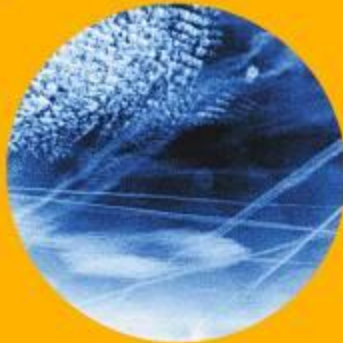
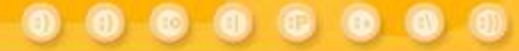


# Network Protection Solution



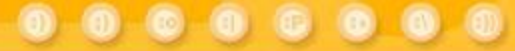
**Toni Ala-Mutka**

[talamutka@allot.com](mailto:talamutka@allot.com)



<b>Solution</b>	<b>Enhances Service Gateway solution with security services:</b> <ul style="list-style-type: none"><li>• Based on Esphion's netDeFlect™</li><li>• Automated DDoS detection and prevention system</li><li>• System to identify/manage infected subscribers (Zombies)</li></ul>
<b>Products</b>	<ul style="list-style-type: none"><li>• New detection probe – “NetDeflector”<ul style="list-style-type: none"><li>• Will also be implemented on Service Gateway blade</li></ul></li><li>• New centralized threat processing server</li></ul>
<b>Synergy</b>	<ul style="list-style-type: none"><li>• NetDeflector provides detection</li><li>• NetEnforcer provides mitigation</li></ul>

# Addressable Market



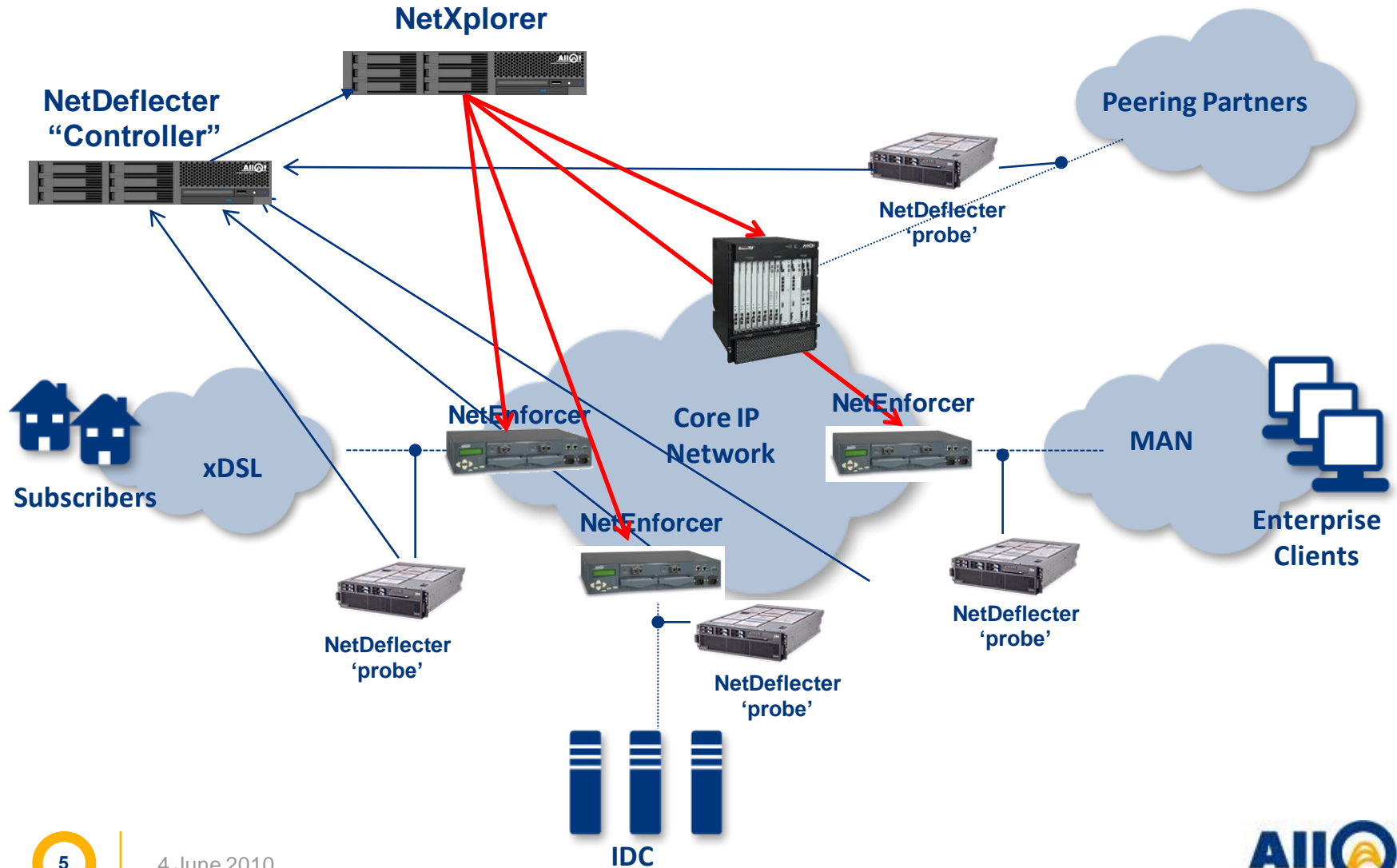
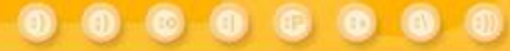
- **Targets service provider market**
  - **Covering security needs**
- **Network protection**
  - **Attacks that risk service availability**
  - **Propagation of worms**
  - **Attacks on subscribers and high value customers**
  - **Mitigation by filtering/limiting bad traffic**
- **Infected subscribers**
  - **Subscriber-generating attacks, SPAM etc.**
  - **Mitigation by filtering/limiting or isolating to captive portal for cleaning**

