CISCO DDoS MITIGATION SERVICE PROVIDER SOLUTIONS

February 15, 2005

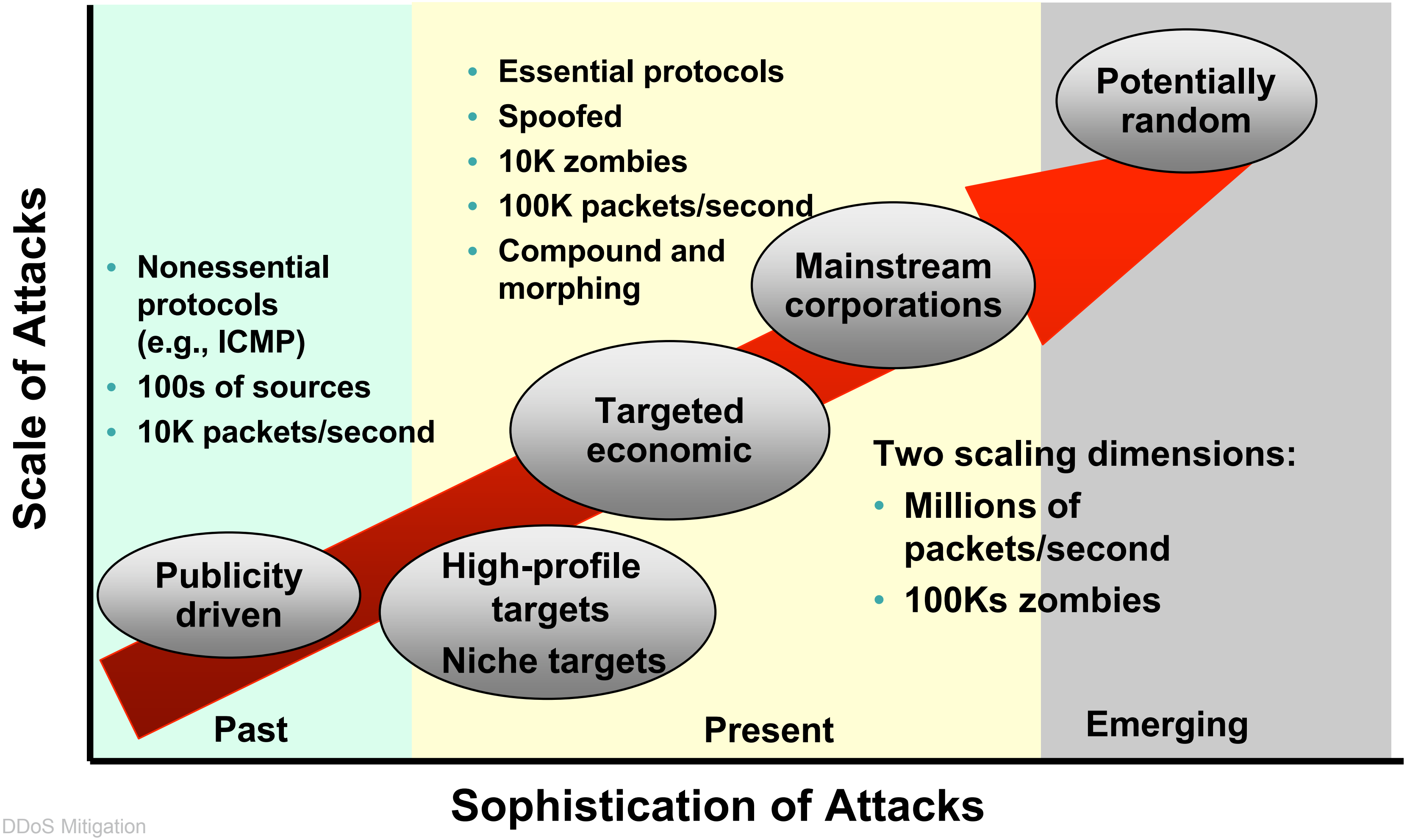
Executive Summary

- Detects AND MITIGATES the broadest range of distributed denial of service (DDoS) attacks
- With the granularity and accuracy to ENSURE BUSINESS CONTINUITY by forwarding legitimate transactions
- Delivering the performance and architecture suitable for the LARGEST ENTERPRISES AND PROVIDERS
- Addresses DDoS attacks today, and its network-based behavioral anomaly capability will be extended to additional threats

THE DDoS PROBLEM

Attack Evolution

Stronger and More Widespread



- Nonessential protocols (e.g., ICMP)
- 100s of sources
- 10K packets/second

- Essential protocols
- Spoofed
- 10K zombies
- 100K packets/second
- Compound and morphing

Two scaling dimensions:

- Millions of packets/second
- 100Ks zombies

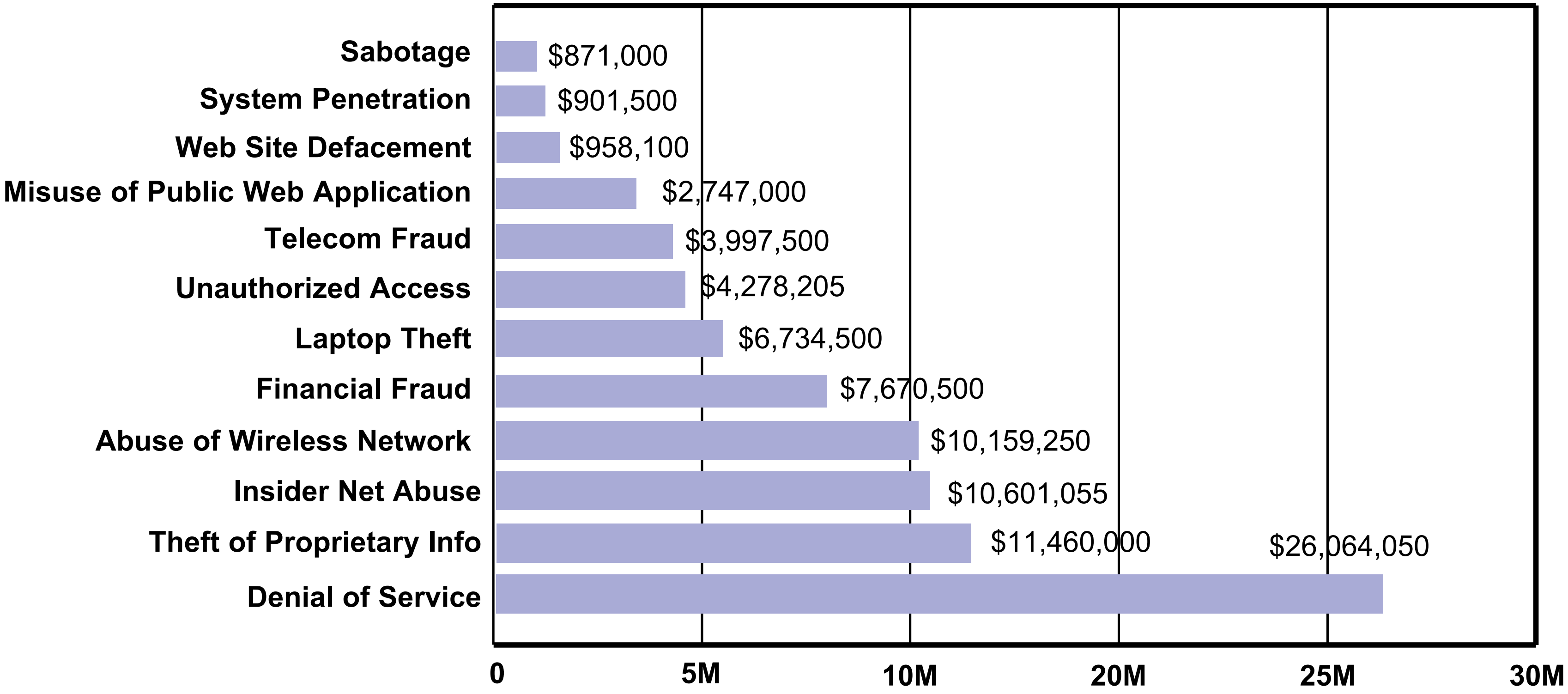
“Much larger attack network than anything before. This horsepower could take down thousands of big sites…at the same time, and keep them down for quite a while.”

“MyDoom Taste of Viruses to Come, Says Security Analyst,” Reuters, February 3, 2004

Security Challenges

The Cost of Threats

Dollar Amount of Loss by Type of Attack (CSI/FBI 2004 Survey)



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

Total Losses for 2004—$141,496,560

2004: 269 Respondents

“E-biz Sites Hit With Targeted Attacks”

“16% of the attacks against e-commerce sites were identified as targeted. Last year, only 4% were aimed at specific sites.”

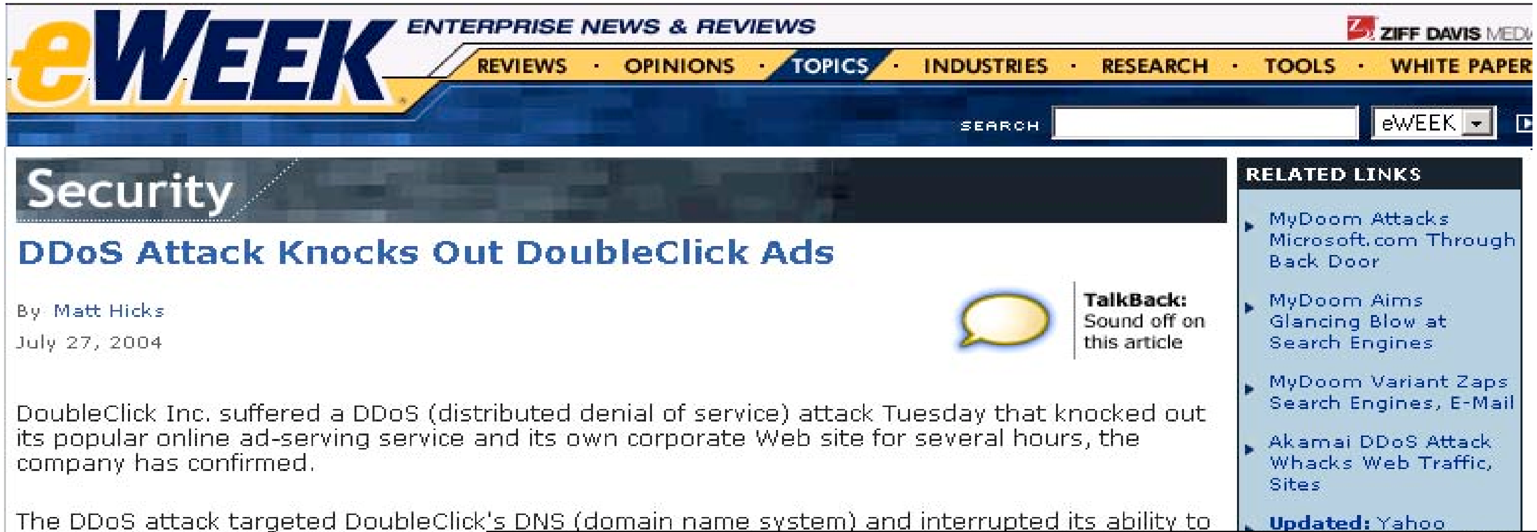
ComputerWorld, September 27, 2004

“Extortion schemes that use attacks like the one against Authorize.Net are becoming more common . . . definitely targeted, ransom-type attacks, and there's going to be a lot more of them.”

John Pescatore, Gartner Inc.
ComputerWorld, September 27, 2004

DDoS Is a Business Issue

Impacts Revenue and Customer Retention



eWEEK
ENTERPRISE NEWS & REVIEWS
ZIFF DAVIS MEDI
REVIEWS · OPINIONS · TOPICS · INDUSTRIES · RESEARCH · TOOLS · WHITE PAPER
SEARCH
eWEEK
Security
RELATED LINKS
TalkBack: Sound off on this article

DDoS Attack Knocks Out DoubleClick Ads

By Matt Hicks
July 27, 2004

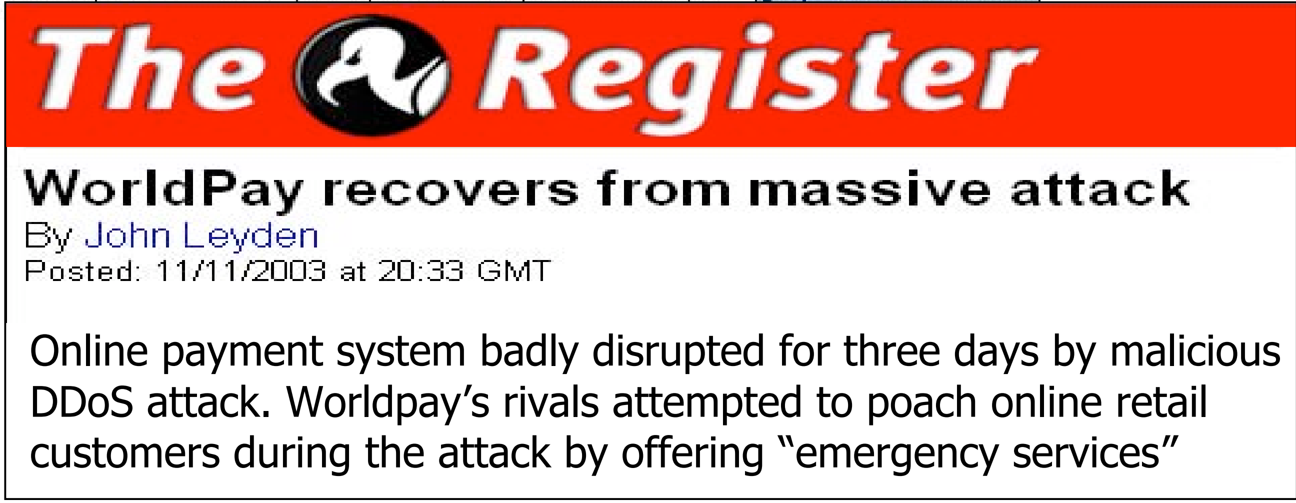
DoubleClick Inc. suffered a DDoS (distributed denial of service) attack Tuesday that knocked out its popular online ad-serving service and its own corporate Web site for several hours, the company has confirmed.

