Service Provider Solutions

DDoS Protection Solution Enabling “Clean Pipes” Capabilities

June 2005

Service Provider Security Highlights

- **Security is the heart of internetworking's future—A secure infrastructure forms the foundation for service delivery**
- **We have moved from an Internet of implicit trust to an Internet of pervasive distrust**
- **The Miscreant Economy is here to stay and has created a damaging business opportunity of criminal intent**
- **All the other functionality of the router merges into a pervasive policy enforcement model**

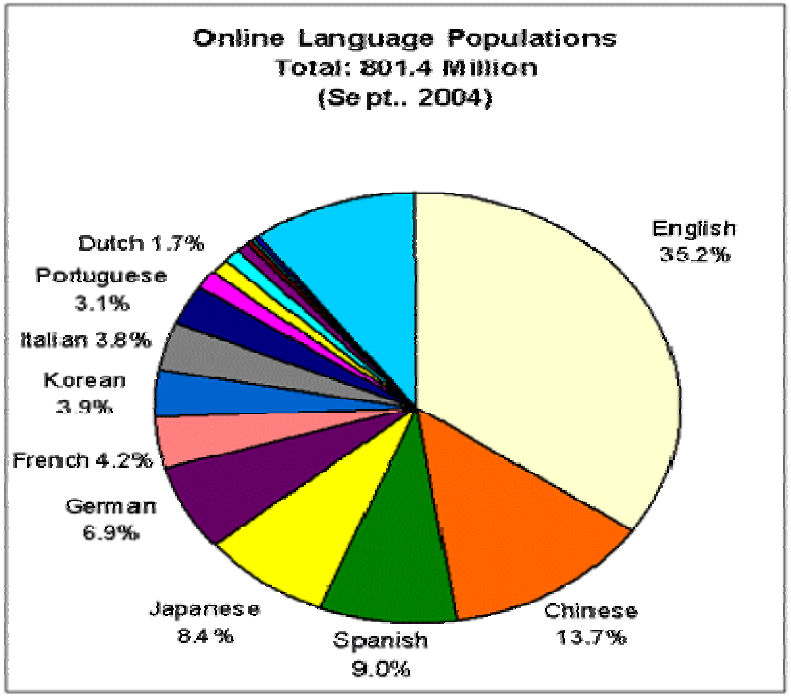
  QoS = Security

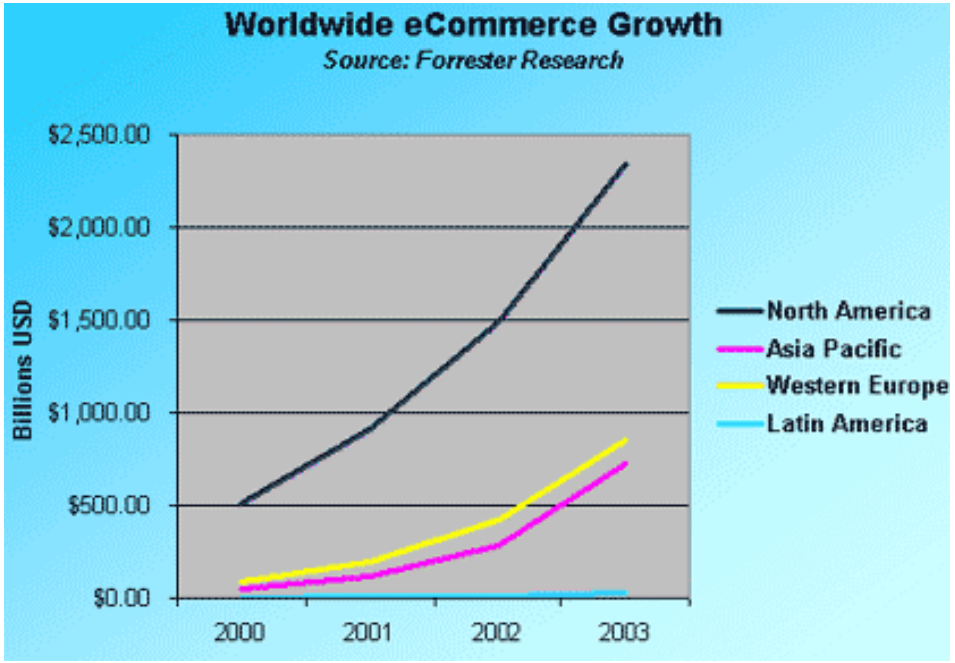
  HA = Security

  Edge Policy = Security

- **We must improve reaction times, reduce windows of vulnerability, and ensure service delivery across the network**