# Benefits to Customers

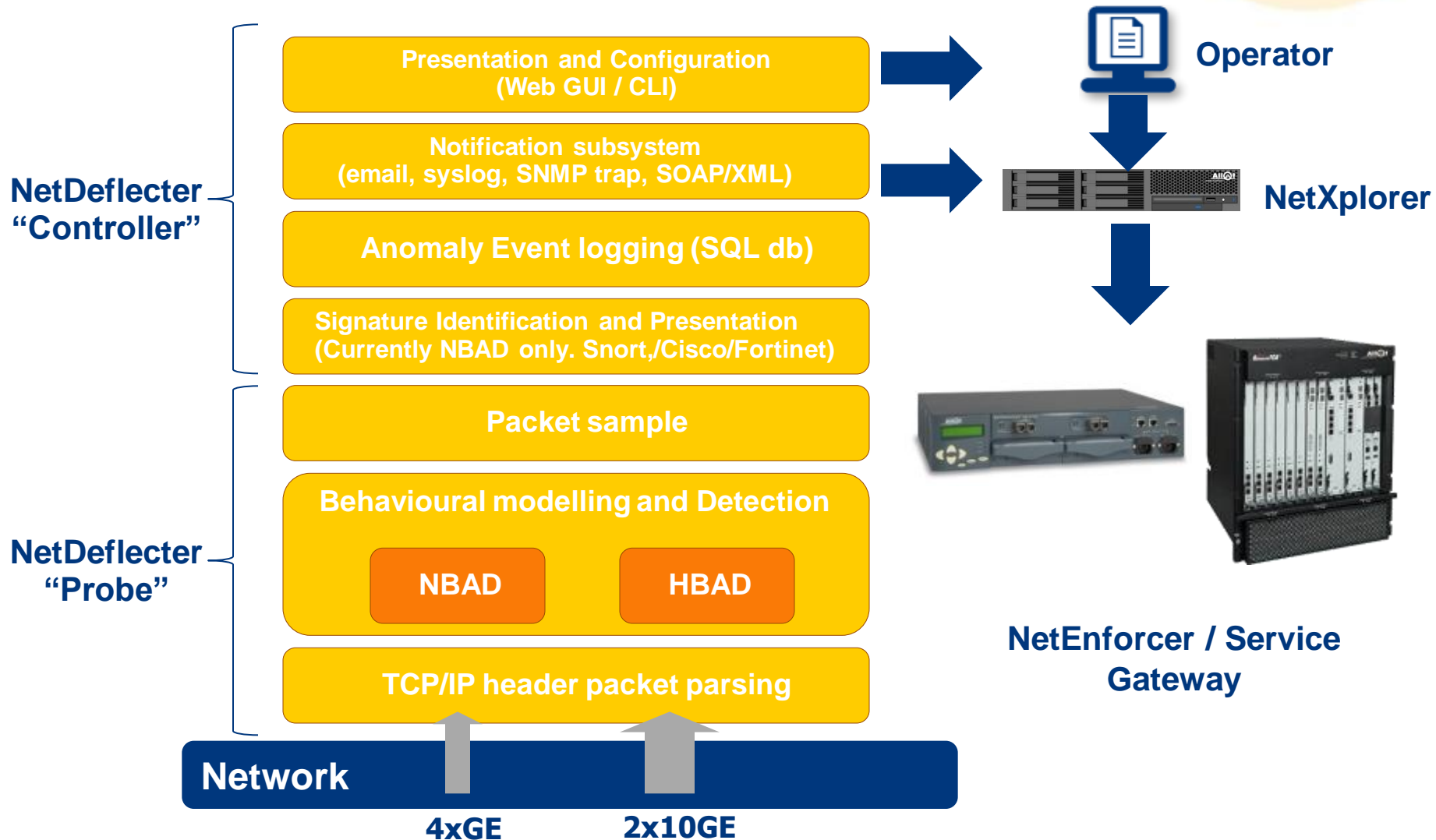


- **Risk Management**
  - Reduce network service disruption/outages
  - Prevent blacklisting and brand damage
- **Opex/Capex Savings**
  - International bandwidth
  - Infrastructure upgrade – MTA, router, peering links
  - Call center complaints
- **Opportunity for Value-Added Services**
  - New revenues from protection services