The DDoS attack targeted DoubleClick's DNS (domain name system) and interrupted its ability to serve online ads to its 900 customers
Jennifer Blum said.

- MyDoom Attacks Microsoft.com Through Back Door
- MyDoom Aims Glancing Blow at Search Engines
- MyDoom Variant Zaps Search Engines, E-Mail
- Akamai DDoS Attack Whacks Web Traffic, Sites
- **Updated:** Yahoo

Not just downtime:

- Lost customers
- Damaged reputations
- Contractual liabilities



WorldPay recovers from massive attack

By John Leyden
Posted: 11/11/2003 at 20:33 GMT

Online payment system badly disrupted for three days by malicious DDoS attack. Worldpay’s rivals attempted to poach online retail customers during the attack by offering “emergency services”

SOLUTION OVERVIEW

DDoS Protection
Cisco Service Modules

FCS 1QCY05

Cisco Anomaly Guard Module

Attack ANALYSIS AND MITIGATION

Diverts traffic flows for ON-DEMAND SCRUBBING

Cisco Traffic Anomaly Detector Module

Attack DETECTION to support on-demand, shared scrubbing

Monitors COPY OF TRAFFIC

Cisco DDoS Product Family

**Maximum deployment flexibility.
Similar functionality and performance.
Interoperable for mixed deployments.**

DDoS Mitigation

Cisco Guard XT 5650

Cisco Anomaly Guard Module

DDoS Detection

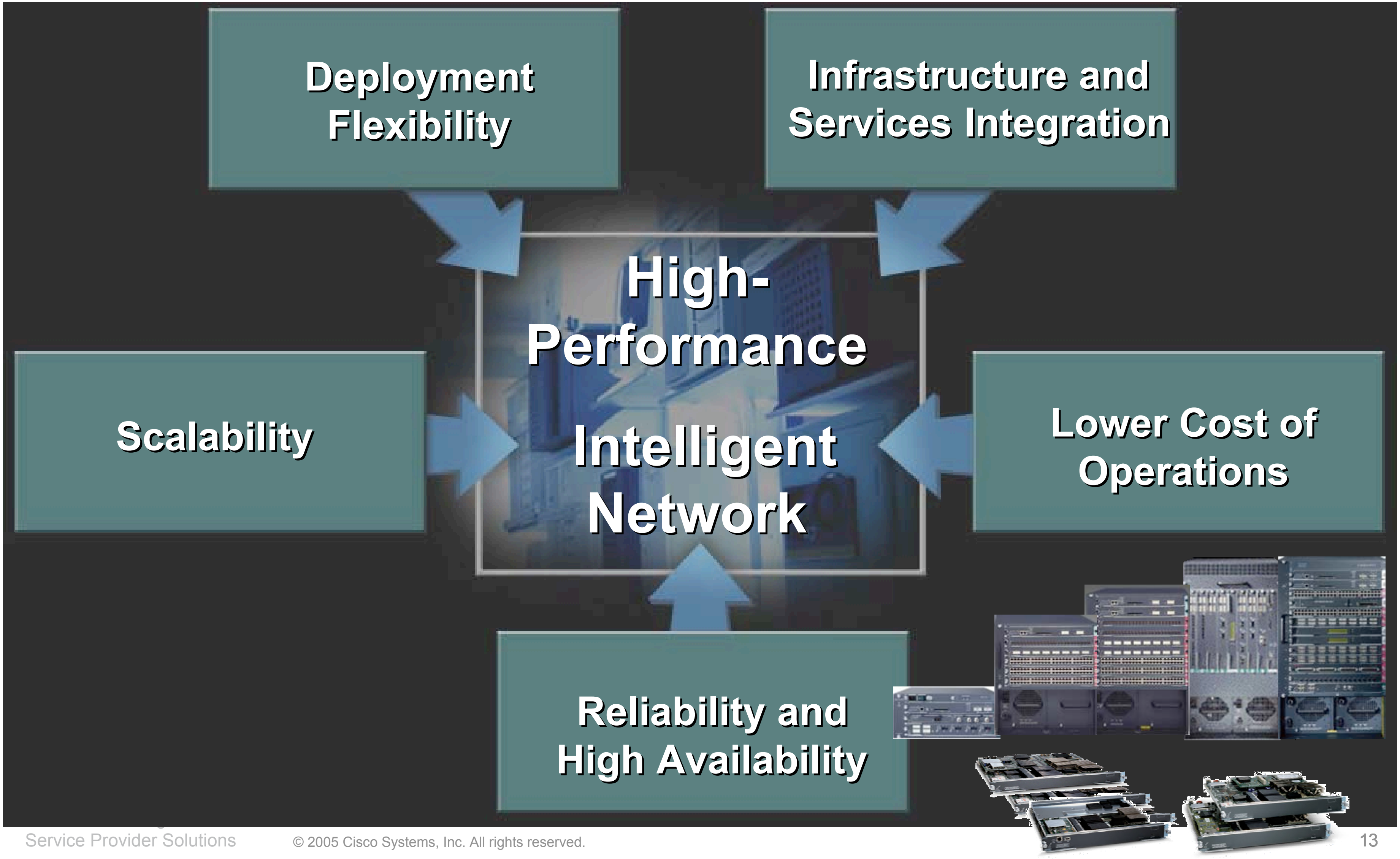
Cisco Traffic Anomaly Detector XT 5600

Cisco Traffic Anomaly Detector Module

DDoS Protection
Cisco Service Modules (cont.)

- Guard/Detector MVP-OS Release 4.0
- Single-slot modules for Cisco Catalyst® 6500 Switch and 7600 Router
- Interfaces via backplane—no external ports
- Gigabit performance—future licensed upgrade to multigigabit supported
- Native Cisco IOS® 12.2(18)SXD3
- Multiple Guards and Detectors per chassis and single-destination IP/zone
- CLI, Web GUI, and SNMP management

Integrated Services Benefits



Deployment Flexibility

Infrastructure and Services Integration

High-Performance

Scalability

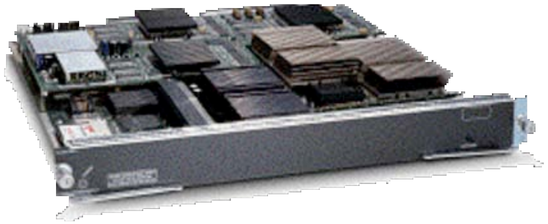
Intelligent Network

Lower Cost of Operations

Reliability and High Availability

Layer 4–7 Services Modules Family

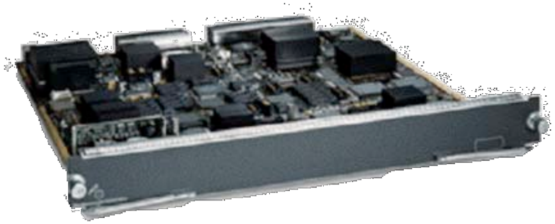
NAM-1 and NAM-2 Module



Firewall Module

IDSM-2 Module

CSM Module



VPN Module

SSL Module

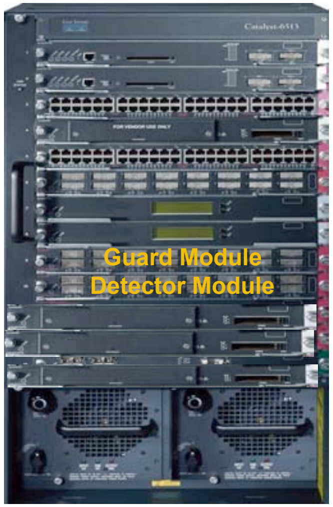
Cisco Anomaly Guard Module

Cisco Traffic Anomaly Detector Module

Flexible Deployment Options

Integrated system:

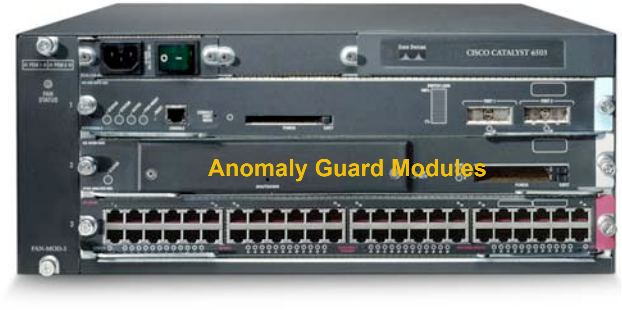
- **Fits existing switch/routing infrastructure with other services**
- **Utilizes available slots—no interface ports or rack space**
- **Ideal for data center deployments of 1–3 modules**
- **Intrachassis diversion**



Flexible Deployment Options (cont.)

Dedicated system:

- New chassis dedicated to DDoS
- Supports large range of flexible I/O
- Ideal for high-capacity deployments (4+ modules) with supervisor for load leveling
- External diversion via Cisco IOS® supervisor routing