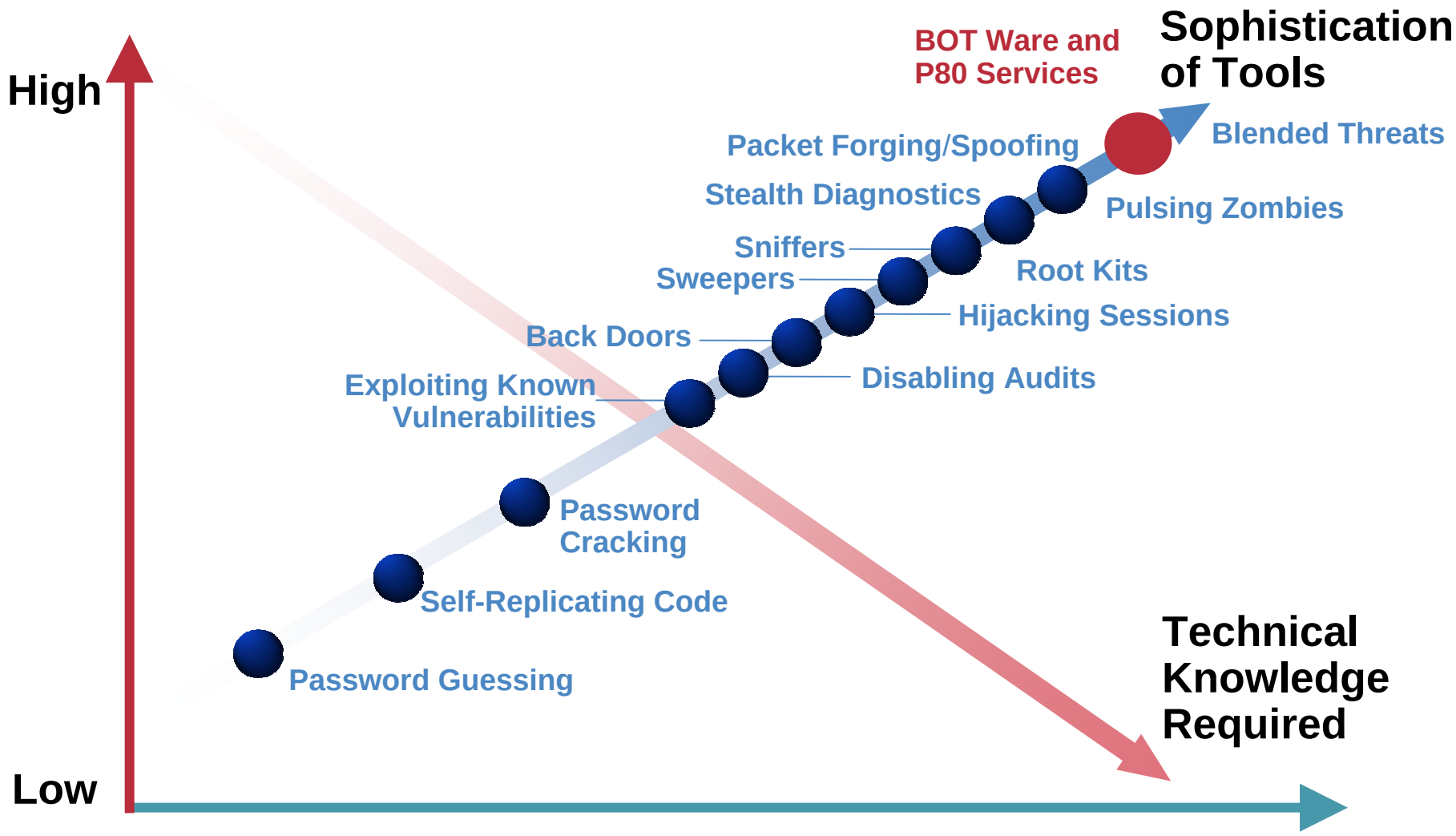
Macro Trends Fueling DDoS Attacks



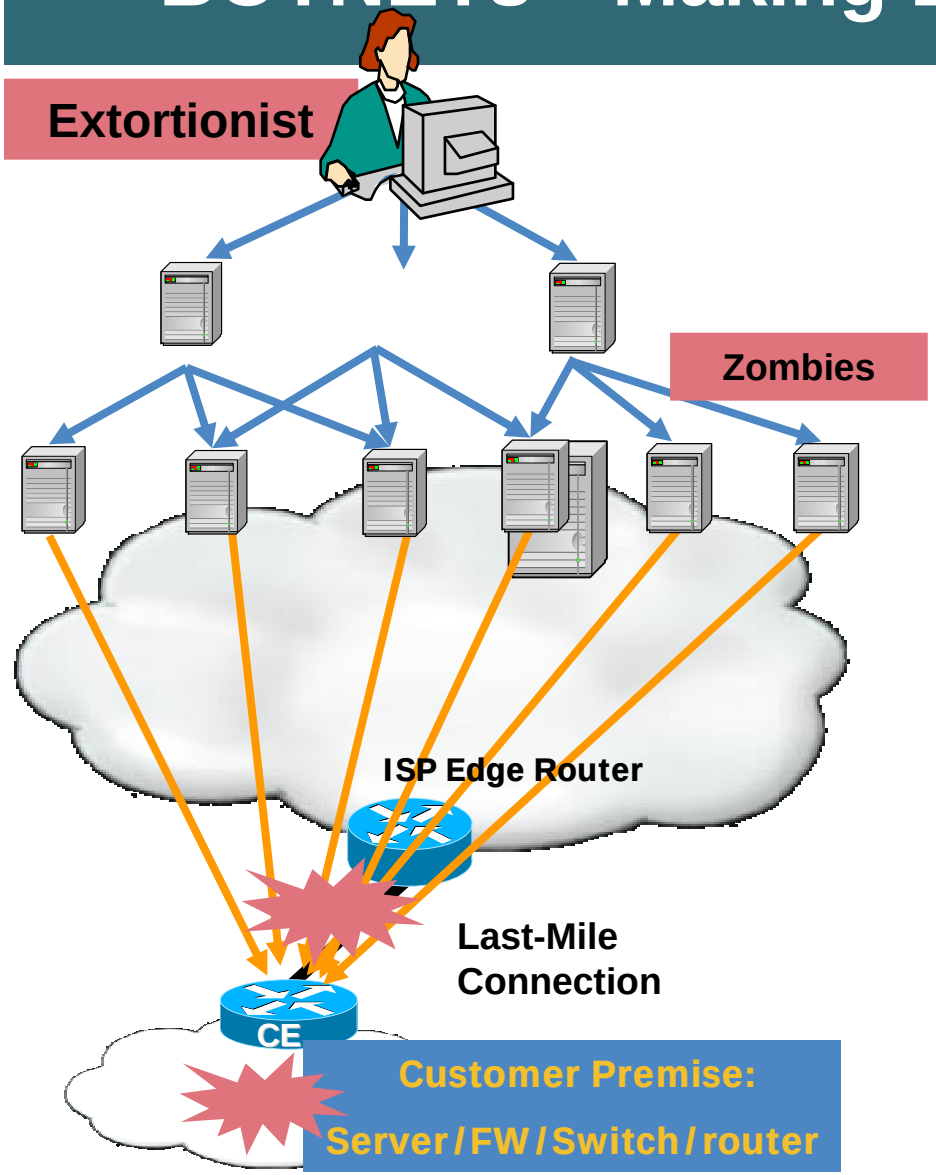


- **World Internet usage between 2000–2005 has grown 146.2% to 800+ million**
- **Broadband explosion has resulted in an increasing number of poorly secured home PCs with always-on Internet connections just waiting to be discovered and taken over by miscreants**
- **eCommerce growth has made dependence on Internet more critical than ever**
- **Globalization due to the dot com explosion, outsourcing, and peer-to-peer applications has increased international traffic exchange significantly**
- **Most attacks launched from multinational origins—very hard to isolate and take action on the extortionists**

Evolution of Threats and Exploits



BOTNETs—Making DDoS Attacks Easy



2-for-1 Special

- **BOTNETs for Rent**
- **A BOTNET is comprised of computers that have been broken into and planted with programs (zombies) that can be directed to launch attacks from a central controller computer**
- **BOTNETs allow for all the types of DDOS attacks: ICMP attacks, TCP attacks, UDP attacks, and http overload**
- **Options for deploying BOTNETs are extensive and new tools are created to exploit the latest system vulnerabilities**
- **A relatively small BOTNET with only 1000 zombies can cause a great deal of damage**
- **For example: 1000 home PCs with an average upstream bandwidth of 128 kBps can offer more than 100 MBps**
- **Size of attacks are ever increasing**

Elements Impacted by DDoS

- **Applications**

  Attacks will exploit the usage of TCP/HTTP to overwhelm the computational resources

- **Host/servers**

  Attacks will attempt to overload the resources using protocol attacks—Critical servers will not respond to normal request

- **Bandwidth**

  Attacks will saturate the bandwidth on IP data connections that limit or block legitimate traffic flows