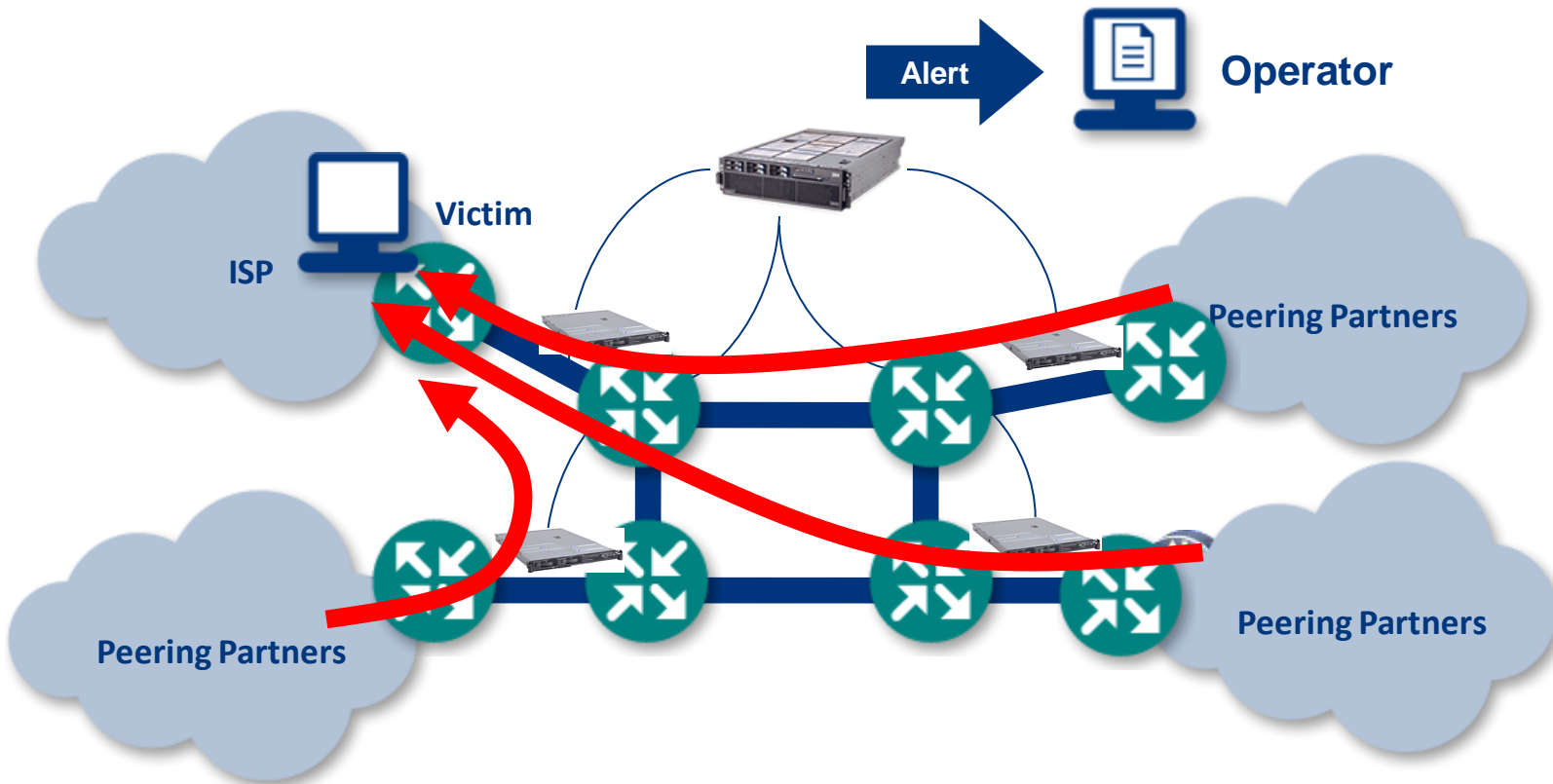
# Deployment and System Components



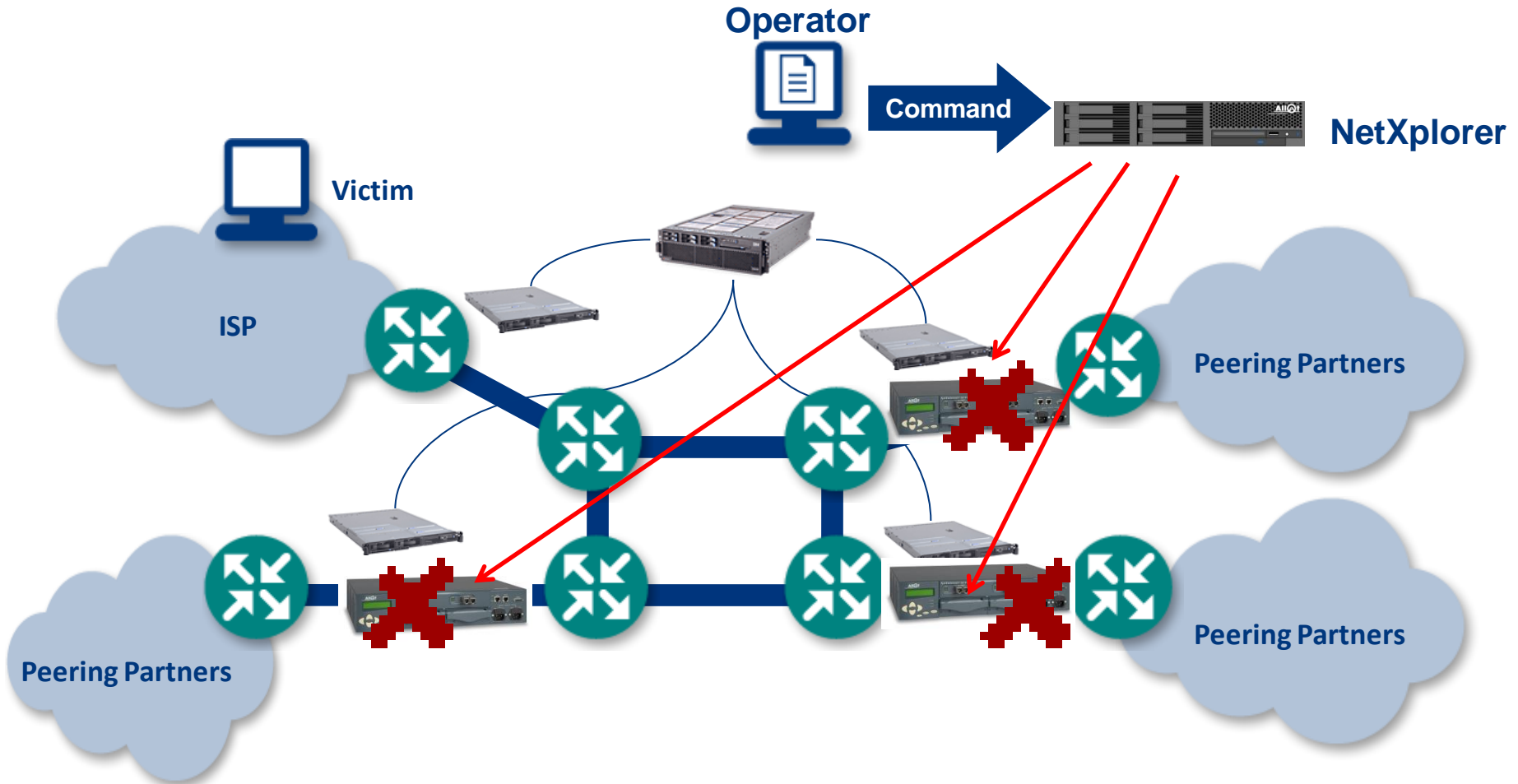
# System Architecture



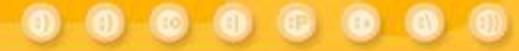
# DDoS Attack Starts



# Issue Command to Block/Rate-Limit



# Case Study: DDoS Network Protection



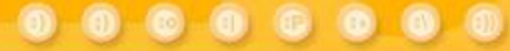
- **Leading Asian ISP >1million BB subscribers**
- **12 x GE probes and 1 x Controller**
  - **Deployed on GE peering links and subscriber links**
  - **Use router ACLs to mitigate DDoS**
- **DDoS attacks affected many customers**
  - **Difficulty identifying and tracking down attacks**
  - **Too many false alarms from IDS**
- **Esphion didn't require 'flow' from routers**
  - **Low false positive rate, high true positive rate**
- **Enabled unprecedented 10 minute (internal) SLA**




# Case Study: Isolating Zombie Subscribers



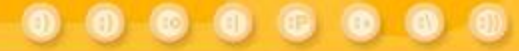
- **Leading Asian ISP > 500K BB subscribers**
- **4 x 10GE probes and 1 x Controller**
  - **Deployed on 10GE aggregation links**
  - **RedBack BRAS to quarantine subscribers**
- **Problems with subscriber zombies**
- **Esphion was the only available 10GE solution**
  - **False alarms from IDS**
  - **Antivirus gateways were unsuitable**

# Customer Success Stories



Customer	Before	After
<p data-bbox="142 348 349 386">Hong Kong</p> 	<p data-bbox="479 351 1263 625">Service outage, degradation and collateral damage to customer network services. Difficulty identifying and isolating DDoS attacks quickly and efficiently</p>	<p data-bbox="1306 351 1808 625">Unprecedented SLAs for mitigating attacks. Pre-emptive blocking, reduced frequency and duration of outages</p>
<p data-bbox="166 701 330 739">Australia</p> 	<p data-bbox="479 701 1224 919">Loss of network services to key hosting clients during DDoS attacks. Previously difficult to identify and isolate DDoS attacks quickly</p>	<p data-bbox="1306 701 1846 862">Saved A\$750K/year in SLA penalties and network engineering costs</p>
<p data-bbox="170 998 324 1036">Thailand</p> 	<p data-bbox="479 1001 1257 1272">SPAM, DOS and other 'zombie' activity leading to loss of services, performance degrade, brand damage, excessive international Internet costs, OPEX costs</p>	<p data-bbox="1306 1001 1889 1153">Automatic identification and management of undesirable subscriber network behavior</p>

# Esphion and DDoS Competition



## Esphion Today

- High performance