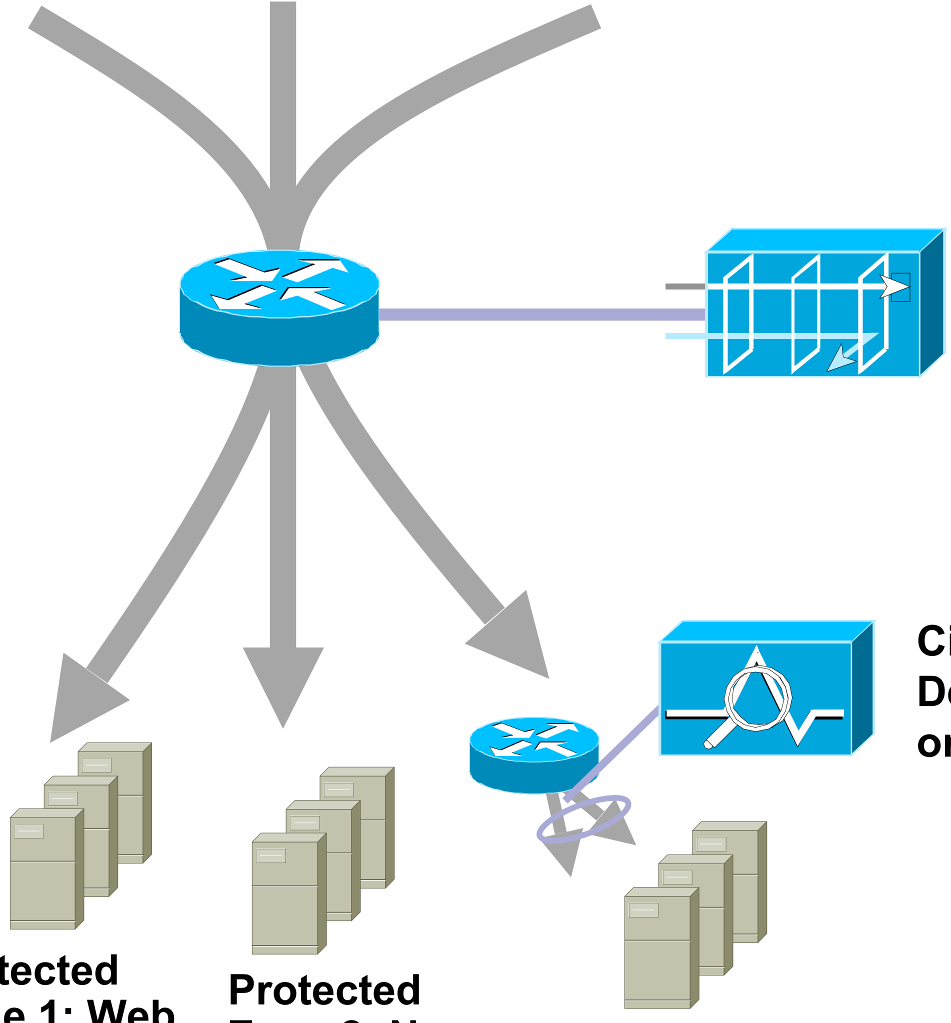
Key Features

DIVERSION ARCHITECTURE

MULTISTAGE VERIFICATION PROCESS

DIVERSION ARCHITECTURE

Dynamic Diversion At Work



Cisco Anomaly Guard Module

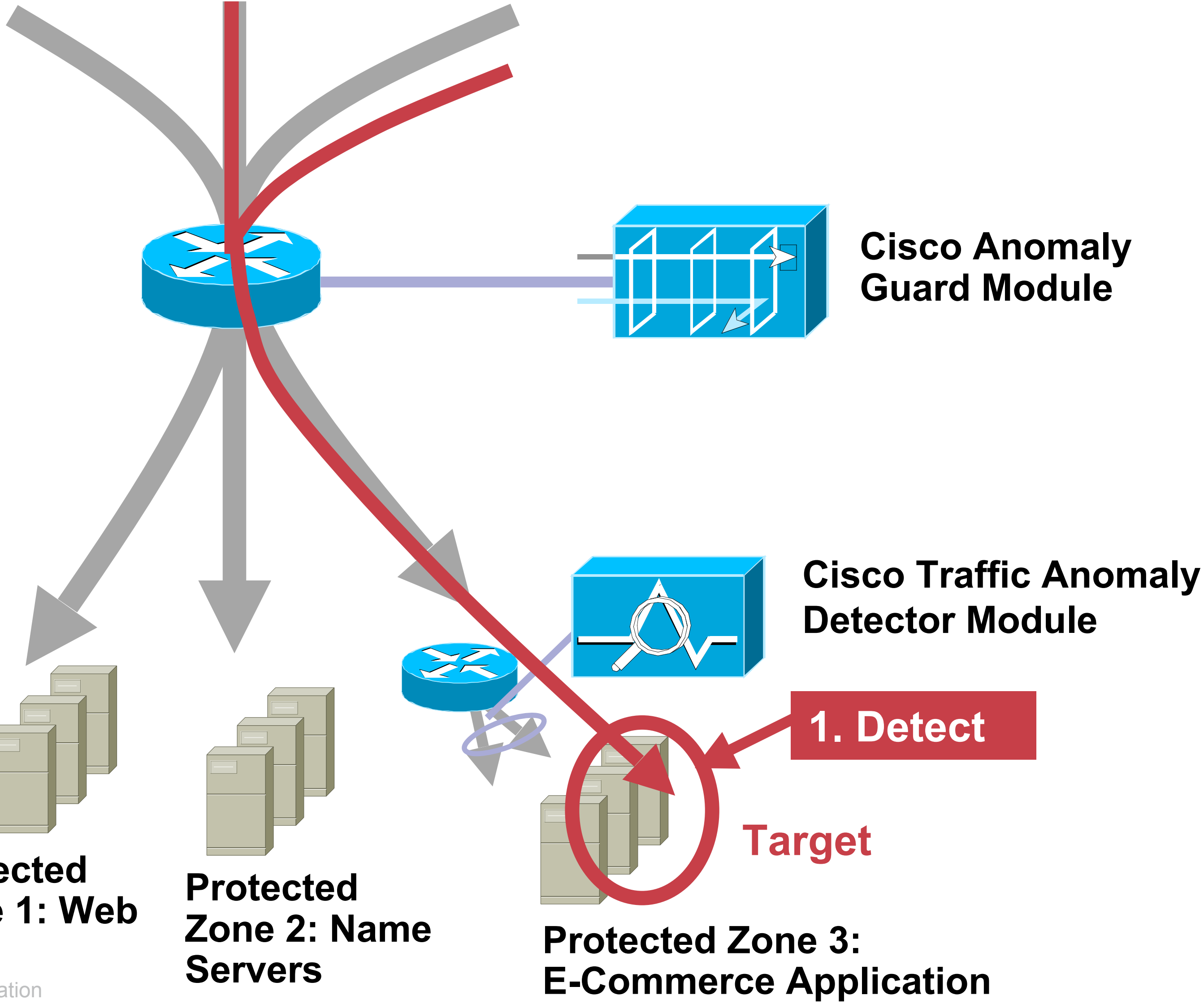
Cisco Traffic Anomaly Detector Module (or Cisco IDS or third- party system)

Protected Zone 1: Web

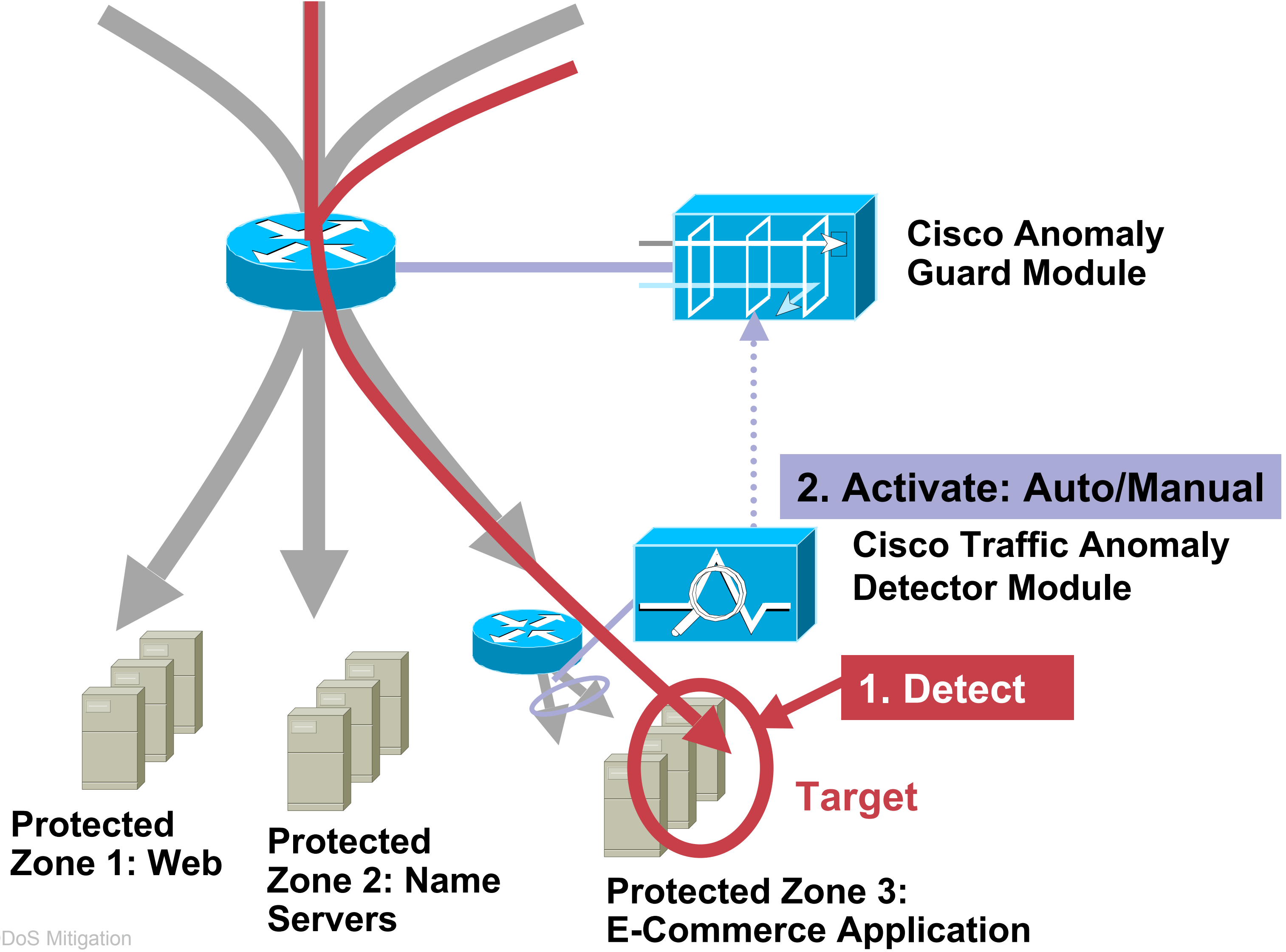
Protected Zone 2: Name Servers

Protected Zone 3: E-Commerce Application

Dynamic Diversion At Work


Cisco Anomaly Guard Module
Cisco Traffic Anomaly Detector Module
1. Detect
Target
Protected Zone 1: Web
Protected Zone 2: Name Servers
Protected Zone 3: E-Commerce Application