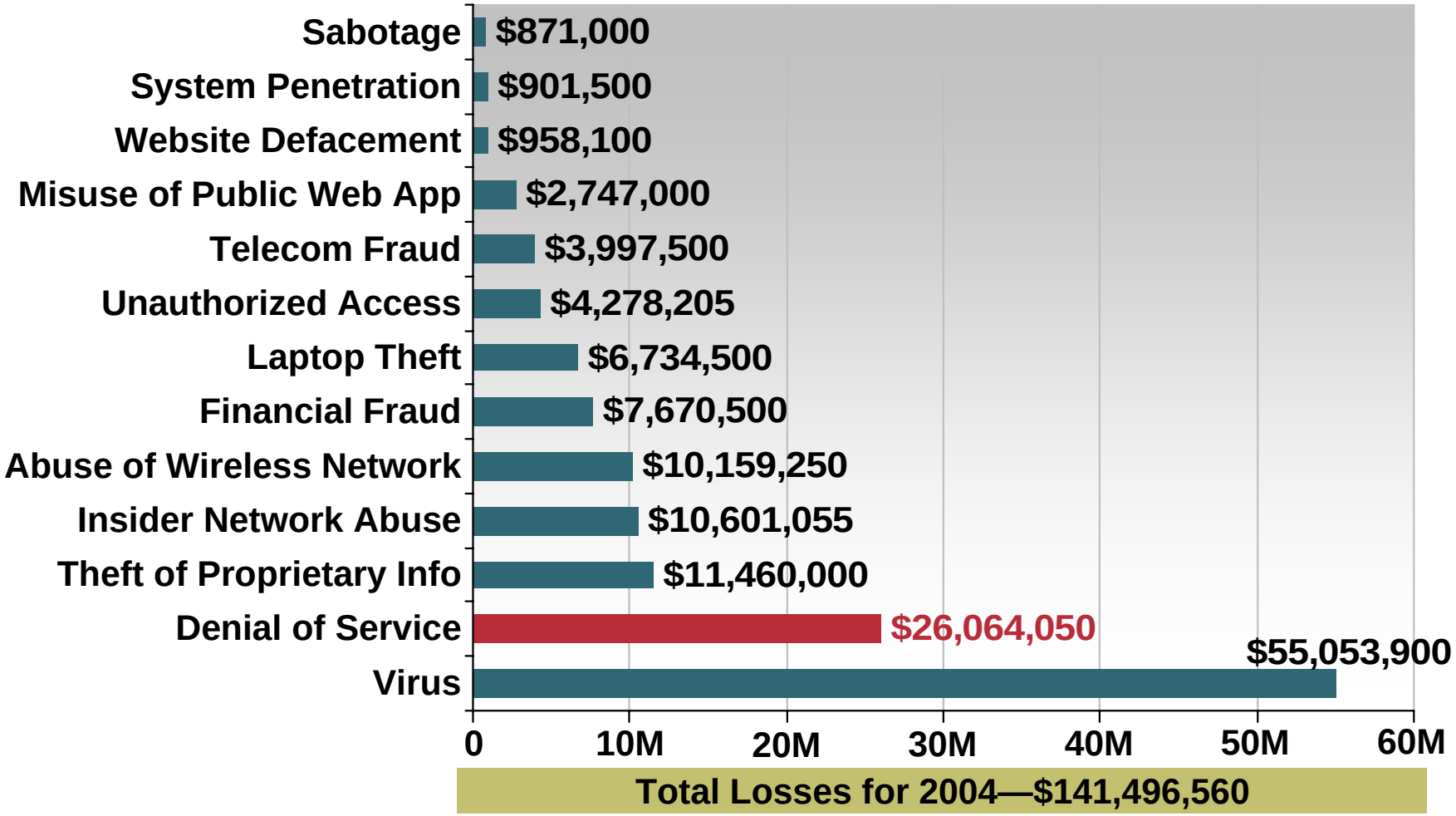
- **Infrastructure**

  Attack target critical assets of network including routers, DNS/DHCP servers, and others devices that deliver network connections

- **Collateral damage**

  Attacks that impact devices not originally targeted such as computation overload by devices that carry the DDoS attack

Impacts Caused by Denial of Service



CSI/FBI 2004 Computer Crime and Security Survey
Source: Computer Security Institute

2004: 269 Respondents

Quotes from the Industry

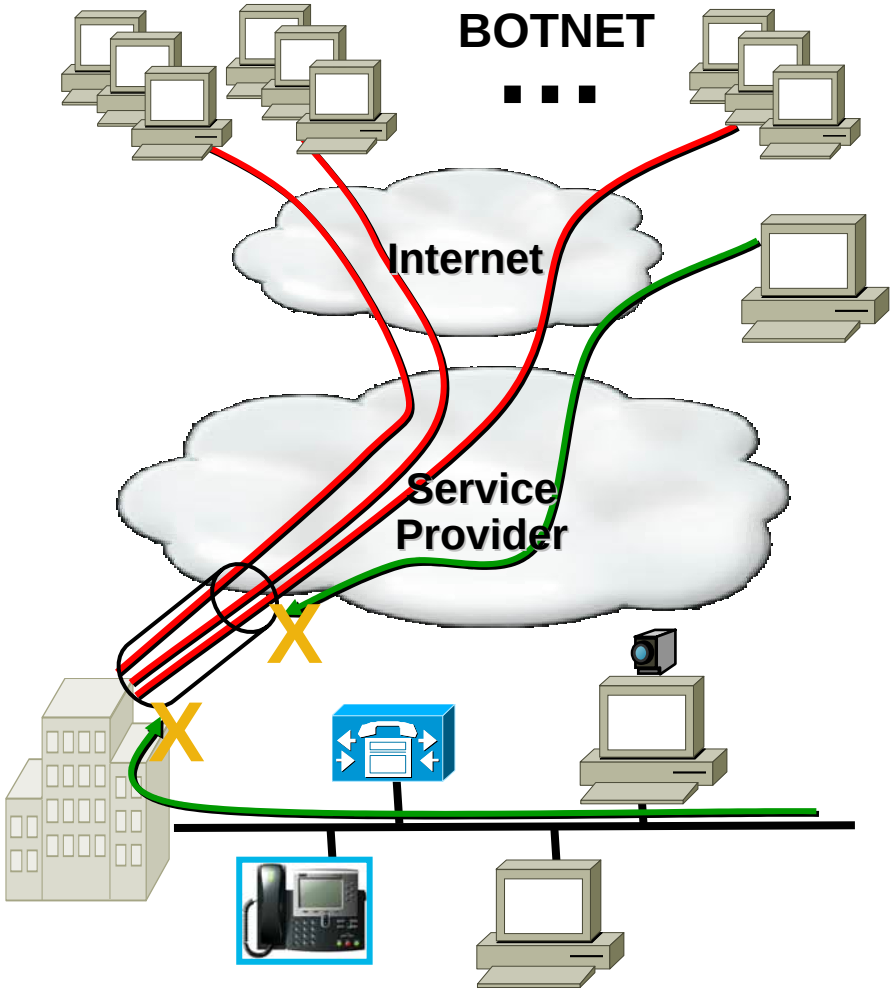
Extortion is "becoming more commonplace," says Ed Amoroso, chief information security officer at AT&T. "It's happening enough that it doesn't even raise an eyebrow anymore."

"We've had [extortion attempts] happen to our customers," says Bruce Schneier, CTO at managed security services provider Counterpane Internet Security. "More often than I'd like, they're paying up."

"Antidistributed DoS services cost around $12K per month from carriers such as AT&T and MCI," says John Pescatore, Gartner security analyst. "The most popular type of antidistributed DoS equipment used by SPs is Cisco® Riverhead gear and Arbor Networks' detection tools. This equipment can filter about 99% of the attack traffic."

