**CISCO SYSTEMS**

# CISCO DDoS MITIGATION ENTERPRISE SOLUTIONS

**February 15, 2005**

# Integrated Security

## Foundation for Self-Defending Networks

### PRIVACY

**Secure Connectivity System**

**Secure transport of applications across numerous network environments**

### PROTECTION

**Threat Defense System**

**Collaboration of security and network intelligence services to minimize impact of both known and unknown**

### CONTROL

**Trust and Identity Management System**

**Contextual identity management for policy enforcement, network entitlement, and trust**
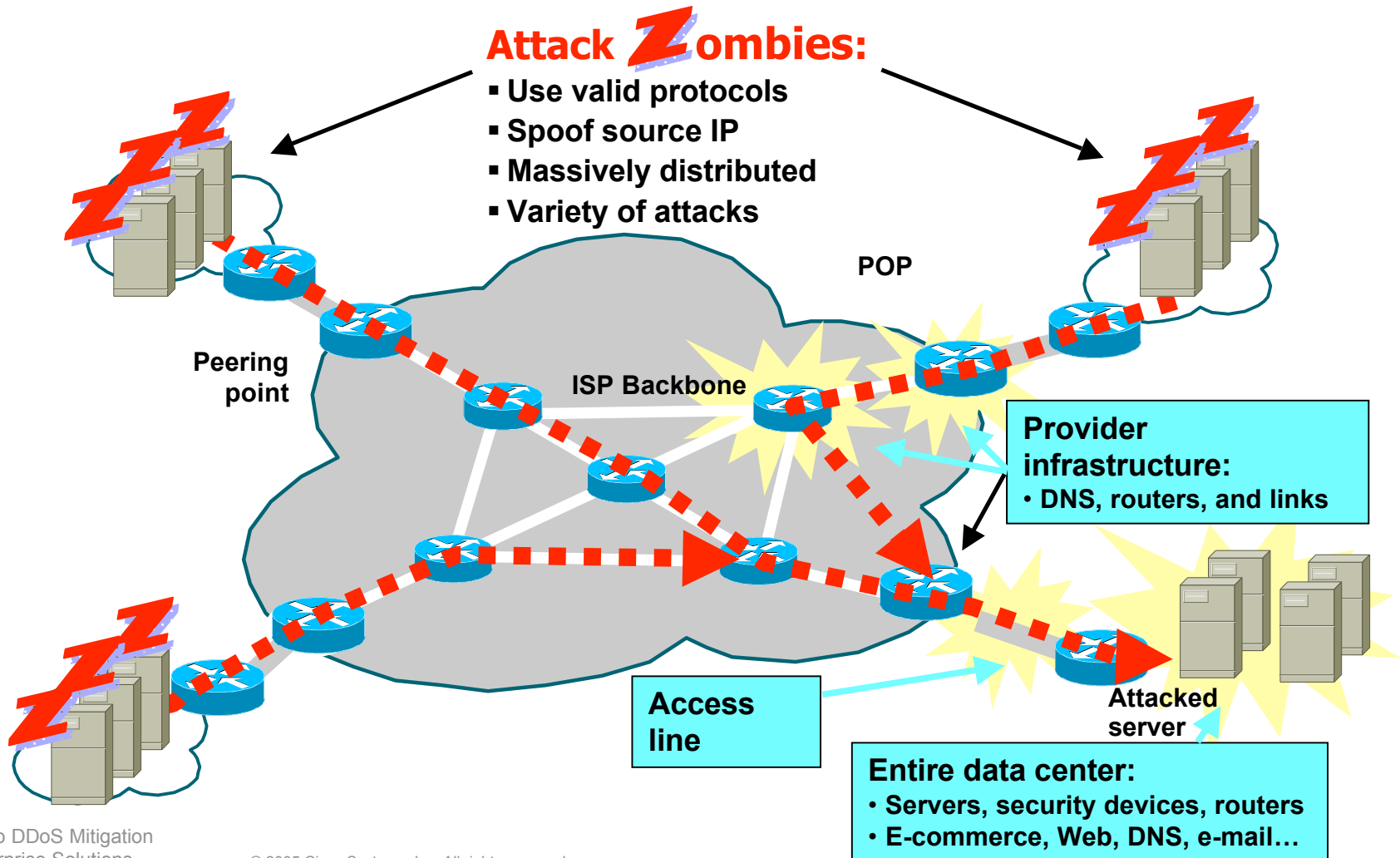
## Management and Analysis

# Executive Summary

- **Detects AND MITIGATES the broadest range of distributed denial of service (DDoS) attacks**