- Low network disruption
- High reliability
- Low false positives
- High quality signatures

## Main DDoS Competition



# Competitive Advantage



Espion	Arbor, Cisco, IPSs
<p><b>HIGH PERFORMANCE</b> 10GE in production today. Full line rate 4GE.</p>	<p>Arbor/Cisco – don’ have a DDoS solution for 10GE networks! IPS’s - lack performance required for SP networks.</p>
<p><b>LOW NETWORK DISRUPTION</b> Does NOT require ‘flows’ from routers.</p>	<p>Arbor/Cisco - require ‘flows’ output from routers for detection. “Off and on-ramp cleansing” requires significant implementation. Cisco - is limited for heterogeneous networks.</p>
<p><b>HIGH RELIABILITY</b> Independent of router – no CPU loading. Speed improves with attack magnitude.</p>	<p>Arbor/Cisco – number of flows can increase with attack size. Collector overload, network congestion, router failure. IPS’s – latency and dropped-packets increase during heavy attacks</p>
<p><b>LOW FALSE POSITIVES</b> &lt;5% false alarms &gt;95% rate true positives</p>	<p>Arbor - “too many false positives” and “missed legitimate attacks” Cisco - detection is not traditionally used with Cisco mitigation. IPS’s - suffer from too many false alarms on SP networks</p>
<p><b>HIGH QUALITY SIGNATURES</b> Produced in real-time on n/w. Very accurate.</p>	<p>Arbor/Cisco – filters/fingerprints lack accuracy and will block both good and bad traffic. IPS’s – new signatures takes days and weeks to publish and lack accuracy. Inadequate for new or Zero Day attacks.</p>

## Available Now

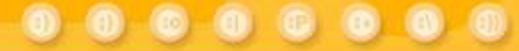
- External probe
- Manual transfer of Esphion rule to NetXplorer/NetEnforcer policy

## Roadmap

- Automated transfer of Esphion rule (under operator control)
- Detection blade inside Service Gateway
- Integration of management systems



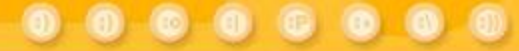
# Target Customers



- **New and current SPs using Allot**
  - **AC-1000, AC-2500 or SG-Omega customers**
  - **Tier 1 and Tier 2**
  - **SPs with more than 100,000 subscribers or with significant number of business customers**
- **SPs looking for ...**
  - **DPI and DDoS capabilities**
  - **Pure DDoS solution (detect and mitigate)**
  - **Subscriber SPAM, subscriber zombies**
  - **DNS attacks**
- **SPs offering managed services**
  - **Online gaming, banks/finance, content portals, government**
- **SPs with internal/external SLA problems due to DDoS**