The Risk to Your Business

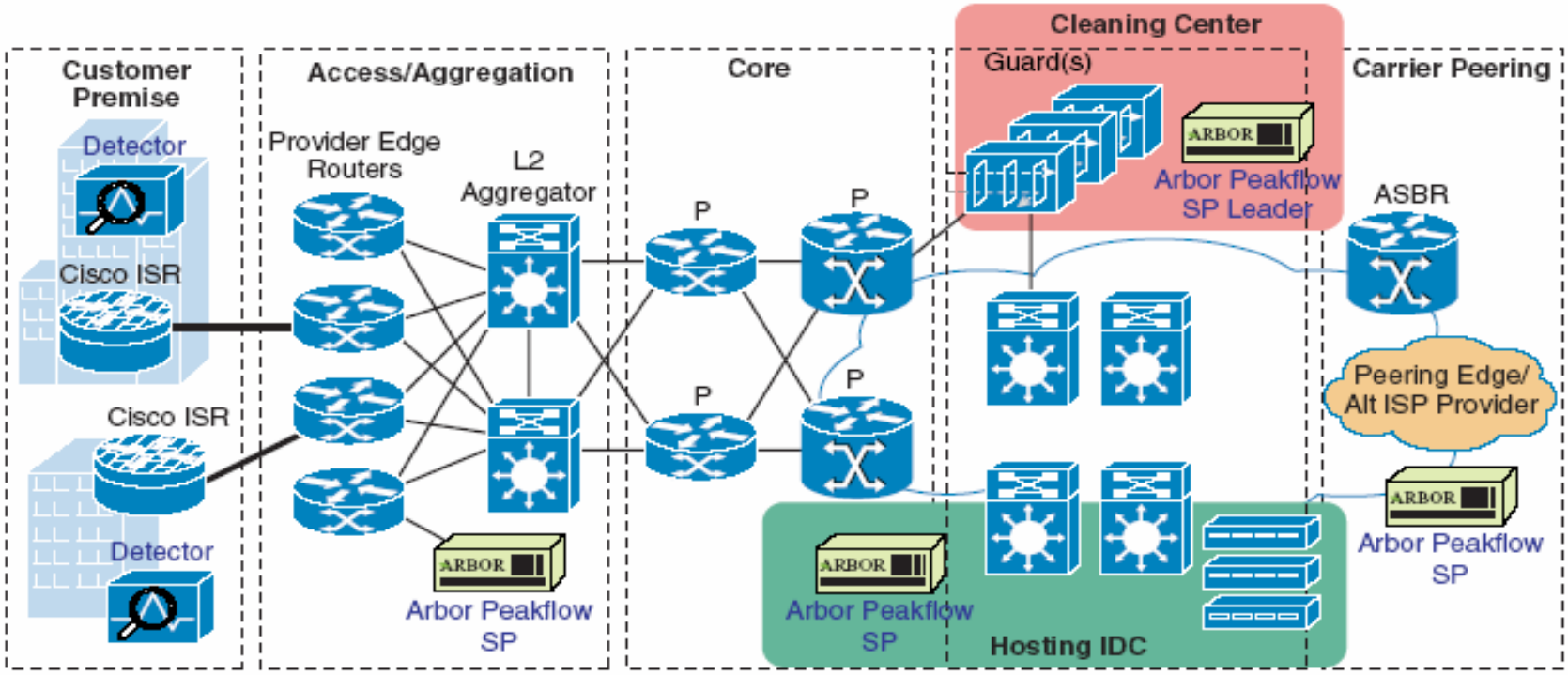
- **At risk:**
  - **The network is at risk to extortion**
  - **Maintaining business availability**
  - **Preserving reputation and customer retention**
  - **Regulatory obligations—SOX, GLBA, …**
  - **Legal and service-level liabilities**
- **What can you do**
  - **Take a proactive stance**
  - **Plan and prepare for the worst case**
  - **Apply appropriate security tools ➔ DDoS prevention solution**



What are Clean Pipes Capabilities?

- **A solution set to protect against security threats on the data pipe that are critical to deliver connectivity and services**
- **The data pipe choke point could be:**
  - **Enterprise/SMB/Consumer—Last-mile data connection**
  - **Federal—Data connections accessing critical information**
  - **Service Provider—All data connections (i.e., Peering Points, Peering Edges, Data Center…)**
- **Most damaging types of threats that reside on the data pipe:**
  - **Distributed Denial of Service (DDoS)**
  - **Worms**
  - **Viruses**
- **Goal is to remove the malicious traffic from the data pipe and only deliver the legitimate traffic before the link is compromised**
- **Service providers can protect themselves from attacks and can deliver security services for protection**

DDoS Protection Solution Overview



Network Management	Detection	Diversion/Injection	Mitigation
	Identify and classify attacks based on anomaly characteristics.	Divert "dirty" traffic to the cleaning center to be "scrubbed", inject clean traffic back to the DDoS targeted host	Anti-spoofing, anomaly recognition and packet inspection and cleaning (scrubbing) of "dirty" traffic
	Network Foundation Protection		