Dynamic Diversion At Work



Cisco Anomaly Guard Module

2. Activate: Auto/Manual

Cisco Traffic Anomaly Detector Module

1. Detect

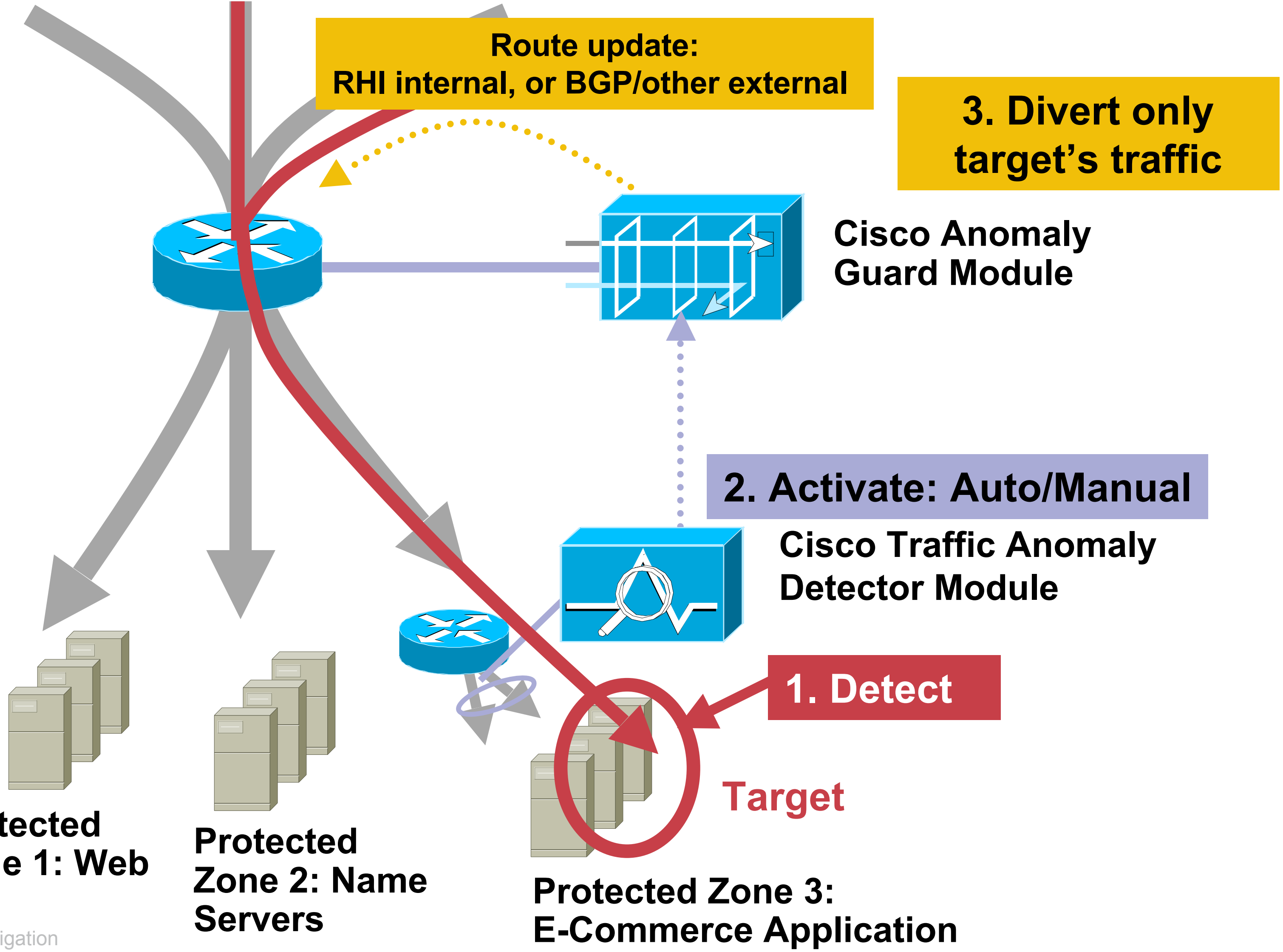
Target

Protected Zone 1: Web

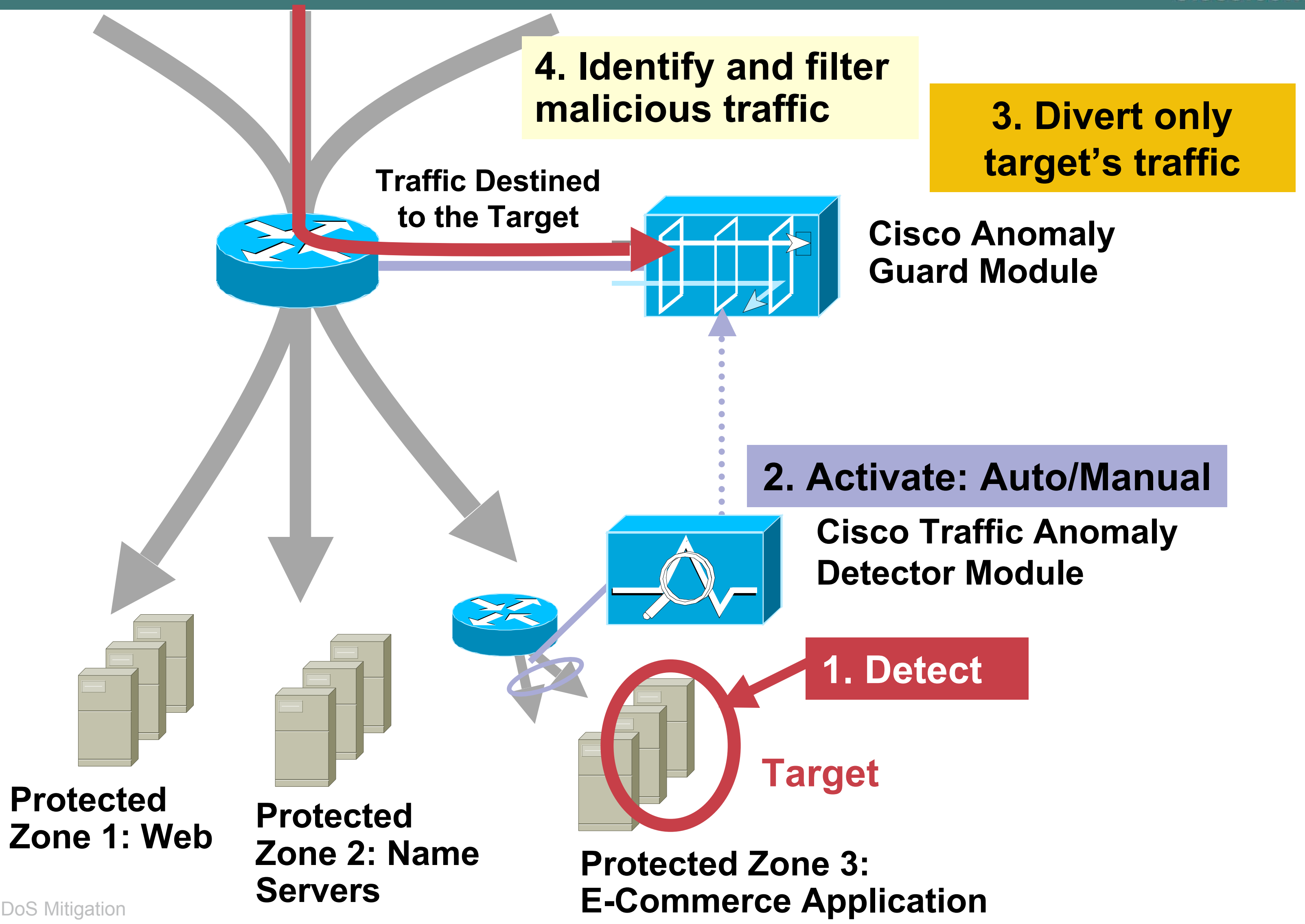
Protected Zone 2: Name Servers

Protected Zone 3: E-Commerce Application

Dynamic Diversion At Work


Route update:
RHI internal, or BGP/other external
3. Divert only target's traffic
Cisco Anomaly Guard Module
2. Activate: Auto/Manual
Cisco Traffic Anomaly Detector Module
1. Detect
Target
Protected Zone 1: Web
Protected Zone 2: Name Servers
Protected Zone 3: E-Commerce Application

Dynamic Diversion At Work



4. Identify and filter malicious traffic

3. Divert only target's traffic

Traffic Destined to the Target

Cisco Anomaly Guard Module

2. Activate: Auto/Manual

Cisco Traffic Anomaly Detector Module

1. Detect

Target

Protected Zone 1: Web

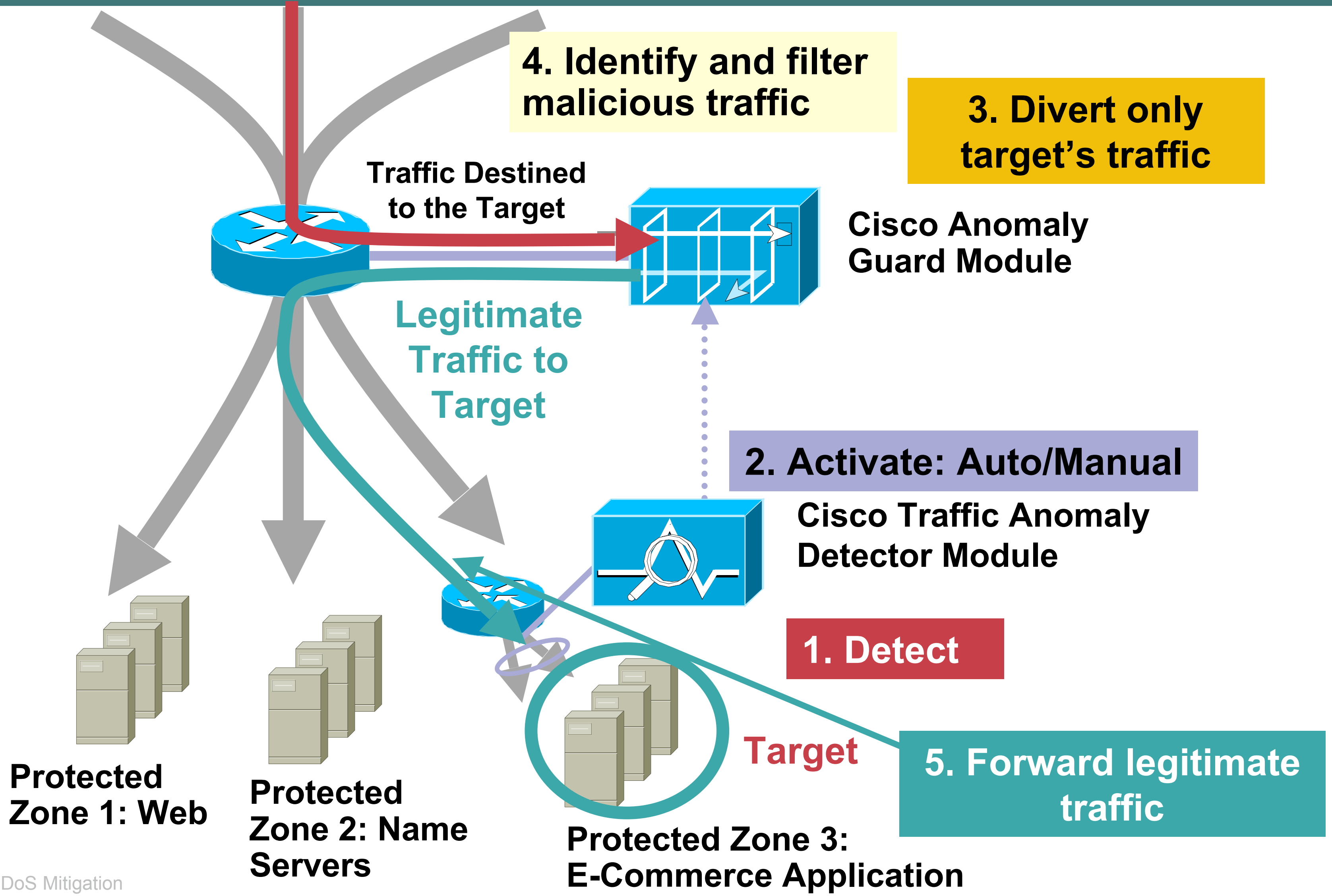
Protected Zone 2: Name Servers

Protected Zone 3: E-Commerce Application

```
O       192.168.3.0/24 [110/2] via 10.0.0.3, 2d11h, GigabitEthernet2
B       192.168.3.128/32 [20/0] via 10.0.0.2, 00:00:01
```

192.168.3.128 = zone   10.0.0.2 = Guard

Dynamic Diversion At Work



4. Identify and filter malicious traffic

3. Divert only target's traffic

Traffic Destined to the Target

Cisco Anomaly Guard Module

Legitimate Traffic to Target

2. Activate: Auto/Manual

Cisco Traffic Anomaly Detector Module

1. Detect

Target

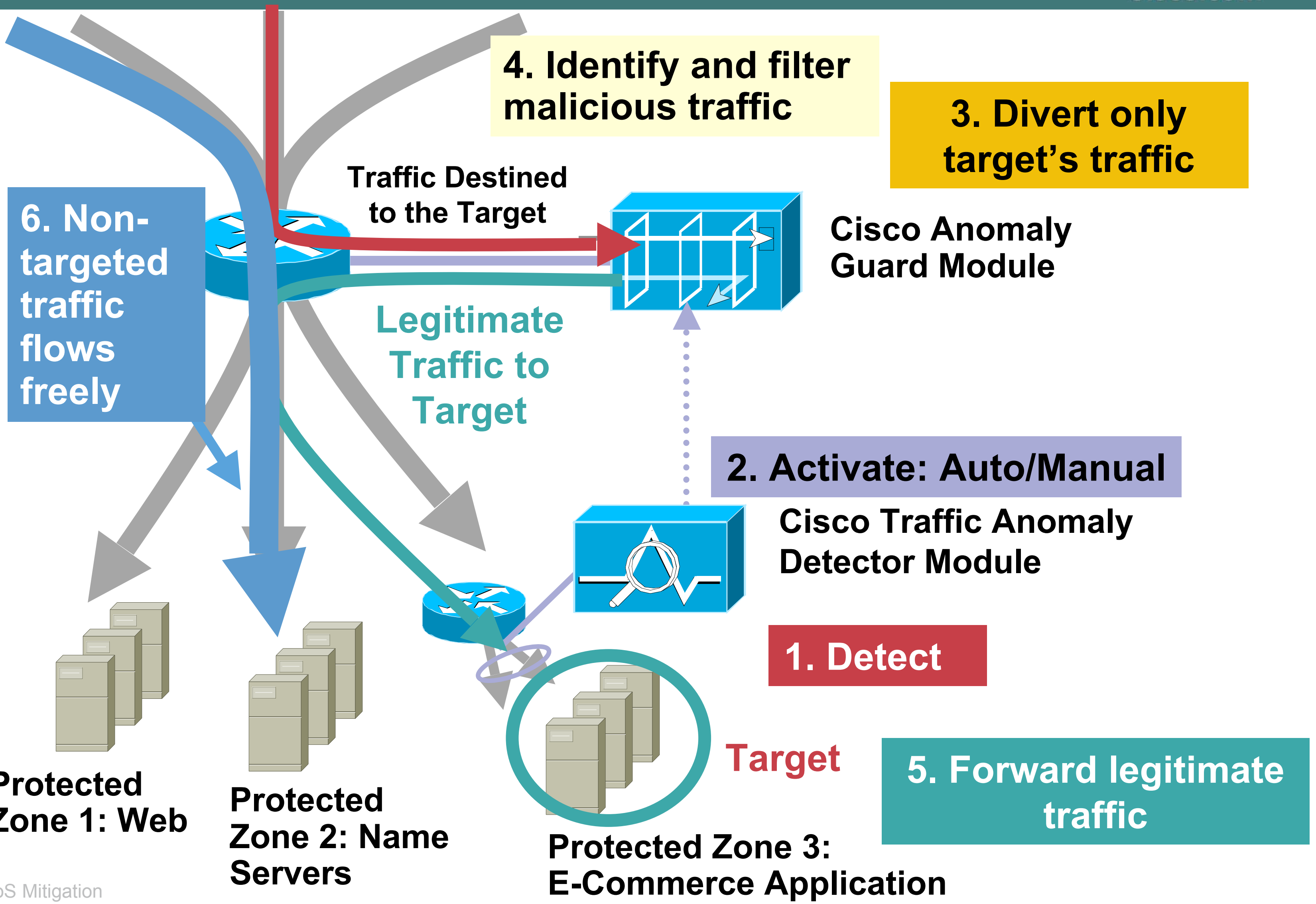
5. Forward legitimate traffic

Protected Zone 1: Web

Protected Zone 2: Name Servers

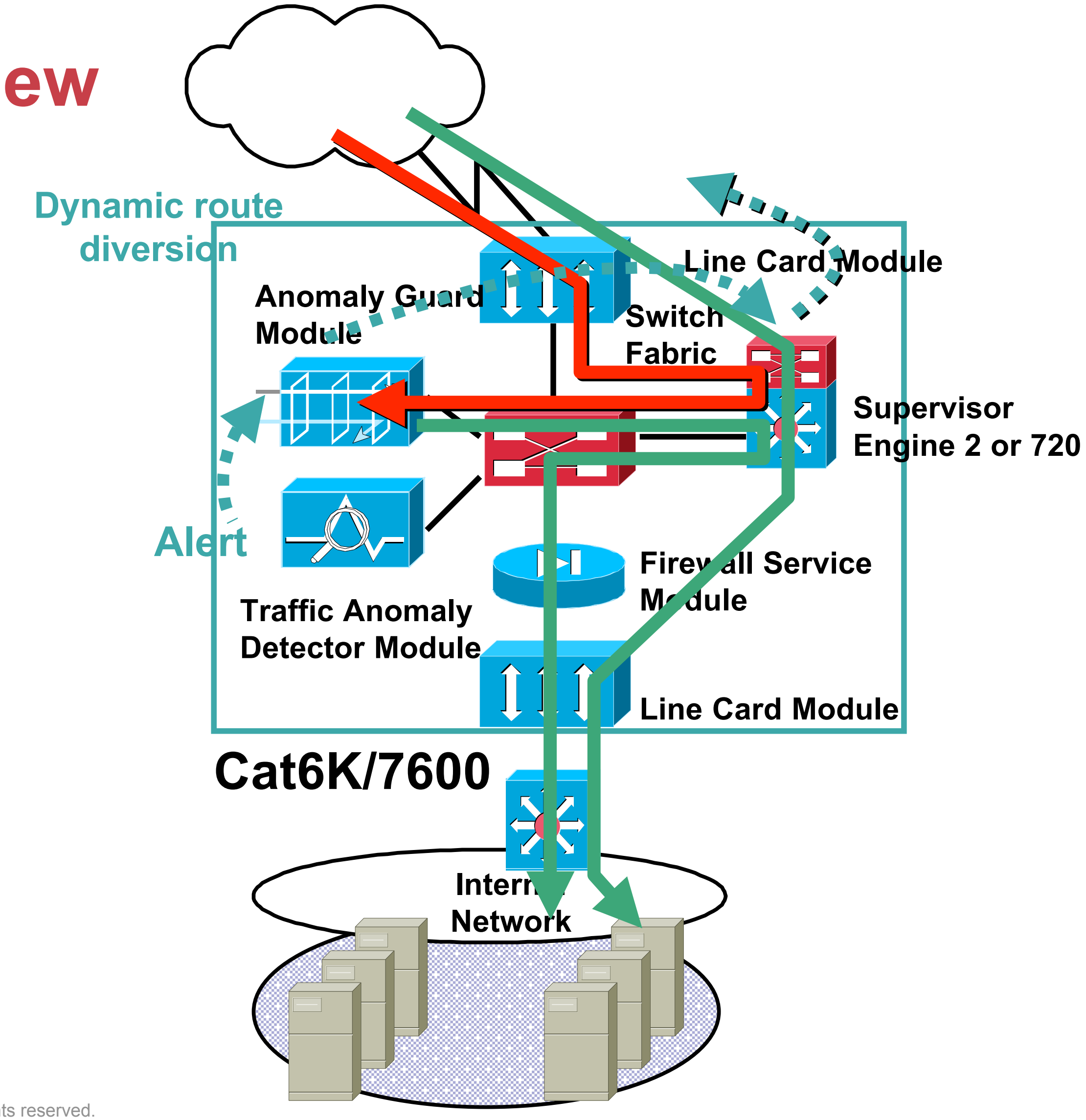
Protected Zone 3: E-Commerce Application