- **Identify telco/ISP needs**
  - **Experiencing/recent PAIN?**
  - **Planning new products or services?**
  - **PROBLEMS driving upgrade/expansion?**
- **Presentation focus points**
- **Proof of concept**
  - **1-2 month high-touch fine-tuned exercise**
  - **‘Simulate’ attacks if they don’t occur naturally**
- **Objections/competitors**

# Identify Needs



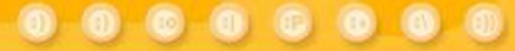
- **Experiencing/recent PAIN?**
  - **Widespread high profile outages**
  - **High profile victims**
- **Planning new PRODUCTS or services?**
  - **DDoS protection services**
  - **Tiered subscriber services**
- **PROBLEMS driving upgrade/expansion?**
  - **International bandwidth costs**
  - **Call center Opex**
  - **Capex**

# Presentation Points



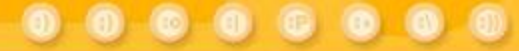
- **Focus on needs**
- **Namely ...**
  - **Reduce Opex**
  - **Manage/delay Capex**
  - **Manage risk**
  - **Increase revenue from value added services**
- **Refer to “Benefits” slide**

# Proof of Concept (POC)



- **Identify ideal POC location**
- **Installation and tuning: 1-2 days**
- **Product test/familiarization time: 1-2 months**
  - **Assurances of stability**
  - **See real-life attacks**
  - **Simulate attacks if not naturally occurring**
  - **Demonstrate mitigation with NetEnforcer**
- **Fine-tune for low alarm rate and high reliability**
- **High contact with stakeholders**

# Typical Objections



- **Company stability/longevity**
- **Technology credibility – speed, accuracy, 10GE**
- **Scalability**
- **Integrated solution for detection and mitigation**
- **After-sales in-country support**
- **GUI user friendliness**
- **We already use “X”**
- **We are a Cisco shop**

# Questions and Answers



# BACKUP SLIDES





# Email Alert Is Sent



**Flood x1.demo3:group7:syn-in (126639) - Message (Plain Text)**

File Edit View Insert Format PGP Tools Actions Help Type a question for help

This message has extra line breaks. To remove, click here.

From: demo3@esphion.com Sent: Fri 9/09/2005 10:37 a.m.  
To:  
Cc:  
Subject: Flood x1.demo3:group7:syn-in (126639)

[https://demo3.esphion.com/evp/controller?nextaction=flood\\_report&hs=true&tooltip=Flood%20Report&floodID=126639](https://demo3.esphion.com/evp/controller?nextaction=flood_report&hs=true&tooltip=Flood%20Report&floodID=126639)

Status: ACTIVE ← Detected and diagnosed within 7 secs  
Duration: 00:00:07  
Rank: 4  
IP ratio: 8:1 (SRC:DST in the latest pattern)

Deviation traffic (estimated):  
percent: 171.22 % packets  
171.22 % bits  
count: 44.15 Kpackets  
rate: 4.33577 MiB  
6.30714 Kpps ← Network impacting!  
5.19586 Mbps

Observed traffic:  
count: 69.936 Kpackets  
6.86809 MiB  
rate: 9.99086 Kpps  
8.23053 Mbps

Last update: Fri Sep 09 10:36:42 NZST 2005  
Started: Fri Sep 09 10:36:35 NZST 2005  
Stopped:  
Stop details:

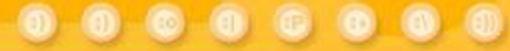
Agent: x1.demo3 ← Detected at this location  
Group: group7 (group7)  
Type: syn-in (incoming TCP SYN flood)  
ID: 126639

Reported by: `detect` at x1.demo3  
Matched filter: grade4k-ddos (importance 10)

Floods meeting this filter condition are important!

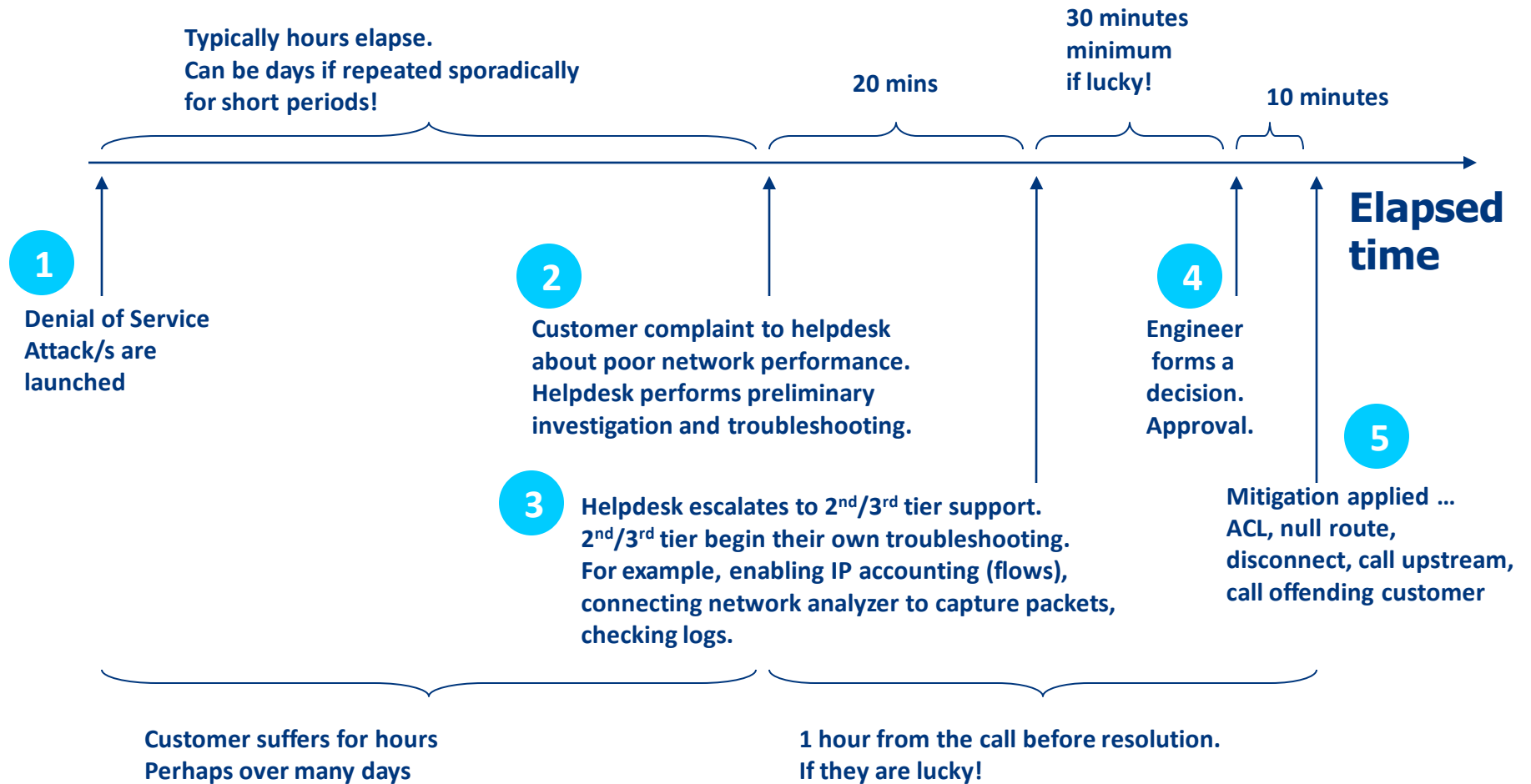
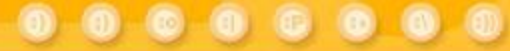