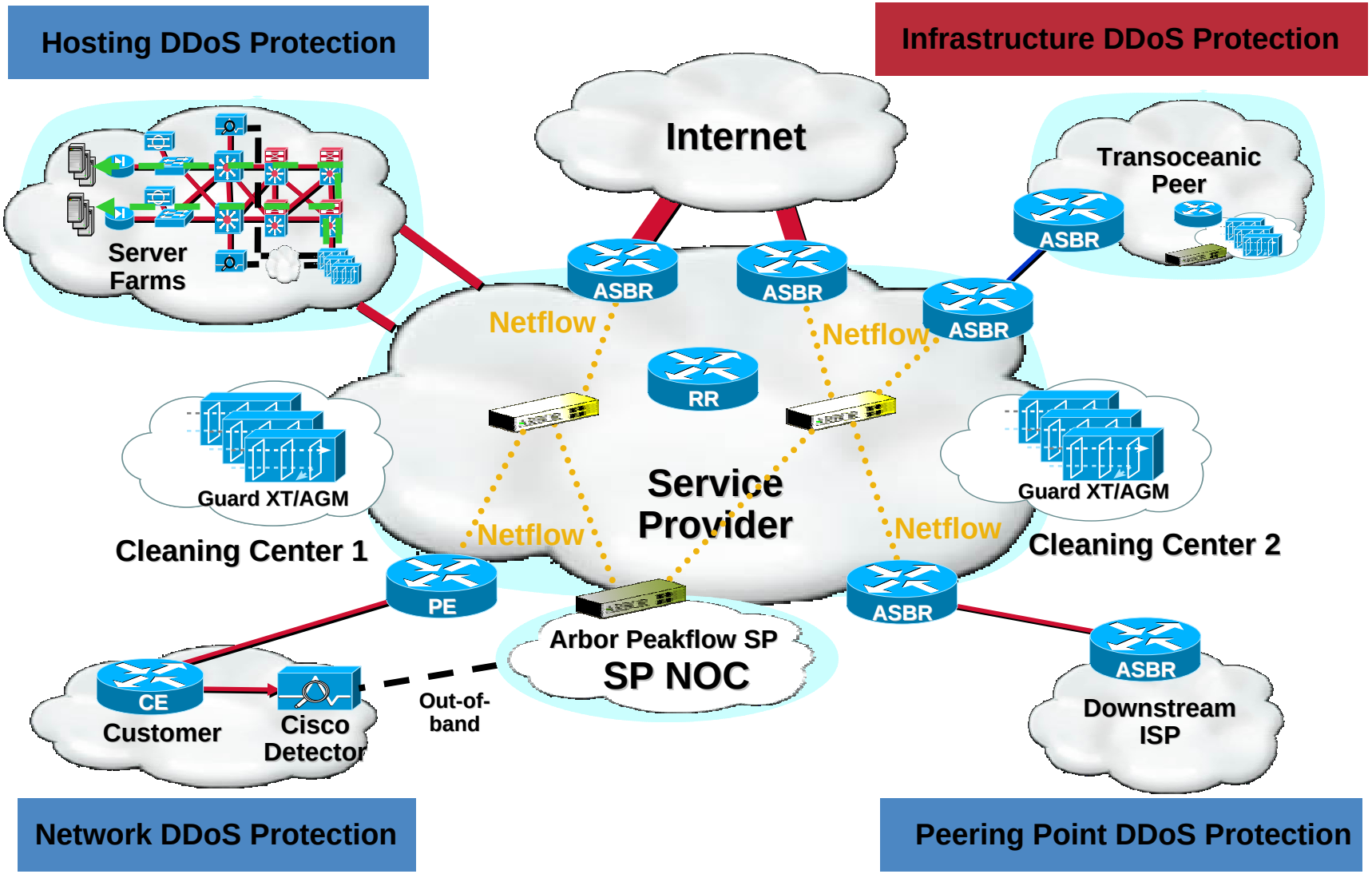
DDoS Protection Models

DDoS Protection Model	Core Function(s)	Key Capabilities
Managed Network DDoS Protection	Last-mile bandwidth protection for the service provider customers	• New SP revenue model • Primary function to enhance business continuance for customers • Protection of critical last-mile bandwidth • Ensure the continual delivery of enhanced services offered over data connections
Managed Hosting DDoS Protection	Protection of data center assets hosted by the provider	• New SP revenue model • Ensure uptime of critical assets hosted by the service provider • Differentiation of the hosting service
Managed Peering Point DDoS Protection	Provide DDoS-free wholesale connections for downstream ISPs	• New SP revenue model • Provide clean wholesale connections • Better promote a DDoS-free environment
DDoS Infrastructure Protection	Protection model for the service provider to defend their networks and protect service delivery	• Protect critical assets in the data center • Mitigate attacks on critical routing infrastructure (Peering Points, Provider Edges and Core routers) • Reduce OPEX by reduction of unwanted traffic across expensive transoceanic links • Reduce collateral damage impacts