Dynamic Diversion At Work


4. Identify and filter malicious traffic
3. Divert only target's traffic
Traffic Destined to the Target
Cisco Anomaly Guard Module
6. Non-targeted traffic flows freely
Legitimate Traffic to Target
2. Activate: Auto/Manual
Cisco Traffic Anomaly Detector Module
1. Detect
Target
5. Forward legitimate traffic
Protected Zone 1: Web
Protected Zone 2: Name Servers
Protected Zone 3: E-Commerce Application

Cisco Catalyst Service Module

Solution Overview



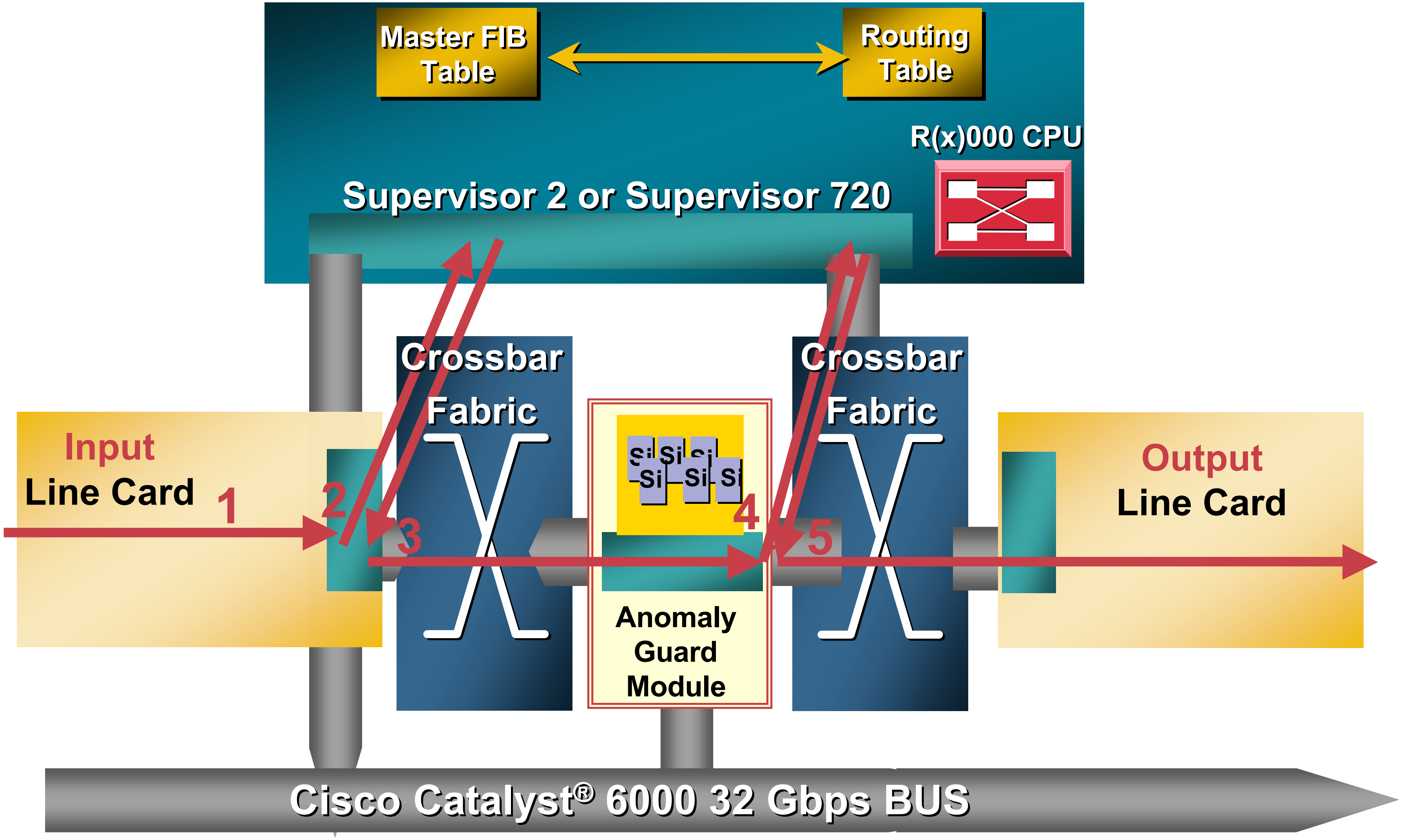
Cisco Catalyst Service Module (cont.)

- Maintains "on-demand" scrubbing model
  - Internal to chassis from Supervisor to Guard
  - Uses Route Health Injection protocol
- Supports dedicated "appliance" mode
  - Suitable for cluster
  - Supervisor redistributes route update

- Cisco Catalyst® 6K/7600 Router benefits:
  - IOS routing: extensive protocol and tunneling support and familiar CLI
  - Extensive interfaces including fiber OC/STM
  - Control Plane Policing for DDoS hardening

Anomaly Guard Module Packet Flow

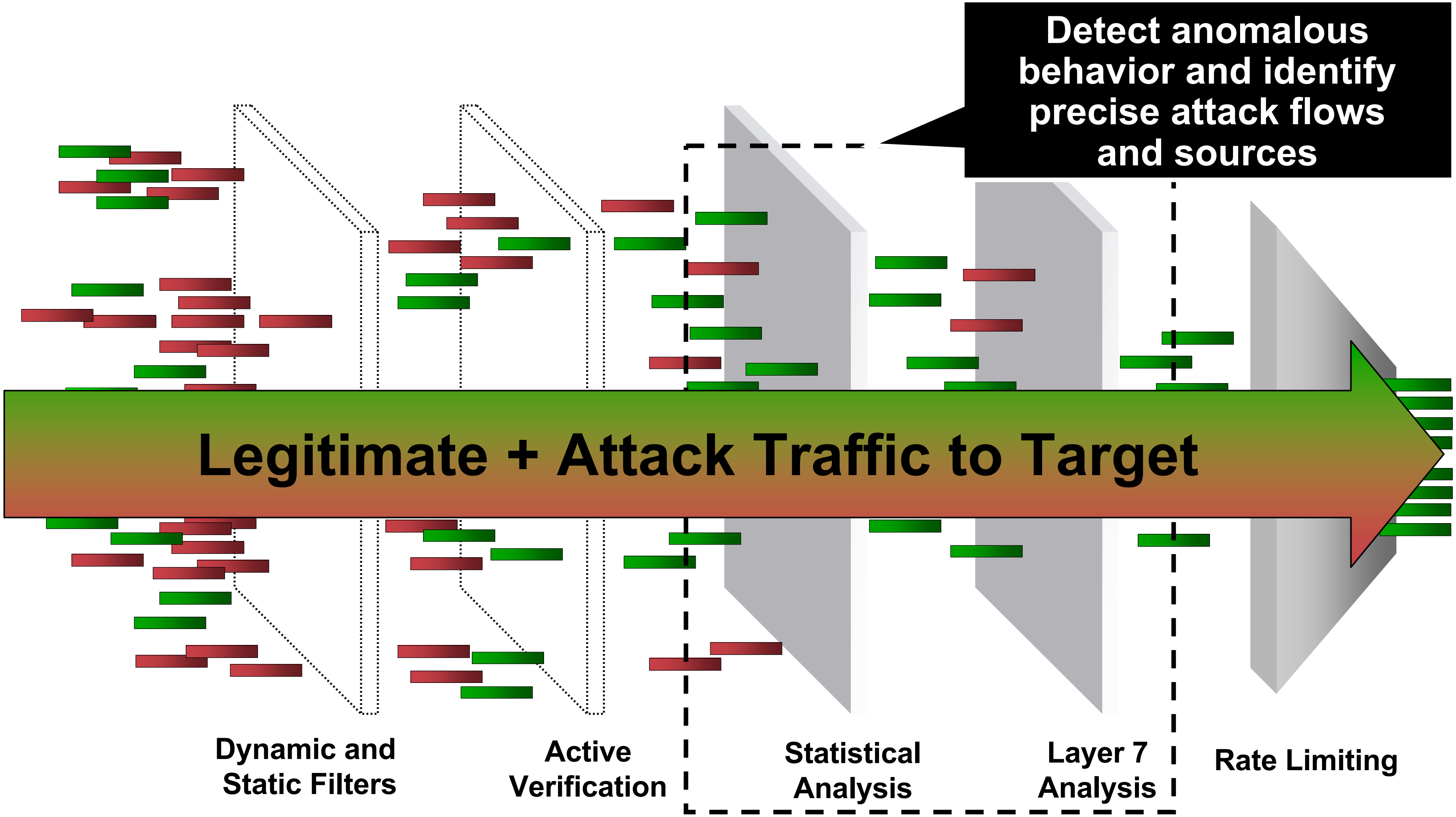
Supervisor 2/SFM or Supervisor 720



MULTISTAGE VERIFICATION PROCESS

Multiverification Process (MVP)

