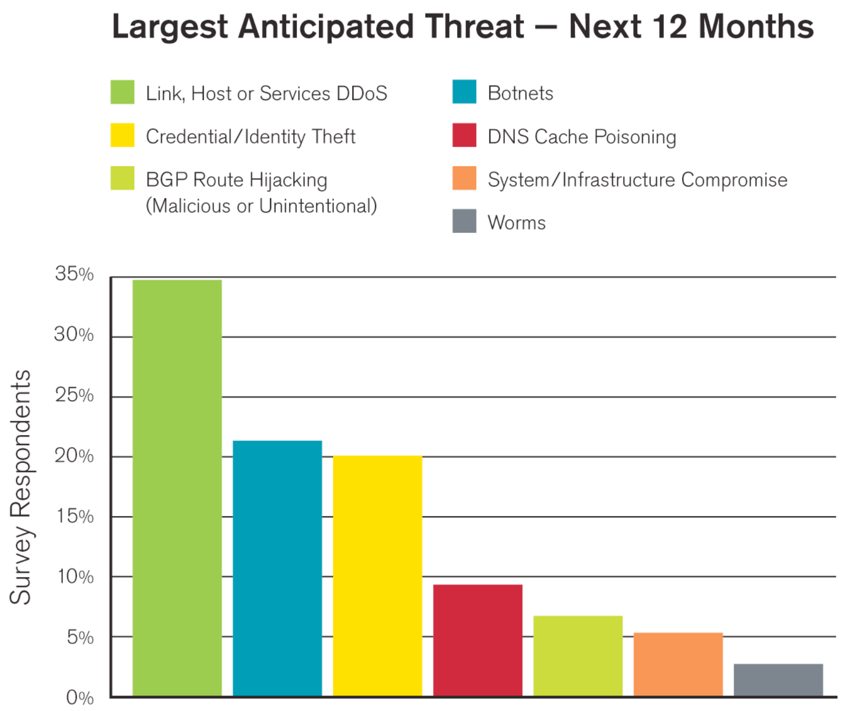
- **Objective:**
  - Enable informed decisions about the use of network security technology for protection of mission-critical infrastructure.
  - Be a general resource for trends and employment of various infrastructure security techniques.

Key Findings

- ✓ Attacks Shift to the Cloud
- ✓ DDoS Attack Size Still on the Rise, But at a Slower Pace
- ✓ Internet Architecture and Operations Facing Perfect Storm
- ✓ The Internet Is *Not* IPv6 Ready

Attacks Shift to the Cloud

- #1 security threat to the adoption of the cloud computing model
- Attacks crafted to exploit architectural and operational weaknesses.
- Several ISPs reported multi-hour outages of prominent Internet services due to application-level attacks
- Primary threat vectors for attacks targeting the cloud
  - ✓Domain Name System (DNS) infrastructure
  - ✓Firewalls, Load balancers
  - ✓Large-scale SQL server back-end infrastructure



Source: Arbor Networks, Inc.

DDoS Attack Size Still on the Rise, But at a Slower Pace

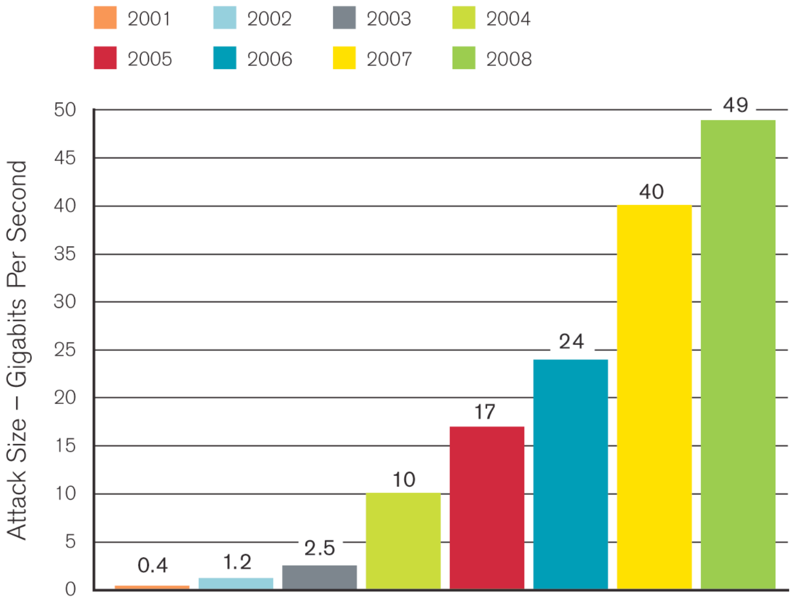
- The largest attack reported was 49 Gbps