# About Esphion

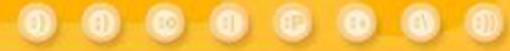


- **Pronounced [es-fee-un]**
- **Launched 2002, VC funded, R&D HQ in Auckland, New Zealand**
- **Primarily focused on APAC**
- **Customers in Australia, NZ, China, Hong Kong, Thailand, JV in Japan**
- **Mainly focus on large, mature, mission-critical Internet businesses and IP networks – Telcos, ISPs, IDCs, ICPs - also enterprise success stories!**

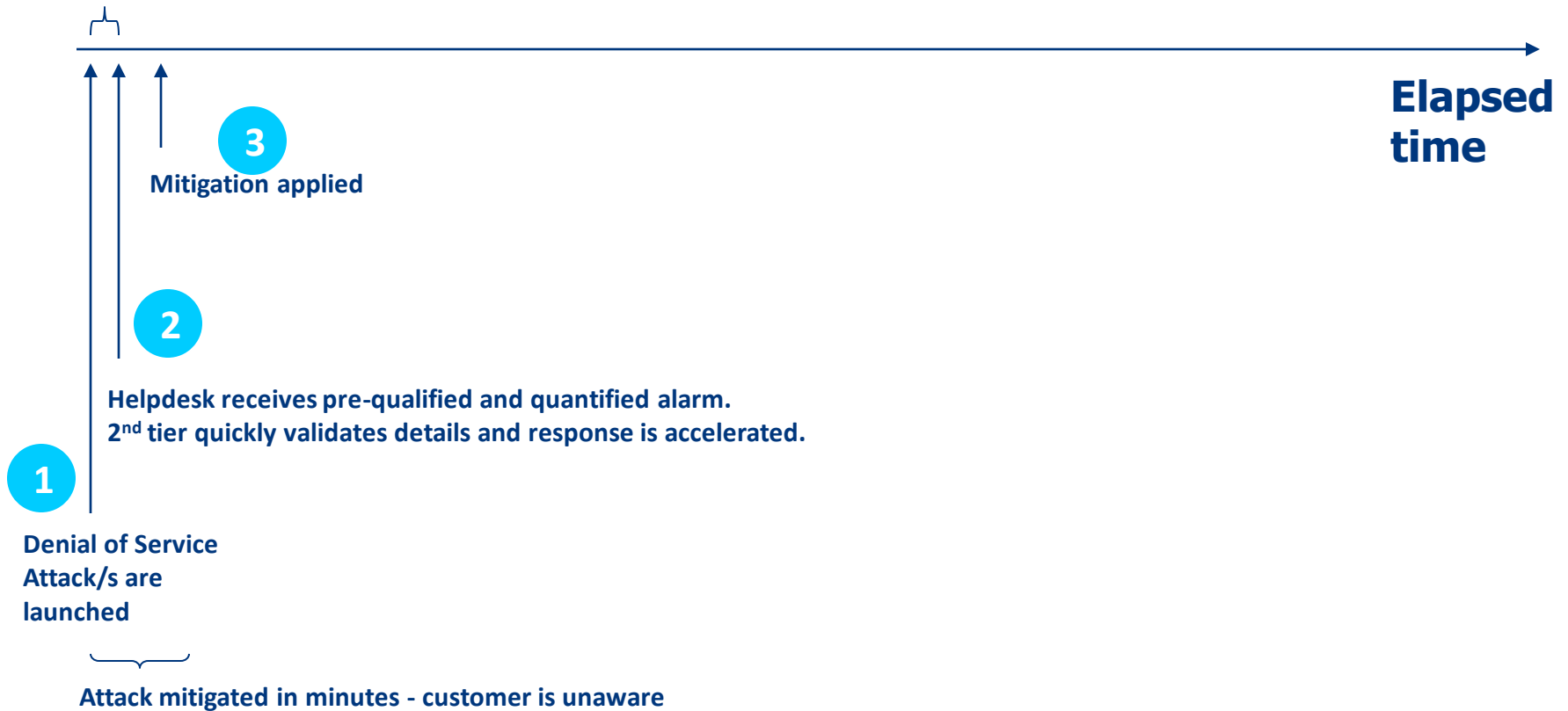
# Typical DDoS Resolution Process



# Process Enabled by Esphion



Detect and alert within 1 minute

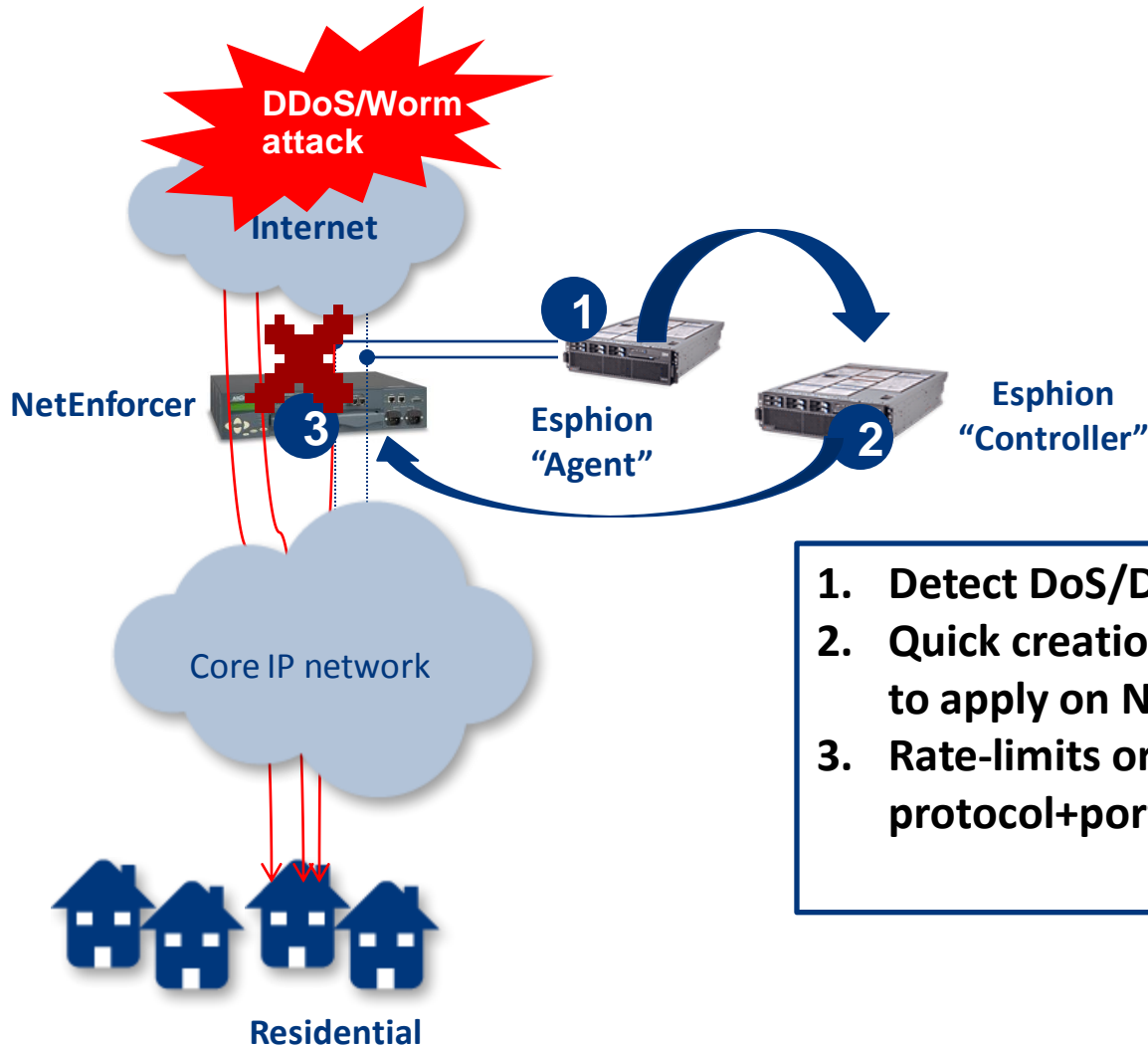
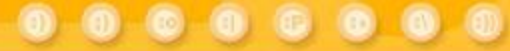


# Problems with Current Solutions



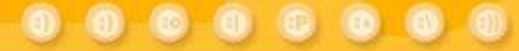
- **Manual approaches (Sniffer, flow /log analysis) are reactive and too SLOW and INCONSISTENT to meet internal/external SLAs**
- **Flow-based detection is UNRELIABLE during attacks due to router deprioritization of flow generation, flow congestion on network and overload of flow collector**
- **IDS/IPS packet signature detection approaches often fail to detect ad hoc attacks such as DDoS and Zero Day worms**
- **Stateful/application level systems are not intended for network level flooding attacks – introducing potential choke point or point of failure**