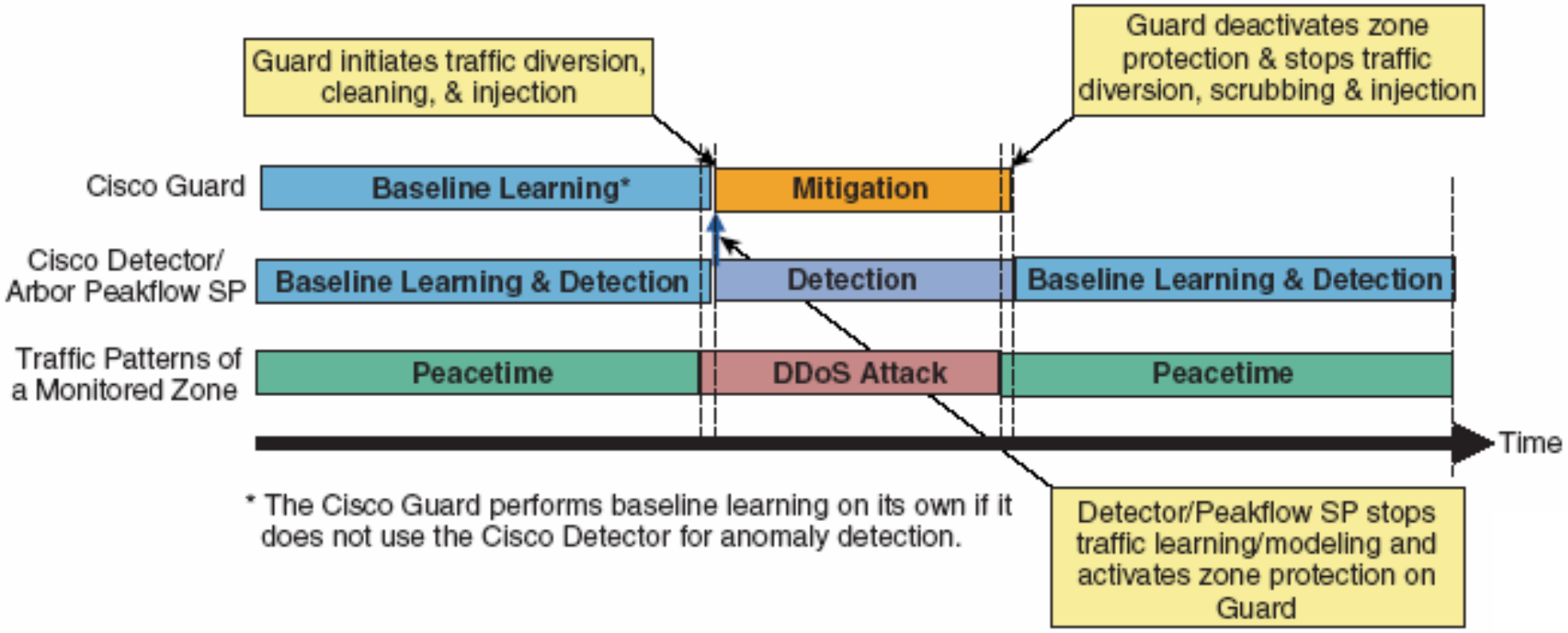
DDoS Protection Solution Architecture

Managed Service

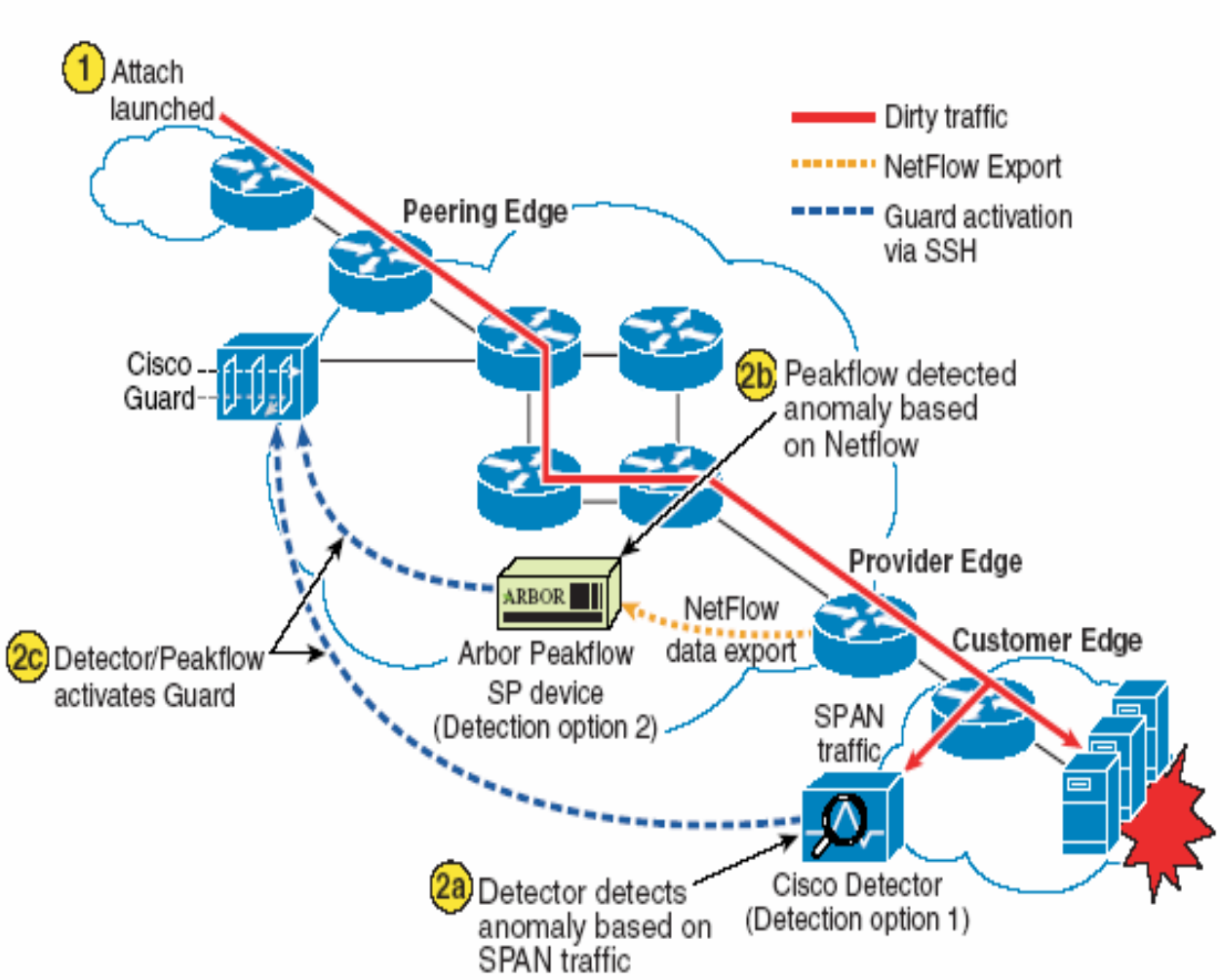
Infrastructure Security



Lifecycle of DDoS Protection



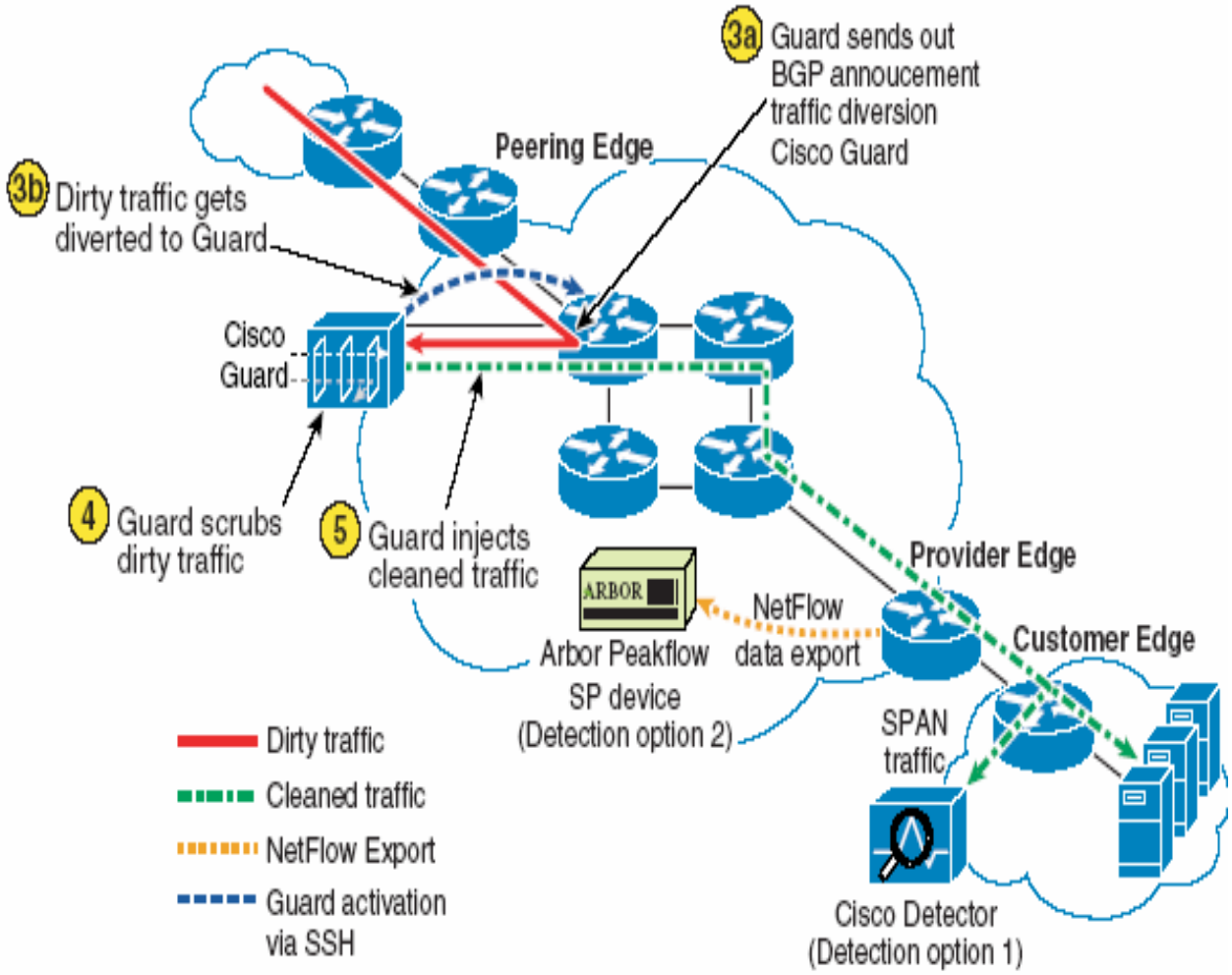
Detection Process



Steps

1. **Attacks are launched by extortionist via BOTNETS.**
2. **Cisco® Detector on the customer premise can precisely detect when the customer is under attack.**
3. **Netflow statistics from Cisco routers are exported to Arbor Peakflow SP for correlation. Anomalies are inspected for unexpected traffic behavior.**
4. **The Detector or Arbor Peakflow SP indicates to the Guard that an attack has commenced.**

Diversion and Mitigation Process



Steps

3a. A BGP announcement is the mechanism used to divert traffic to the Cisco® Guard.

3b. All traffic (malicious and legitimate) to the attacked destination is redirected to the Guard.

4. The Cisco Guard drops the DDoS anomalies and allows only the legitimate traffic to continue.

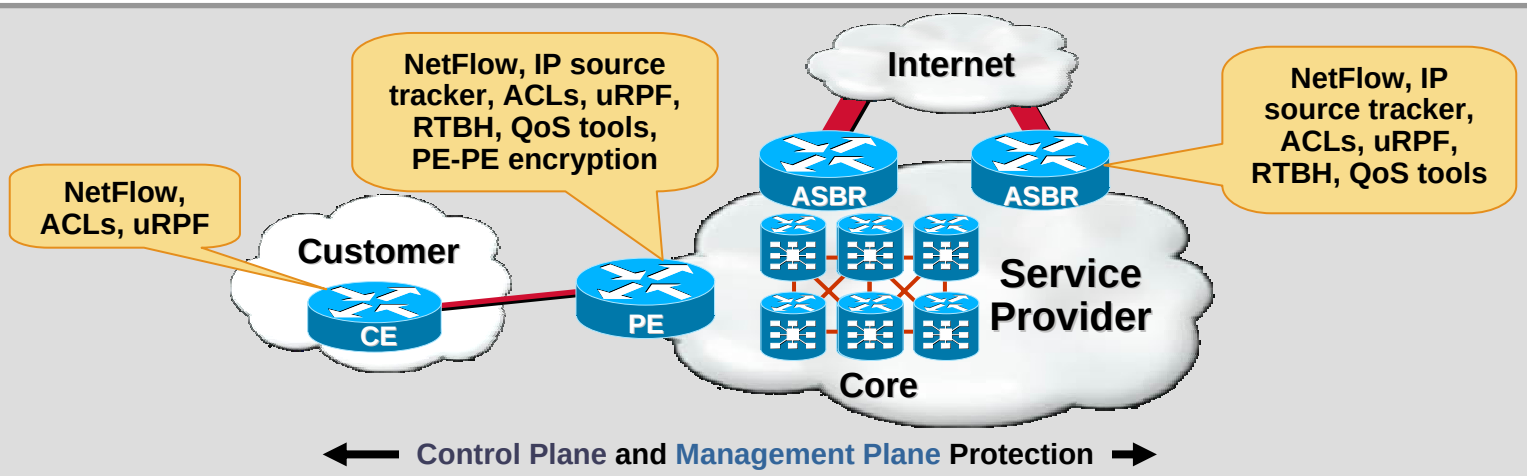
5. Cleaned traffic is injected back to the data path to reach the actual destination.