- The largest sustained attacks reported were 40 Gbps and 24 Gbps, respectively

- However, DDoS attack scale growth has actually slowed over the past 12 months in comparison to previous years

- 2007-2008 Growth: 67%
- 2008-2009 Growth: 20%

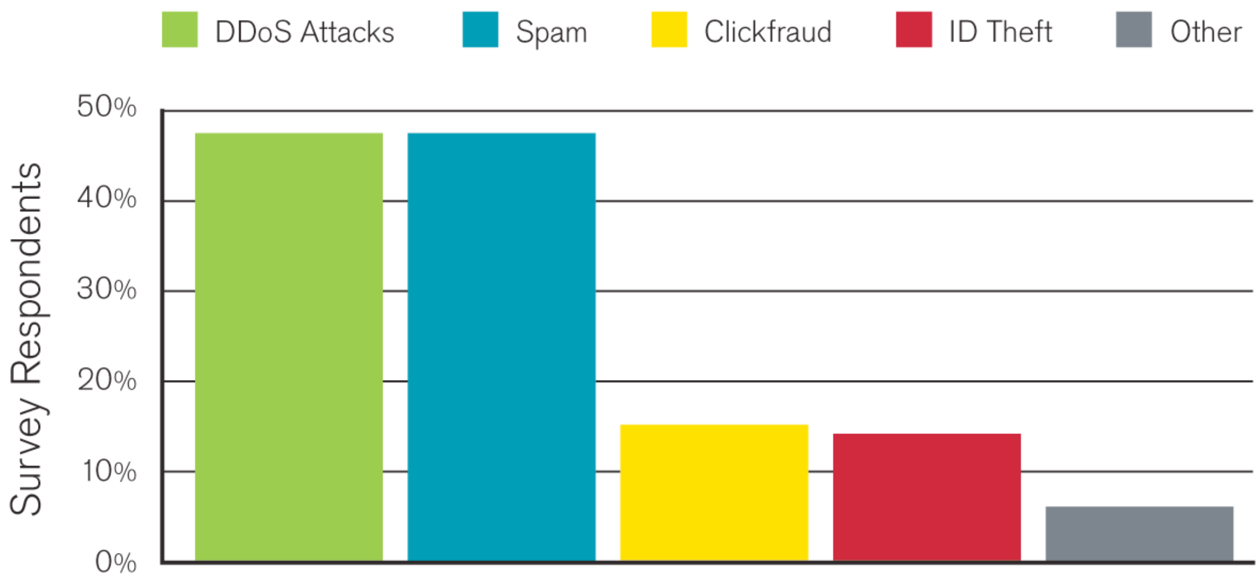
Largest DDoS Attack – 49 Gigabits Per Second



Source: Arbor Networks, Inc.

Botnet Activity – Driven by Spam and DDoS Attacks

- Unsurprisingly, spam and DDoS share the top spot, for botnet-based activity



Observed Bots — Past 12 Months

Source: Arbor Networks, Inc.

Internet Architecture and Operations Facing 'Perfect Storm'

- Looming IPv4 address exhaustion and the preparedness for migration to IPv6, DNSSEC and to 4-byte ASNs are contributing to a “perfect storm” scenario for Internet architecture and operations professionals

- Any one of these changes would constitute a significant architectural and operational challenge for network operators;