# DDoS Protection with NetDeflector + NetEnforcer

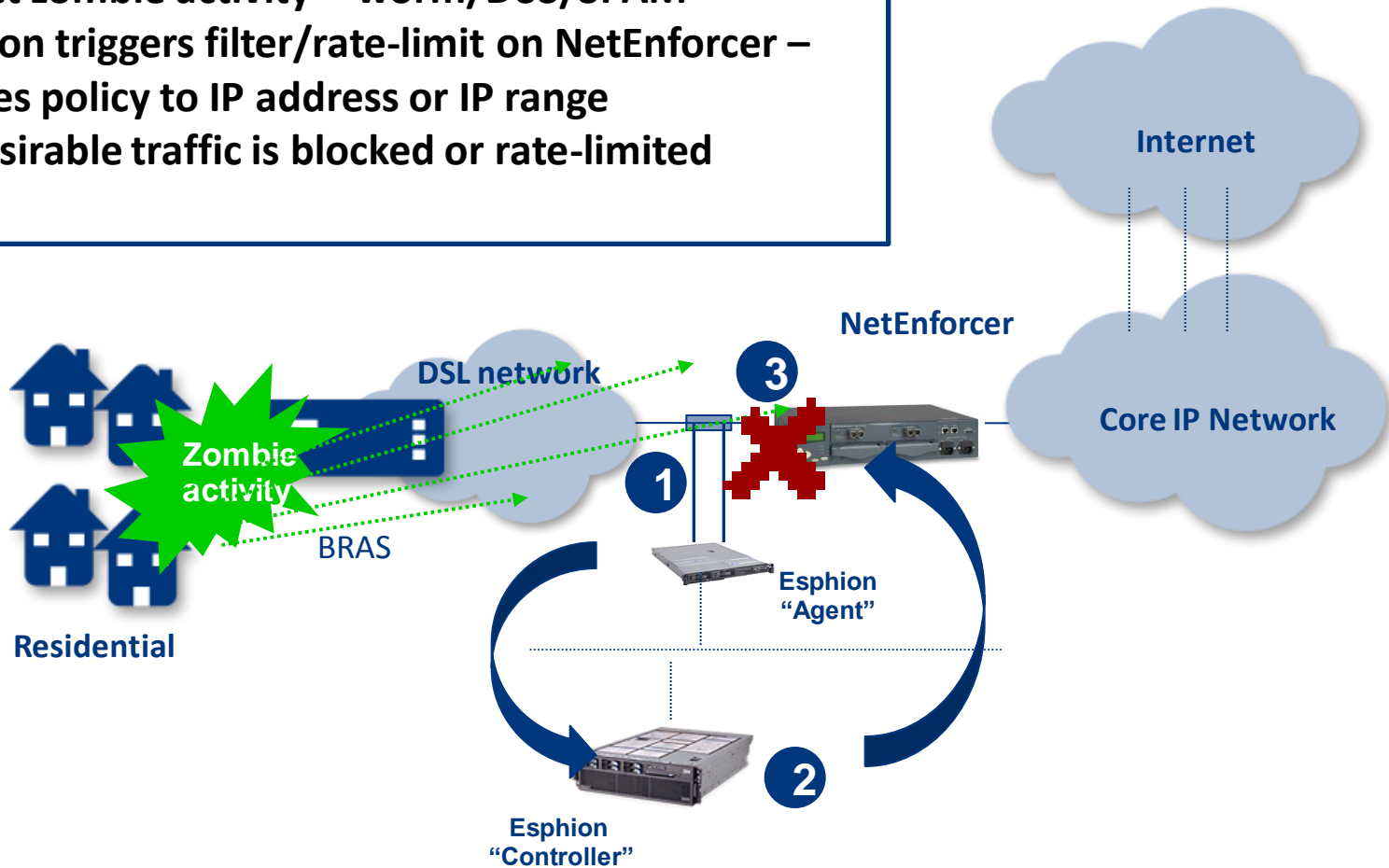


1. Detect DoS/DDoS/Zero Day worm
2. Quick creation of detailed packet filter to apply on NetEnforcer
3. Rate-limits or blocks IP and/or protocol+port to limit/block impact

# Isolate Subscriber Zombies



1. Detect zombie activity - worm/DoS/SPAM
2. Espion triggers filter/rate-limit on NetEnforcer – applies policy to IP address or IP range
3. Undesirable traffic is blocked or rate-limited



# Data Sheet



Component / Feature	Description	Comment
Hardware dimensions	1U / 2U 19" rack mount IBM / HP server	Controller 2U, Agent 1U or 2U
Management interface	10/100/1000T	Dedicated management interface for Controller and Agent
Monitoring interface (Agent only) Version 3.2.*	x4 10/100/1000T	Fixed port, electrical RJ45
	x4 GE	Interchangeable interface via SFP transceivers (T, SX, LX)
	x2 10GE	Interchangeable interface via XFP transceivers (SR, LR)
Add network latency	No	Passive network deployment
Network or router loading	No	Minimal management traffic, no router loading
Agents per Controller	16	-
Groups	400 Agent-Groups per Controller 30 Groups per Agent	-
Third tier Controller	N/A	On Esphion roadmap
Filter recommendations	Yes	Snort, Cisco ACL, Cisco PIX, Fortinet. Others on request.
Alerting/Notification	Yes	Email, SNMP trap, syslog, SOAP/XML, custom
Configurable notifications	Yes	User configurable parameters to filter notifications
Reporting	Yes	Scheduled daily, weekly or monthly. Email PDF.
Signature database	No	Not required - uses network behavior anomaly detection
Netflow / cflow / sflow	No	Not required - create own meta-data from every packet
Real-time signatures	Yes	Includes TCP/IP, Payload and Ethernet layer information

# Performance Specifications



System Capability	Performance	Comment
Reliability detecting network anomalies	Excellent	Detects imbalances in the network behavior - defined mainly by Espion ratios
Detection speed	Typically 5-30 seconds	Smaller anomalies take longer to decide. Large anomalies improve speed of detection
Speed of signature extraction	Typically 10-20 seconds	
TCP/IP signature	Yes	Any TCP/IP header information can contribute to signature creation
Payload signature	Yes (if available)	Any field in the payload can contribute to payload signature creation
Frame layer signature	Yes	Includes SRC and DST MAC address, VLAN tag

Agent Interface Options	Performance	Comment
X4 10/100/1000T	4Gbps full line rate	Internet packet size mix
X4 GE (x2 dual GE NICs)	4Gbps full line rate (any packet size) Max.1.488Mpps per interface	Internet packet size mix Min 60 Byte frame size
X2 10GE (x2 10GE NICs)	10Gbps 1.99Mpps per interface	Internet packet size mix Min 60 Byte frame size