Traffic is continually monitored by Netflow and the Cisco Detector.

Network Foundation Protection

Protects infrastructure, enables continuous service delivery

Data Plane	• Detects traffic anomalies and responds to attacks in realtime • Technologies: NetFlow, IP source tracker, ACLs, uRPF, RTBH, QoS tools
Control Plane	• Defense-in-depth protection for routing control plane • Technologies: Receive ACLs, control plane policing, routing protection
Management Plane	• Secure and continuous management of Cisco® IOS® network infrastructure • Technologies: CPU and memory thresholding, dual export syslog, encrypted access, SNMPv3, security audit



Cisco Traffic Anomaly Detector
Detecting and Defeating Complex DDoS Attacks

Programmable Element Enabling:

- Sophisticated behavior-based anomaly detection
- Granular, per-connection state analysis of all packets
- Behavioral recognition engine eliminates the need to continually update profiles
- Session-state context recognizes validated session traffic

Delivering:

- Highly accurate identification of all types of known and Day Zero attacks
- Fast and thorough detection of the most elusive and sophisticated attacks
- Elimination of the need to continually update profiles
- Reduced number of alerts and false positives common with static signature-based approaches

- **Detects per-flow deviations**
- **Identifies anomalous behavior**
- **Responds based on user preference**

Traffic Anomaly Detector XT 5600

Traffic Anomaly Detector Module

Cisco Guard
Detecting and Defeating Complex DDoS Attacks

Programmable Element Enabling:

- Detailed, granular, per-flow analysis and blocking
- Integrated dynamic filtering and active verification technologies
- Protocol analysis and rate limiting
- Intuitive, Web-based GUI simplifies policy definition, operational monitoring, and reporting

Delivering:

- Precision traffic protection, while allowing legitimate transactions to flow
- Rapid, auto protection against all types of assaults, even Day Zero attacks
- Admission of only traffic volumes that will not overwhelm downstream devices
- Identification/blocking all sizes of attacks, including those launched by distributed zombie hosts

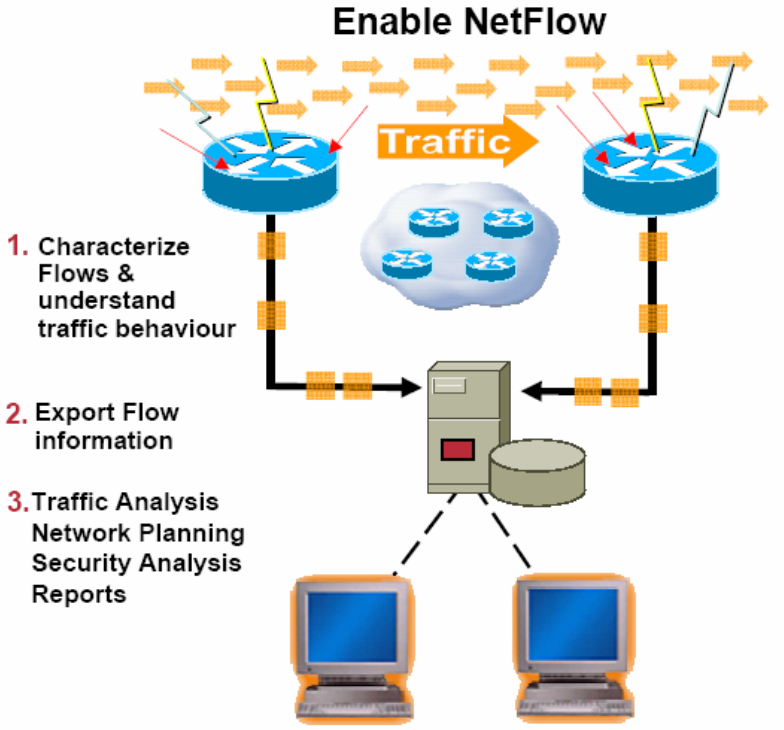
Helps ensure uninterrupted business operations from even the most malicious assaults

Traffic Anomaly Guard XT 5650

Traffic Anomaly Guard Module

Cisco IOS NetFlow

- **NetFlow is a standard for acquiring IP network and operational data**
- **Benefits**
  - **Understand the impact of network changes and services**
  - **Improve network usage and application performance**
  - **Reduce IP service and application costs**
  - **Optimize network costs**
  - **Detect and classify security agents**



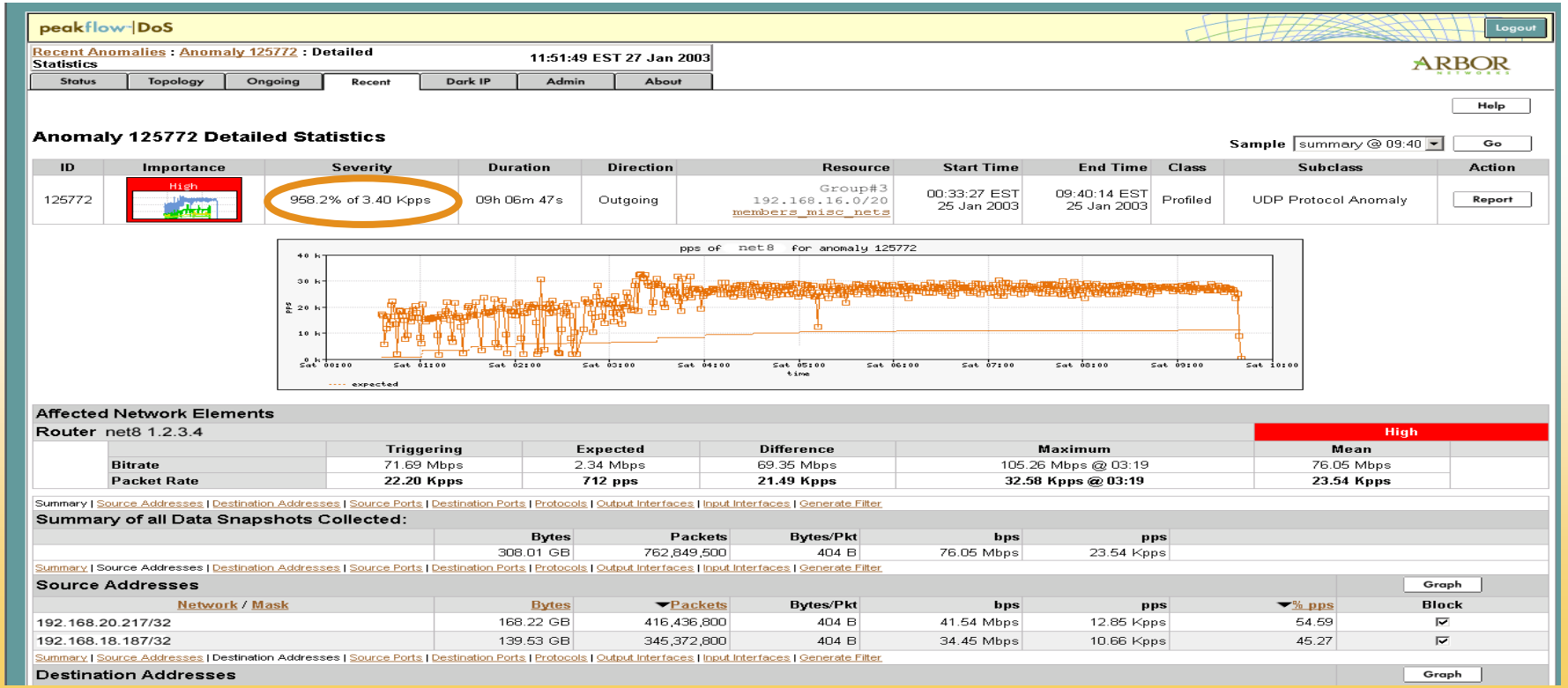
Cisco 800 | Cisco 1700/1800 | Cisco 2600/2800 | Cisco 3600/ 3700/ 3800 | Cisco 4500/ 4700 | Cisco 5300/ 5400/ 5800 | Cisco 7200/ 7300/ 7400/ 7500 | Cisco 4500 ASIC | Cisco 6500/ 7600 ASIC | Cisco 10000/ 12000 CRS-1