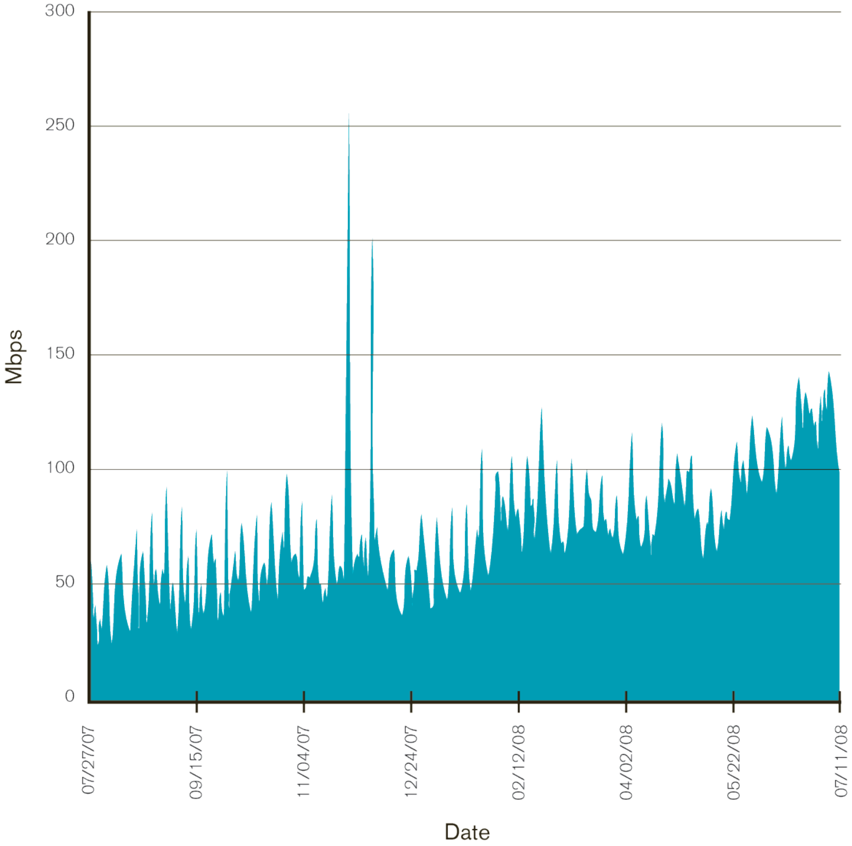
- Considered together, they represent the greatest and potentially most disruptive set of circumstances in the history of the Internet

The Internet is NOT IPv6 Ready

Concerns:

- ✓ IPv6 is still viewed as unproven
- ✓ There is a lack of IPv6 tools and knowledge in operations
- ✓ IPv6 network infrastructure functionality lacks parity with IPv4,
- ✓ Management does not understand the need to invest in preparation for IPv6 interoperation and support

Service Total Observed Inter-Domain IPv6 Traffic



Source: Arbor Networks, Inc.

Conclusions

- The Internet engineering, operational, and security communities are struggling with the rapid evolution of complex security challenges
  - While peak DDoS attack rates did not exceed the 2007 fears of 60-80 Gbps (see last year's survey), providers report that gigabit attacks are now commonplace
  - The complexity of cloud and multi-tenant infrastructure significantly increases the vulnerability of customer-visible services due to the fate-sharing implicit in multi-tenancy
- Any ISP optimism about security issues has been replaced by growing concern over a range of new threats, including DNS poisoning, route hijacking and service-level attacks
  - Though a few providers believe they still have a technical advantage against attackers, this year's survey in part reflects a new general pessimism
- The 'perfect storm' of IPv4 address exhaustion, IPv6 deployment, DNSSEC deployment, and 4-byte ASN support are a source of concern from an architectural, operational, and security standpoint
  - The implementation of these technologies will undoubtedly alter the operational security posture of Internet-connected networks

Additional Arbor Peakflow SP Resources

Visit: www.arbornetworks.com

- Datasheets:

[DATA SHEET]

Arbor Peakflow® SP

[DATA SHEET]

Arbor Peakflow® SP
Threat Management System

[DATA SHEET]

Arbor Peakflow® SP
Flow Sensor

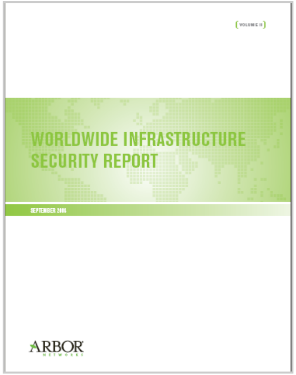
[DATA SHEET]