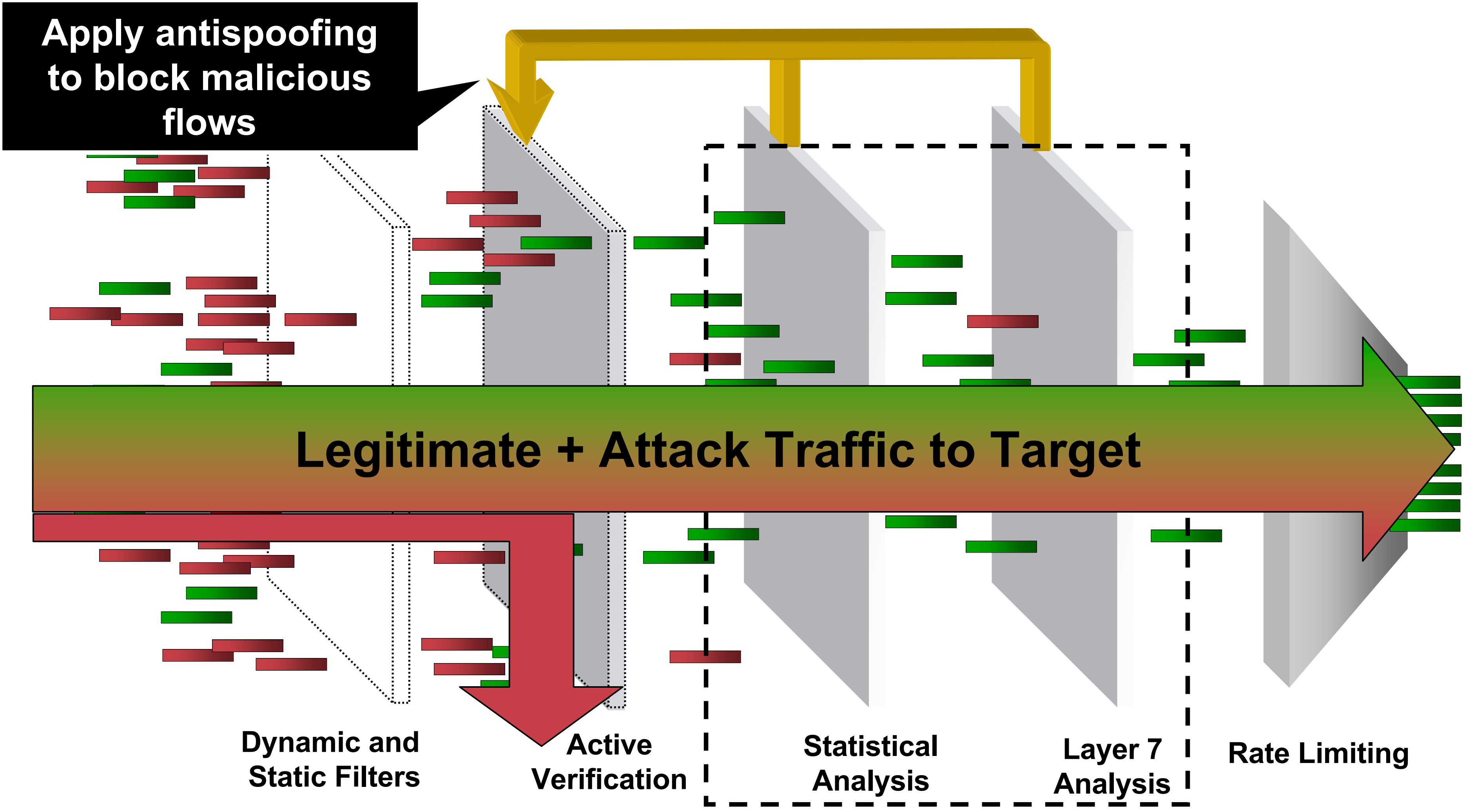
Integrated Defenses in the Guard



Detect anomalous behavior and identify precise attack flows and sources

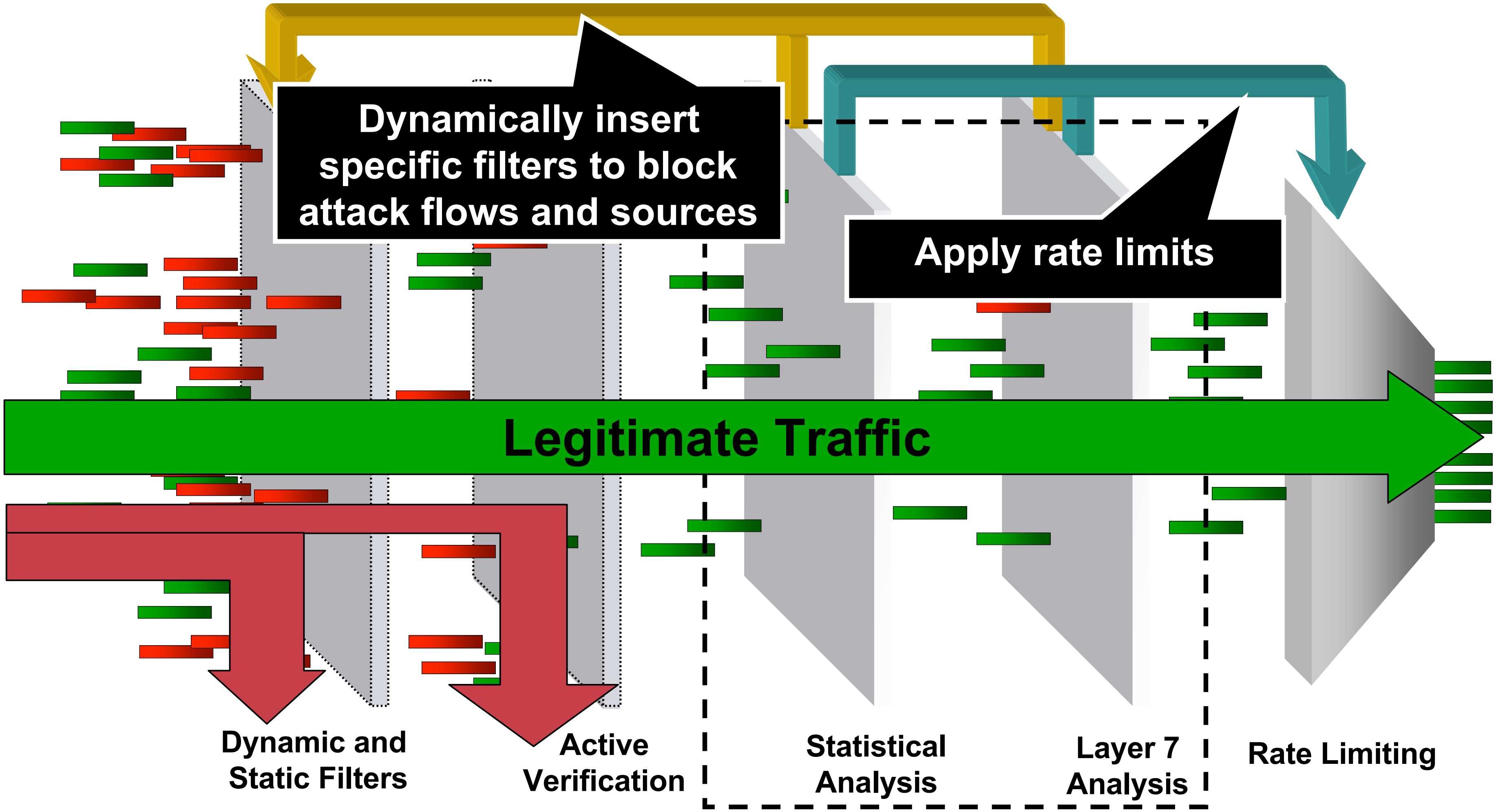
Multiverification Process (MVP)

Integrated Defenses in the Guard


Apply antispoofing to block malicious flows
Legitimate + Attack Traffic to Target
Dynamic and Static Filters
Active Verification
Statistical Analysis
Layer 7 Analysis
Rate Limiting

Multiverification Process (MVP)

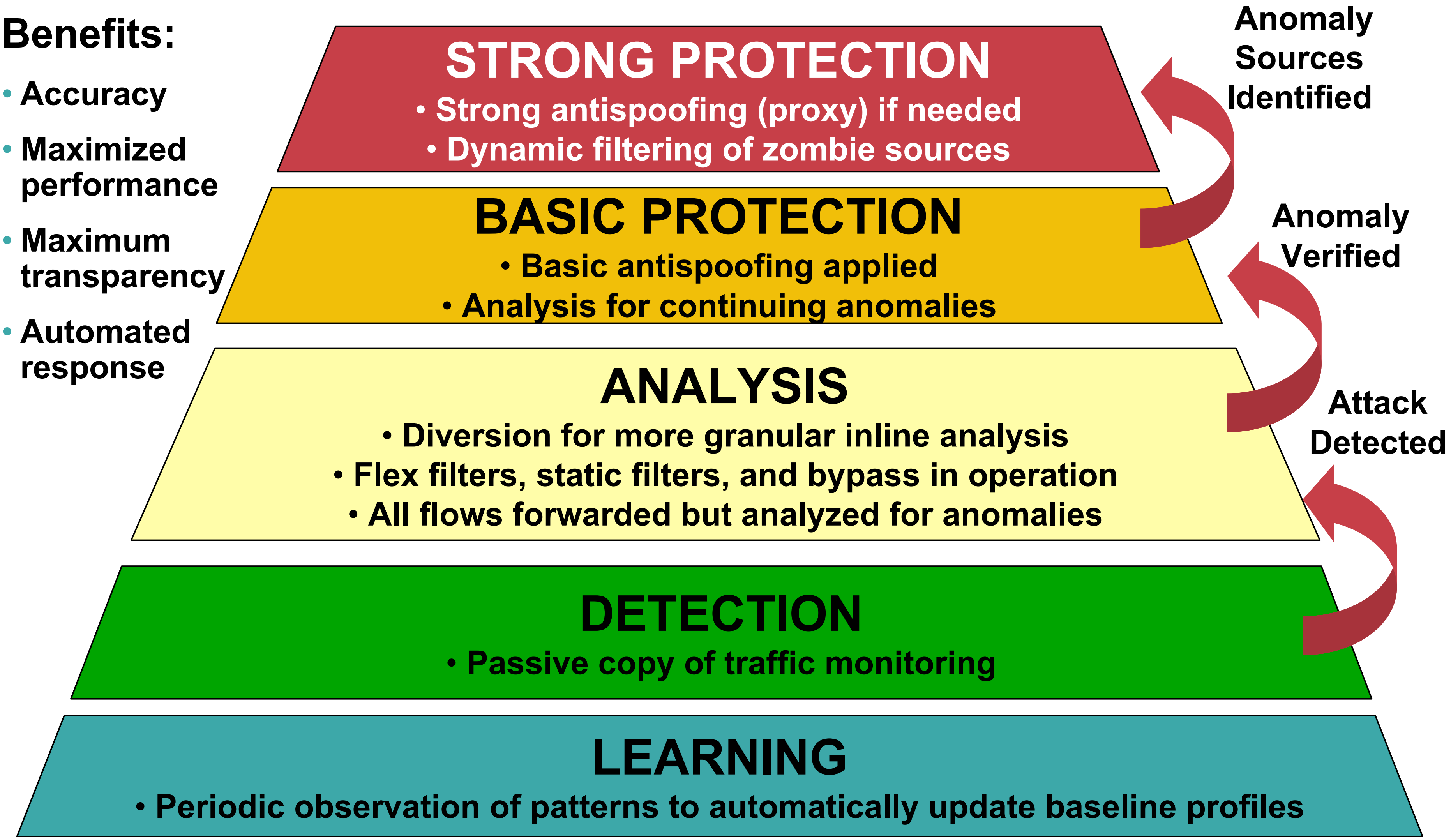
Integrated Defenses in the Guard



Intelligent Countermeasures

Benefits:

- Accuracy
- Maximized performance
- Maximum transparency
- Automated response



STRONG PROTECTION

- Strong antispoofing (proxy) if needed
- Dynamic filtering of zombie sources

BASIC PROTECTION

- Basic antispoofing applied
- Analysis for continuing anomalies

ANALYSIS

- Diversion for more granular inline analysis
- Flex filters, static filters, and bypass in operation
- All flows forwarded but analyzed for anomalies

DETECTION

- Passive copy of traffic monitoring

LEARNING

- Periodic observation of patterns to automatically update baseline profiles

High Performance and Capacity

- 1 MPPS+ most attacks, good and bad traffic, typical features
- 150 K DYNAMIC FILTERS for zombie attacks
- CLUSTERING TO 8 GUARDS for single protected host
- Capacity

  30 CONCURRENTLY PROTECTED ZONES (90 for the Detector) and 500 total1.5 million concurrent connections

  1.5 million concurrent connections
- Latency or jitter: < 1 MSEC

Anomaly Recognition and Active Verification Features (cont.)

Anomaly Recognition:

- Extensive profiling of individual flows

  From individual src-IPs and src-nets to dst-IPs/ports by protocol

- Depth of profiles

  Packets, syns and requests, fragments as well as ratios

  Connections by status, authenication status and protocol specific data…

- Default normal baselines with auto-learning on site

  Baselines for typical as well as top sources and proxies

Anomaly Recognition and Active Verification Features (cont.)

Active Verification/Antispoofing:

- Broad application support

  TCP and UDP applications, including HTTP, HTTPS, SMTP, IRC, DNS and commercial and custom applications

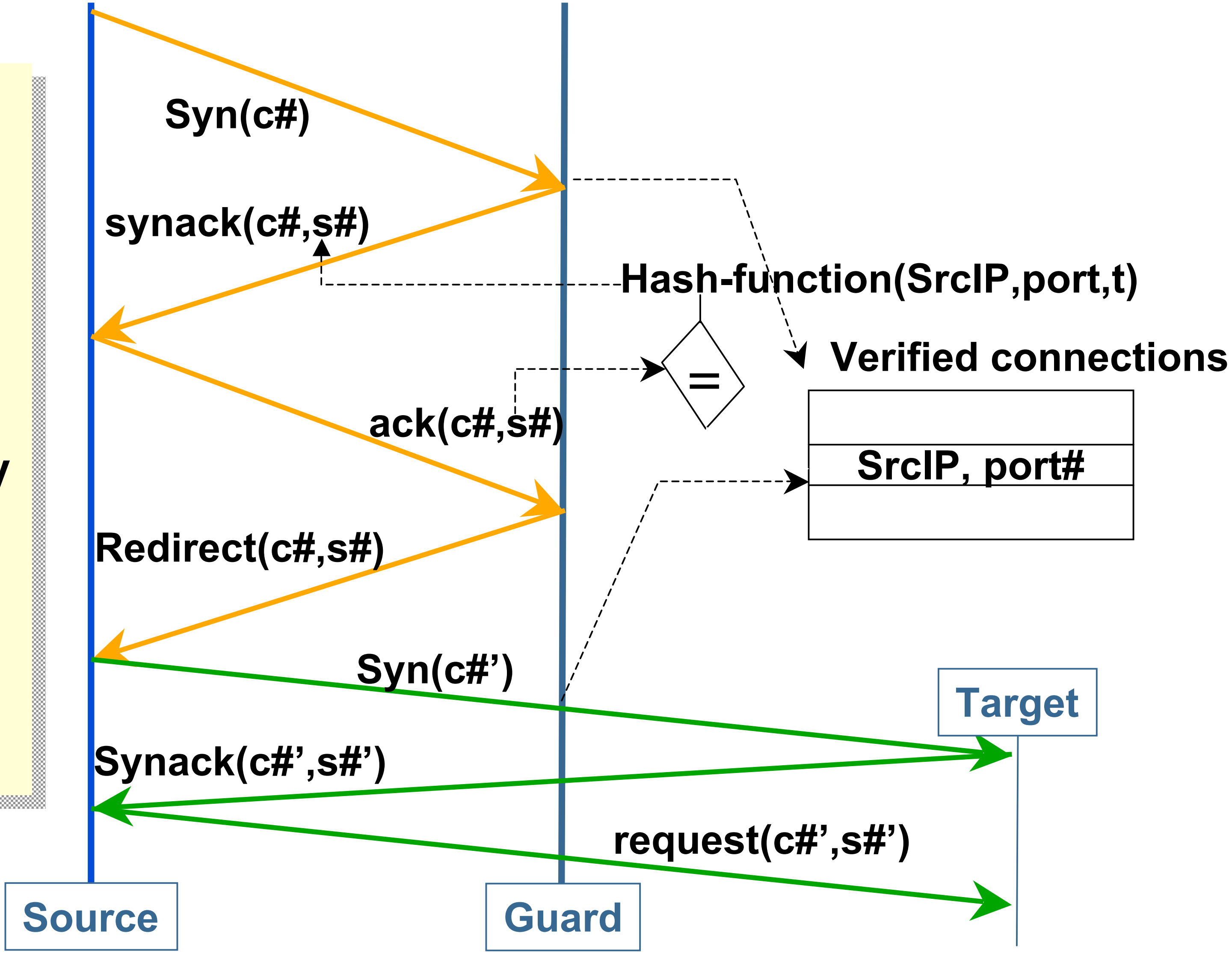
- Authenticates

  SYNs, SYNACKs, FINs, regular TCP packets, DNS requests and replies and more…

Antispoofing Defenses

Example: Basic Level for HTTP Protocol

- Antispoofing only when under attack
- Authenticate source on initial query
- State kept only for legitimate sources
- Subsequent queries verified