Supported Platforms

Day Zero Attack Detection with NetFlow

Benefits:

- **Monitor traffic for anomalies**
- **Identify and classify the attack**
- **Trace attack to its source**



References
Product and Technology Enablers

- **NetFlow IOS® on Cisco® Routers**

  http://www.cisco.com/go/netflow

- **Network Foundation Protection**

  http://www.cisco.com/go/nfp

- **Cisco Guard XT Appliance and Cisco Anomaly Guard Service Module**

  http://www.cisco.com/en/US/products/ps5888/index.html

  http://www.cisco.com/en/US/products/ps6235/index.html

- **Cisco Traffic Anomaly Detector XT Appliance and Cisco Traffic Anomaly Detector Service Module**

  http://www.cisco.com/en/US/products/ps5887/index.html

  http://www.cisco.com/en/US/products/ps6236/index.html

- **Router Security**

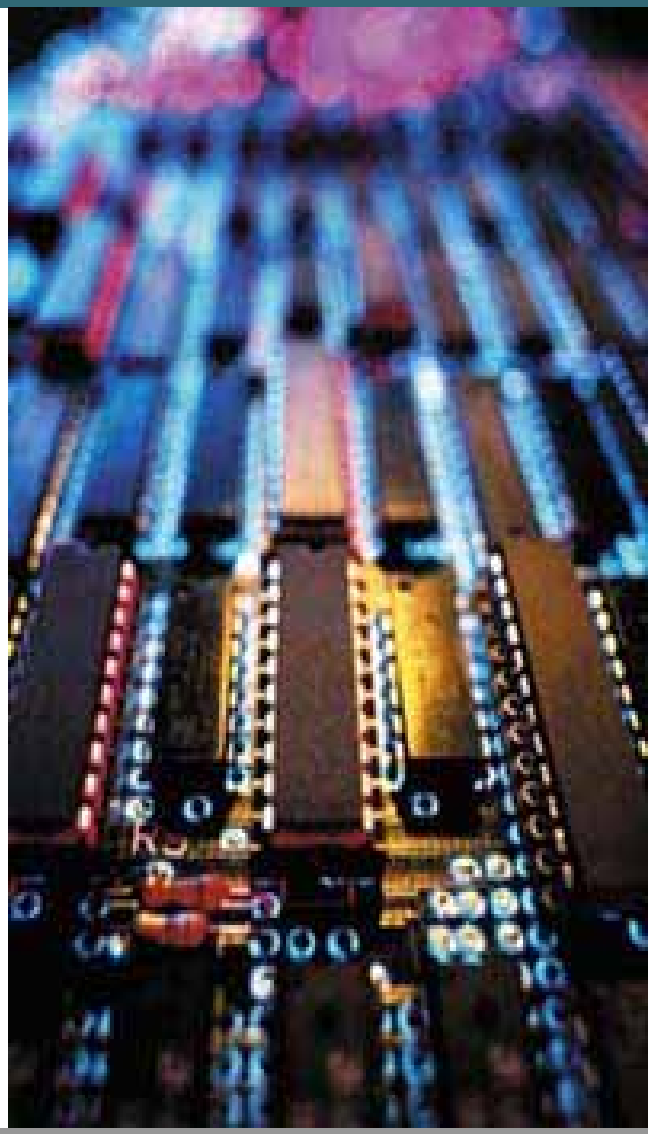
  http://www.cisco.com/go/security

- **Arbor Networks (a Cisco Partner)**

  http://www.arbor.net/products_sp.php

Conclusion

- **DDoS is a real and growing threat that can impact your business delivery and business reputation**
- **Take a proactive approach to handling security on your network**
- **DDoS protection is a managed security service opportunity**
- **Protect your infrastructure with DDoS protection and NFP**
- **Cisco® has the leading products and solutions to address the security threats**
- **Contact your sales contact to find out more today**



Network Foundation Protection Features and Benefits

Plane	Cisco IOS Services	Benefits
Data Plane	NetFlow	• Macro-level anomaly-based DDoS detection; provides rapid confirmation and isolation of attack
	IP source tracker	• Quickly and efficiently pinpoints the source interface an attack is coming from
	Access control lists (ACLs)	• Protect edge routers from malicious traffic; explicitly permit the legitimate traffic that can be sent to the edge router's destination address
	Unicast reverse path forwarding (uRPF)	• Mitigates problems caused by the introduction of malformed or spoofed IP source addresses into either the service provider or customer network
	Remotely triggered black holing (RTBH)	• Drops packets based on source IP address; filtering is at line rate on most capable platforms. Hundreds of lines of filters can be deployed to multiple routers even while the attack is in progress.
	QoS tools	• Protects against flooding attacks by defining QoS policies to limit bandwidth or drop offending traffic (identify, classify, and rate limit)
	PE-to-PE encryption	• Provides strong encryption within service provider network
Control Plane	Receive ACLs	• Control the type of traffic that can be forwarded to the processor
	Control plane policing	• Provides QoS control for packets destined to the control plane of the routers; ensures adequate bandwidth for high-priority traffic such as routing protocols
	Routing protection	• MD5 neighbor authentication protects routing domain from spoofing attacks • Redistribution protection safeguards network from excessive conditions • Overload protection (e.g., prefix limits) enhances routing stability
Management Plane	CPU and memory thresholding	• Protects CPU and memory resources of IOS device against DoS attacks
	Dual export syslog	• Syslog exported to dual collectors for increased availability
	Encrypted access	• Encryption access for users (SSHv2, SSL) and management applications
	SNMPv3	• Secure SNMP management for third-party or custom-built applications
	Security audit	• Provides audit trail of configuration changes