Arbor Peakflow SP
Business Intelligence

[DATA SHEET]

Arbor Peakflow SP
Portal Interface

- Solution Briefs, FAQs, Special Reports, Blog etc:



[VOLUME II]

WORLDWIDE INFRASTRUCTURE
SECURITY REPORT

SEPTEMBER 2006

ARBOR NETWORKS

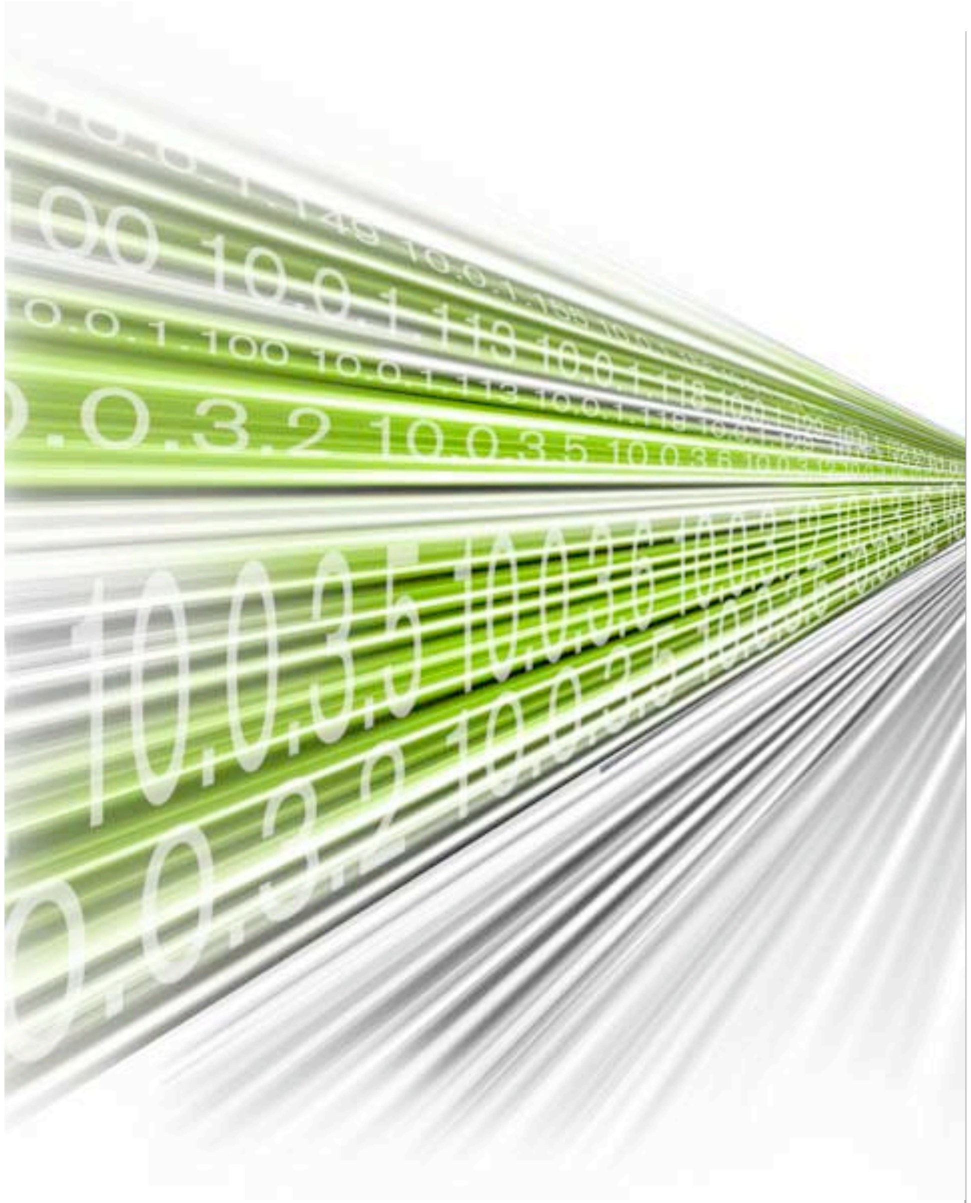
[SOLUTION BRIEF]

Covad Communications Ramps Up
Network Security and Performance
with Arbor Peakflow SP

A|SERT

How to Leverage Arbor Products and Services
to Deliver New Managed Services

ARBOR® NETWORKS



Questions?