Broadest Attack Protection

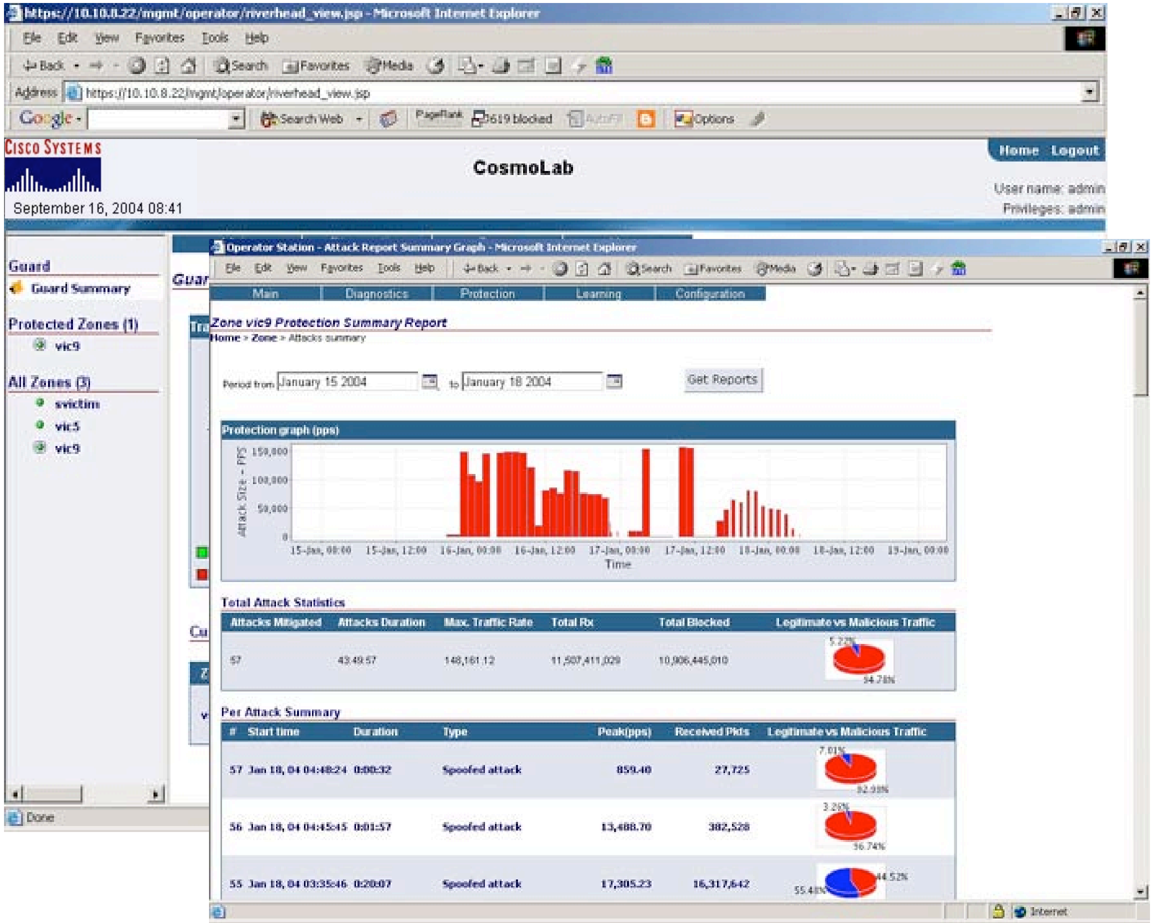
- **Random spoofed attacks (e.g., SYN)**
  - Removes spoofed flows that evade statistical identification
- **Focused spoofed of good source (e.g., AOL proxy)**
  - Distinguishes good vs. bad flows with same src-IP for selective blocking
- **Nonspoofed distributed attack**
  - Capacity for blocking high-volume, massive and morphing botnets of attackers that:
    - Penetrate SYN response defenses
    - Thwart any manual responses

Broadest Attack Protection (cont.)

- **Nonspoofed client attack (e.g., http half-open)**
  - **Identifies low-volume, protocol anomaly attacks that evade sampled flow data**

Management Features

- Console or SSH CLI
- Embedded device manager GUI
- DDoS SNMP MIB and traps
- Extensive syslogging
- Interactive recommendations
- Extensive reporting: GUI, CLI, and XML export by zone
- Packet capture and export
- TACACS+ for AAA
- Future CVDM for Cisco Cisco Catalyst® 6K support


https://10.10.8.22/mgmt/operator/riverhead_view.jsp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.10.8.22/mgmt/operator/riverhead_view.jsp
Google Search Web PageRank 619 blocked AutoFill Options
Home Logout
Guard
Guard Summary
Protected Zones (1)
vic9
All Zones (3)
svictim
vic5
vic9
Done
Operator Station - Attack Report Summary Graph - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Main
Diagnostics
Protection
Learning
Configuration
Get Reports
Protection graph (pps)
Attack Size - PPS
150,000
100,000
50,000
0
15-Jan, 00:00
15-Jan, 12:00
16-Jan, 00:00
16-Jan, 12:00
17-Jan, 00:00
17-Jan, 12:00
18-Jan, 00:00
18-Jan, 12:00
19-Jan, 00:00
Time
Internet

CosmoLab

September 16, 2004 08:41

User name: admin
Privileges: admin

Zone vic9 Protection Summary Report

Home > Zone > Attacks summary

Period from January 15 2004 to January 18 2004

Total Attack Statistics

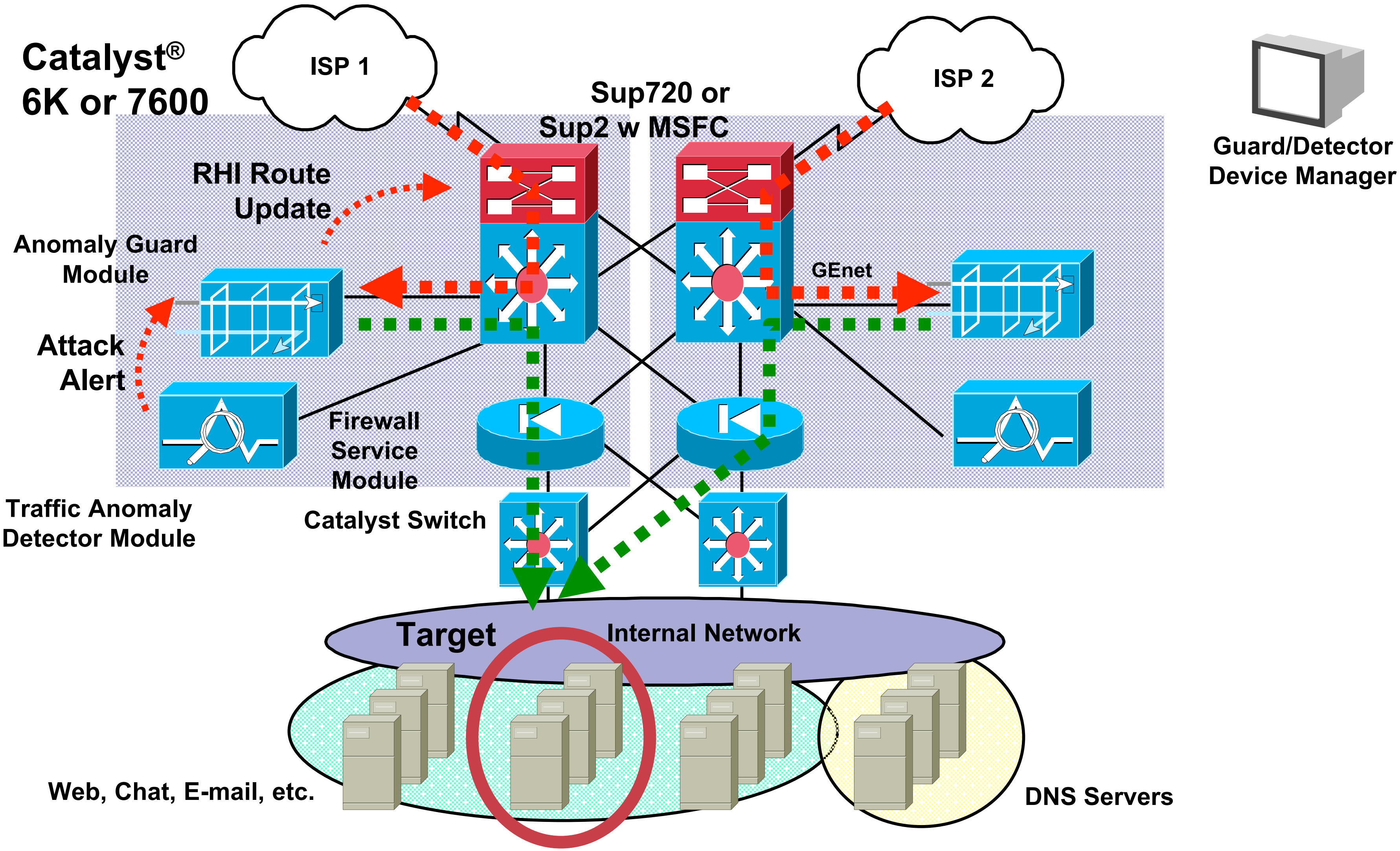
Attacks Mitigated	Attacks Duration	Max. Traffic Rate	Total Rx	Total Blocked	Legitimate vs Malicious Traffic
57	43:49:57	148,161.12	11,507,411,029	10,906,445,010	5.22% 94.78%

Per Attack Summary

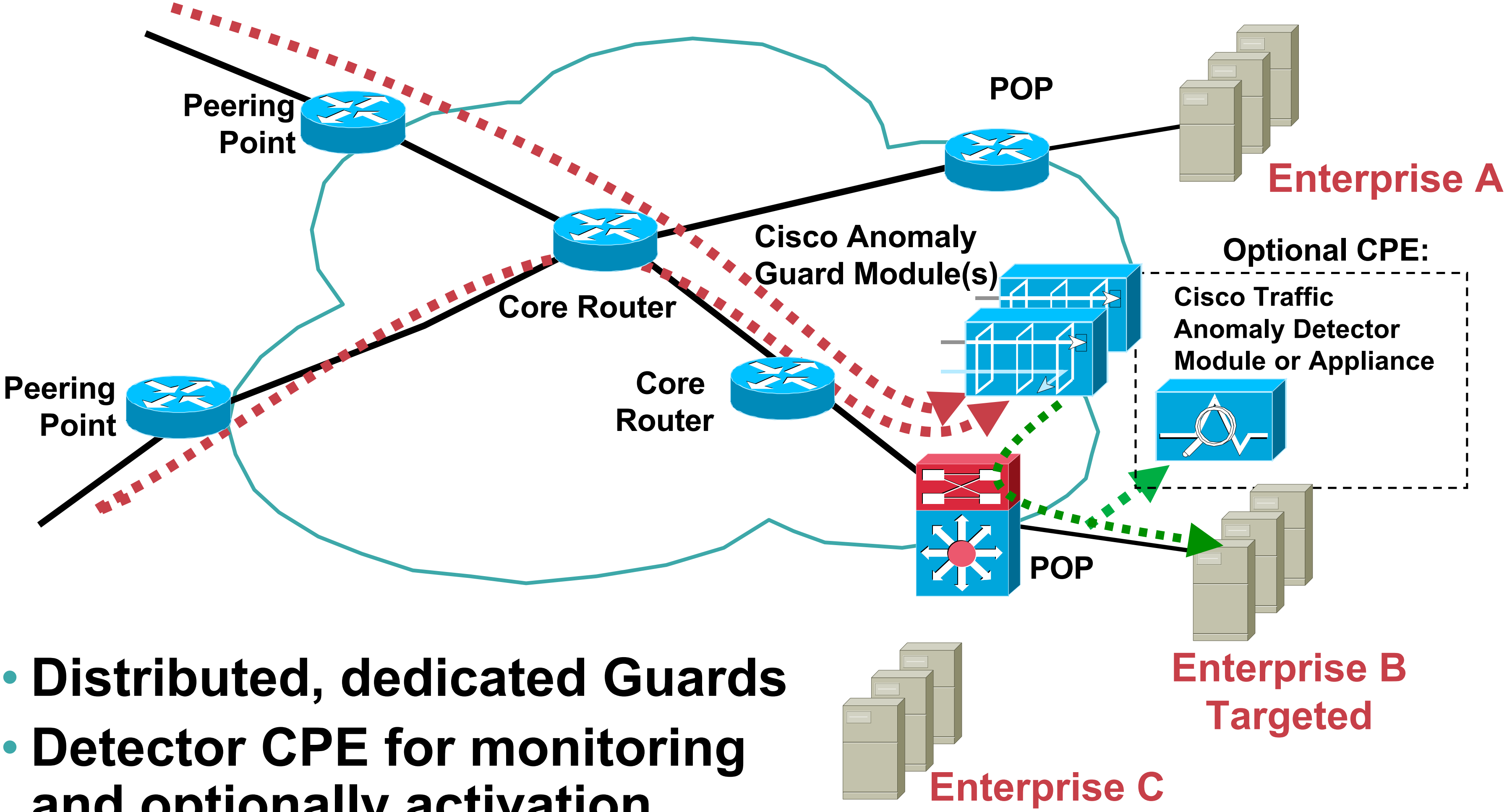
#	Start time	Duration	Type	Peak(pps)	Received Pkts	Legitimate vs Malicious Traffic
57	Jan 18, 04 04:48:24	0:00:32	Spoofed attack	859.40	27,725	7.01% 92.99%
56	Jan 18, 04 04:45:45	0:01:57	Spoofed attack	13,488.70	382,528	3.26% 96.74%
55	Jan 18, 04 03:35:46	0:20:07	Spoofed attack	17,305.23	16,317,642	44.52% 55.48%