Thank You

Gerhard Schmid
+49 89 96 99 88 80
gschmid@arbor.net

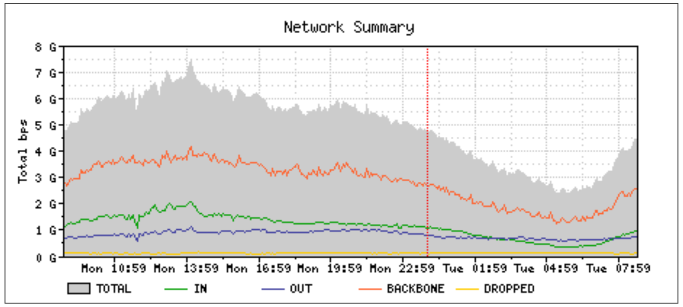
The Peakflow SP Solution

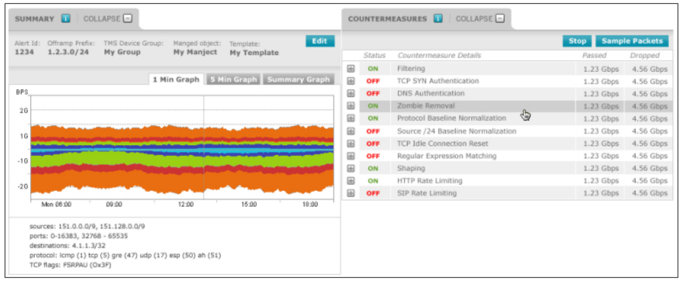
Pervasive and cost-effective visibility and security!

- Pervasive Network Visibility & Deep Insight into Services
  – Leverage “IP flow” technology for broad network visibility; and deep packet inspection (DPI) for insight into applications and services.

- Comprehensive Threat Management
  – Detection, surgical mitigation and reporting of DDoS and application-layer attacks that threaten business services.

- In-Cloud Services Enabler
  – A platform which offers the ability to deliver new, profitable, revenue-generating services (i.e DDoS Protection and MPLS VPN Visibility).





Alert Id: 1234
Offramp Prefix: 1.2.3.0/24
TMS Device Group: My Group
Manged object: My Manject
Template: My Template

sources: 151.0.0.0/9, 151.128.0.0/9
ports: 0-16383, 32768 - 65535
destinations: 4.1.1.3/32
protocol: icmp (1) tcp (5) gre (47) udp (17) esp (50) ah (51)
TCP flags: FSRPAU (0x3F)

Status	Countermeasure Details	Passed	Dropped
ON	Filtering	1.23 Gbps	4.56 Gbps
OFF	TCP SYN Authentication	1.23 Gbps	4.56 Gbps
OFF	DNS Authentication	1.23 Gbps	4.56 Gbps
ON	Zombie Removal	1.23 Gbps	4.56 Gbps
ON	Protocol Baseline Normalization	1.23 Gbps	4.56 Gbps
OFF	Source /24 Baseline Normalization	1.23 Gbps	4.56 Gbps
OFF	TCP Idle Connection Reset	1.23 Gbps	4.56 Gbps
OFF	Regular Expression Matching	1.23 Gbps	4.56 Gbps
ON	Shaping	1.23 Gbps	4.56 Gbps
ON	HTTP Rate Limiting	1.23 Gbps	4.56 Gbps
OFF	SIP Rate Limiting	1.23 Gbps	4.56 Gbps

Peakflow SP
Comprehensive Visibility & Security

Peakflow SP CP

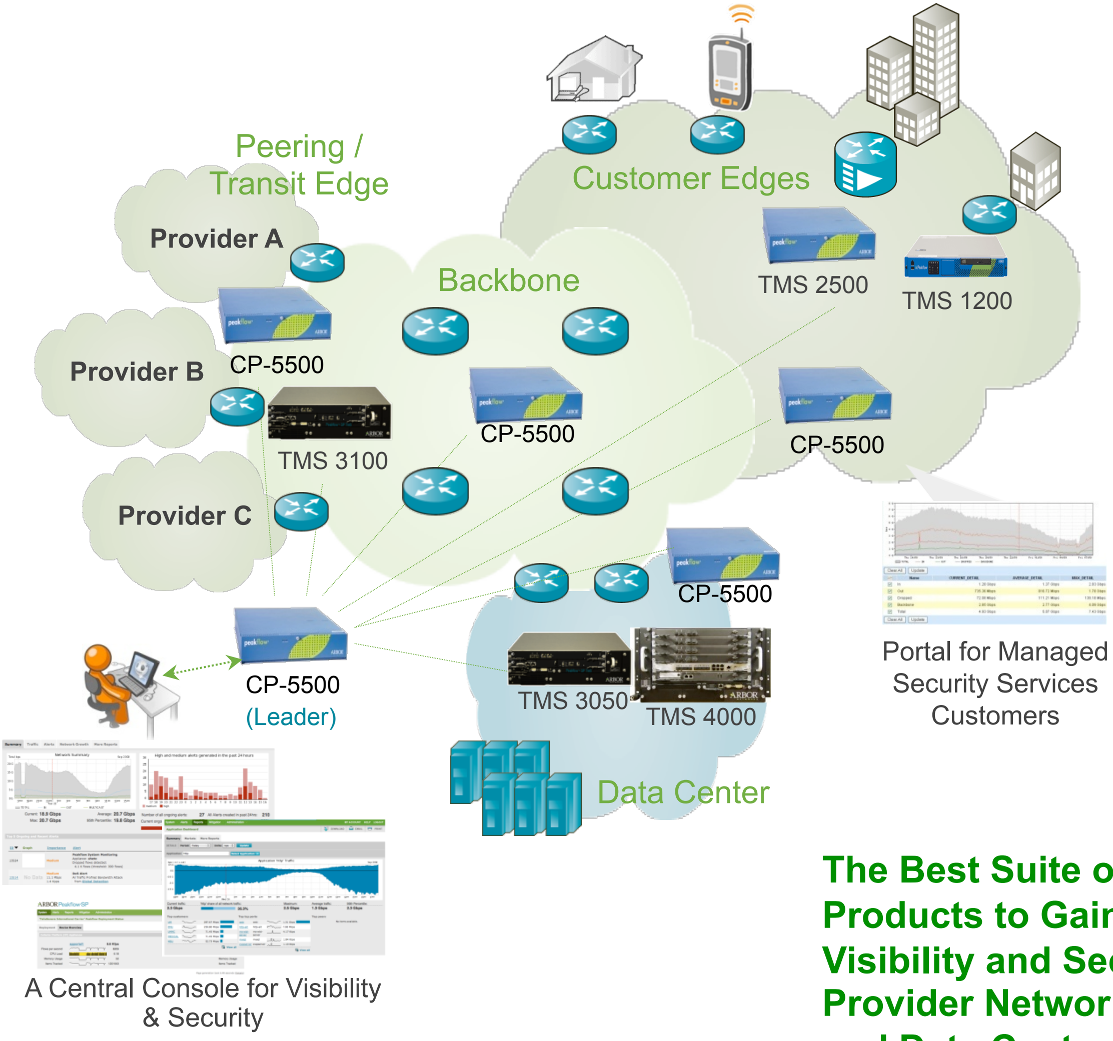
Models: CP-5500

Collector Platform (CP) collects and analyzes IP Flow, BGP, and SNMP data; conducts network anomaly detection; provides user interface; manages other SP devices (i.e. TMS).

Peakflow SP TMS

Models: TMS-1200/2500/ 3000/4000

Threat Management System (TMS) built for carrier-class networks and used for surgical mitigation of attack traffic; conducts service performance monitoring; serves as platform for in-cloud managed security services.



The Best Suite of Products to Gain Visibility and Secure Provider Networks and Data Centers