DEPLOYMENT SCENARIOS

Hosting or Service Provider Data Center
with Service Modules in "Integrated Mode"



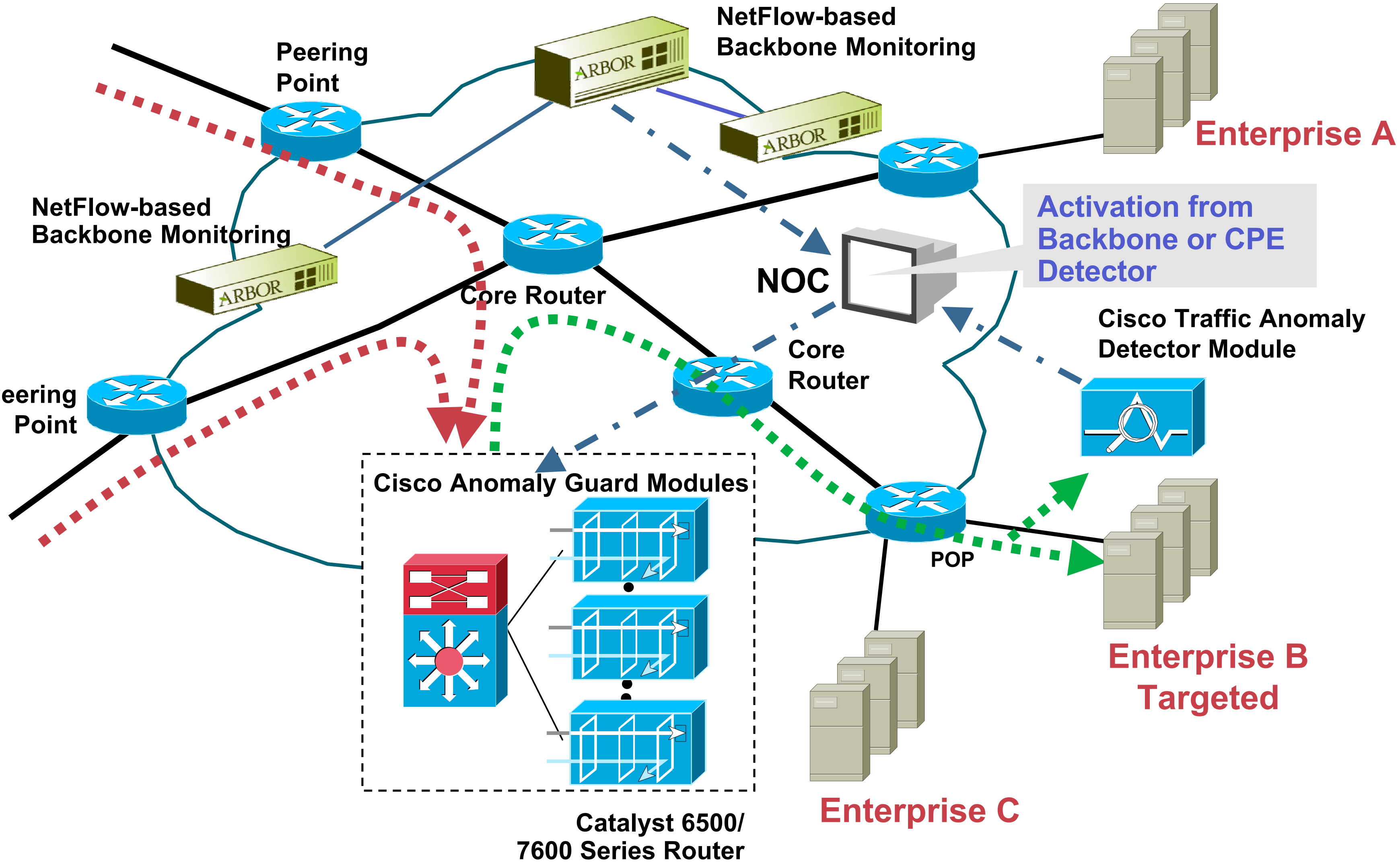
Service Provider
Distributed or Edge Protection



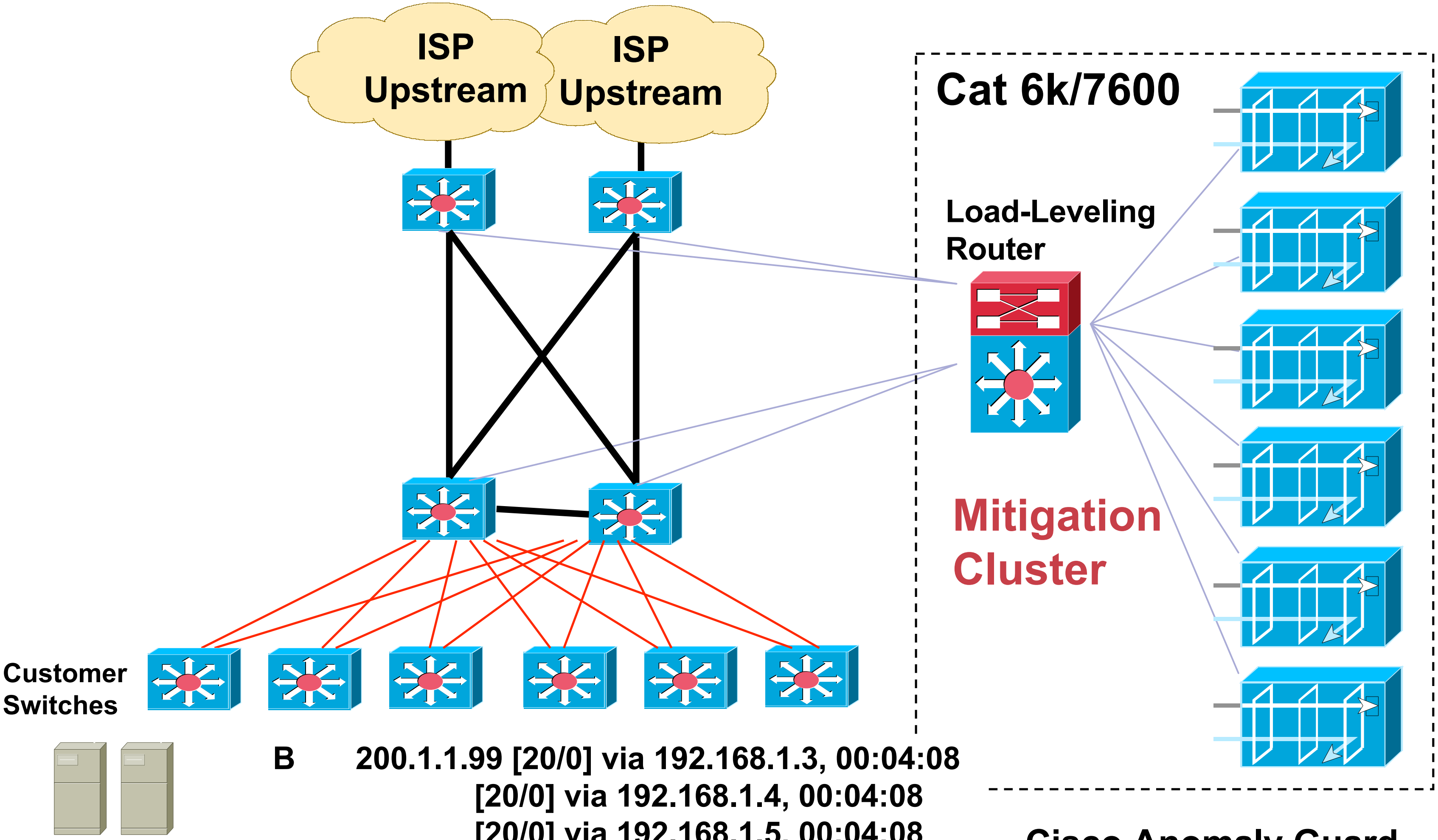
- Distributed, dedicated Guards
- Detector CPE for monitoring and optionally activation

Managed DDoS Service

Centralized Protection



Clustering Topology



```
B       200.1.1.99 [20/0] via 192.168.1.3, 00:04:08
                   [20/0] via 192.168.1.4, 00:04:08
                   [20/0] via 192.168.1.5, 00:04:08
                   [20/0] via 192.168.1.1, 00:04:08
                   [20/0] via 192.168.1.2, 00:04:08
```

200.1.1.99 = zone   192.168.1.1-5 = Guards

Cisco Anomaly Guard Modules

Clustering Topology (cont.)

Equal cost multipath routing

- Load levels traffic to a single destination IP
- Across up to 8 Guards per router
- CEF Layer 3 hash delivers consistent assignment per src-dst pair
- NO SPECIAL LOAD BALANCING SOLUTION REQUIRED
- Additional router provides functional partitioning

PROVIDER FEATURES AND BENEFITS

Solution Supports Critical Managed Service Requirements

- **Significant value-add**
  - Mitigation, not just detection
  - Broadest types of attacks
  - Accuracy and transparency
  - Automation for fast response
- **Proven competitive advantage => customer retention and acquisition**
  - Within hours of attacks that primary provider could not handle, enterprises shifted traffic to backup providers with Cisco DDoS
  - And when subsequently contracting for managed DDoS services, dropped providers that didn't offer
  - Commerical enterprises readily shift hosting providers based on DDoS capability
  - DDoS protection also on new vendor selection criteria

Solution Supports Critical Managed Service Requirements (cont.)

- Cost-effective operation
  - Defaults and templates for efficient provisioning
  - Automated learning for policy tuning
  - Automation for efficient attack response
  - Provider network deployment
  - On-demand scrubbing

Solution Supports Critical Managed Service Requirements (cont.)

- **Provider deployment architecture**

  Supports distributed and centralized deployment

  Dynamic diversion for ease of installation and high reliability

  High performance plus N+X clustering for redundancy, incremental scaling, and maintenance

  SNMP, XML, TACACS+, CLI, syslog for management

  Activation from and data export to third-party systems

- **Shared resources and virtualization supported**

  On-demand scrubbing

  Zone concept

Managed Services Momentum

Almost all available DDoS managed services are based on the Cisco Guard for mitigation:

AT&T — **DDoS Defense Option for Internet Protect managed services**

Sprint. — **IP Defender managed service**

rackspace™ MANAGED HOSTING — **PrevenTier DDoS Mitigation service**

DataPipe — **SureArmour DDoS protection service**

THE PLANET

CABLE & WIRELESS

WEBSITESOURCE your reliable hosting source

and many others

Positive Industry Response

"We are taking a very positive stance on AT&T's DDoS Defense option for its Internet Protect service…."

Current Analysis, June 2004

"This announcement is most important to Sprint customers. The service is attractive to customers that want to increase network uptime and avoid DoS attacks."

Gartner, October 2004

Provider Service Advantages

Managed Service at Provider	Enterprise Deployment at Data Center
Protects last-mile bandwidth and all enterprise infrastructure	Last-mile bandwidth and edge router not protected
Provider can protect against largest attacks	Can only defend against attacks that don’t exceed last-mile bandwidth
Provision and pay only for bandwidth for legitimate traffic	Must overprovision for largest potential attacks and/or pay burst charges
Upstream protection can cover multiple data centers	Must replicate protection at all data centers
DDoS protection can be efficiently offered as managed service	CPE infrastructure only protects locally and cannot be shared
Leverage focused security operations team	Difficult to maintain staff skill on DDoS attacks

CISCO SYSTEMS ®