- **Has the granularity and accuracy to ENSURE BUSINESS CONTINUITY by forwarding legitimate transactions**

- **Delivers 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**
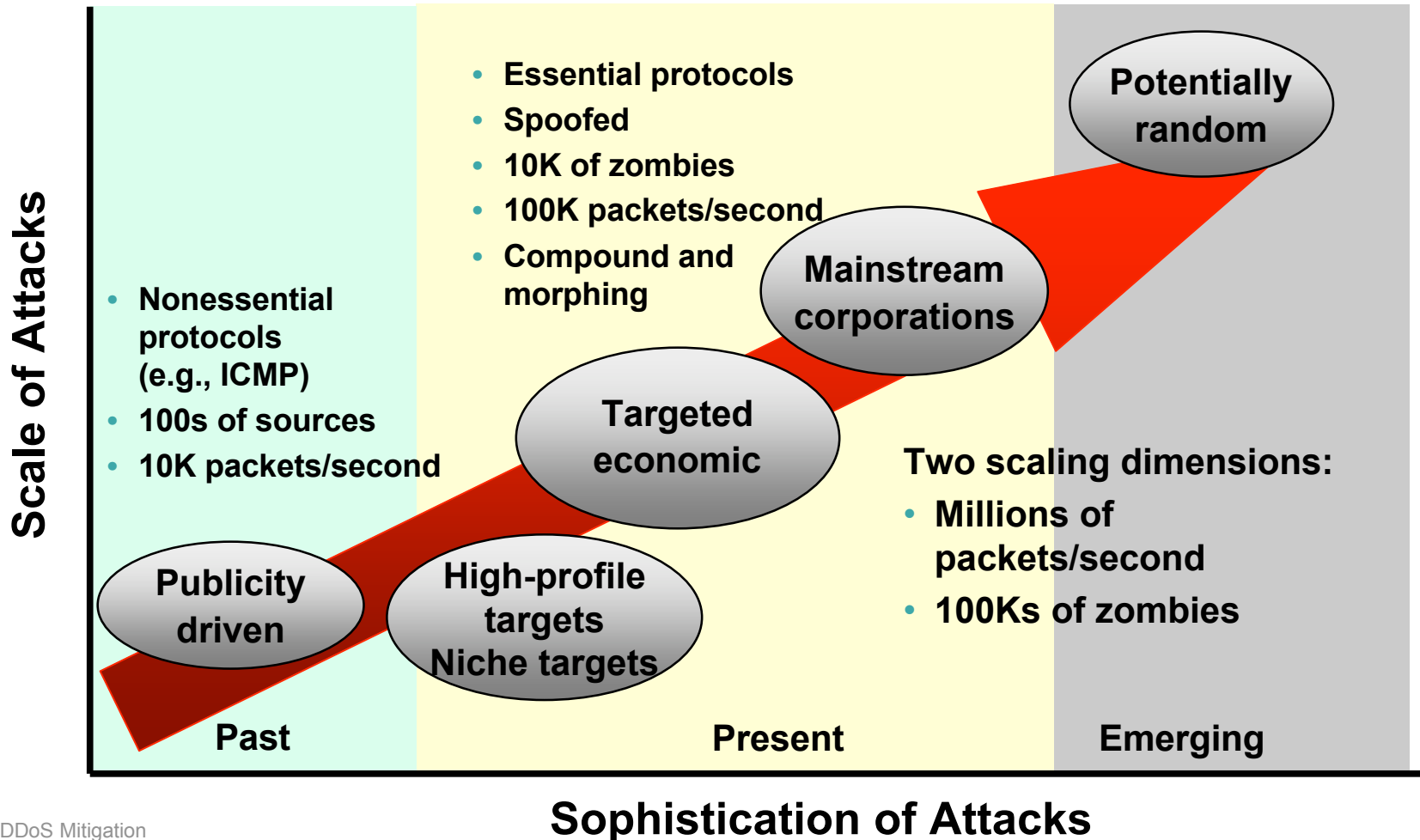
3

# DDoS Vulnerabilities

## Multiple Threats and Targets

**Attack Zombies:**
- **Use valid protocols**
- **Spoof source IP**
- **Massively distributed**
- **Variety of attacks**

**POP**

**Peering point**

**ISP Backbone**

**Provider infrastructure:**
- **DNS, routers, and links**

**Access line**

**Attacked server**

**Entire data center:**
- **Servers, security devices, routers**
- **E-commerce, Web, DNS, e-mail…**
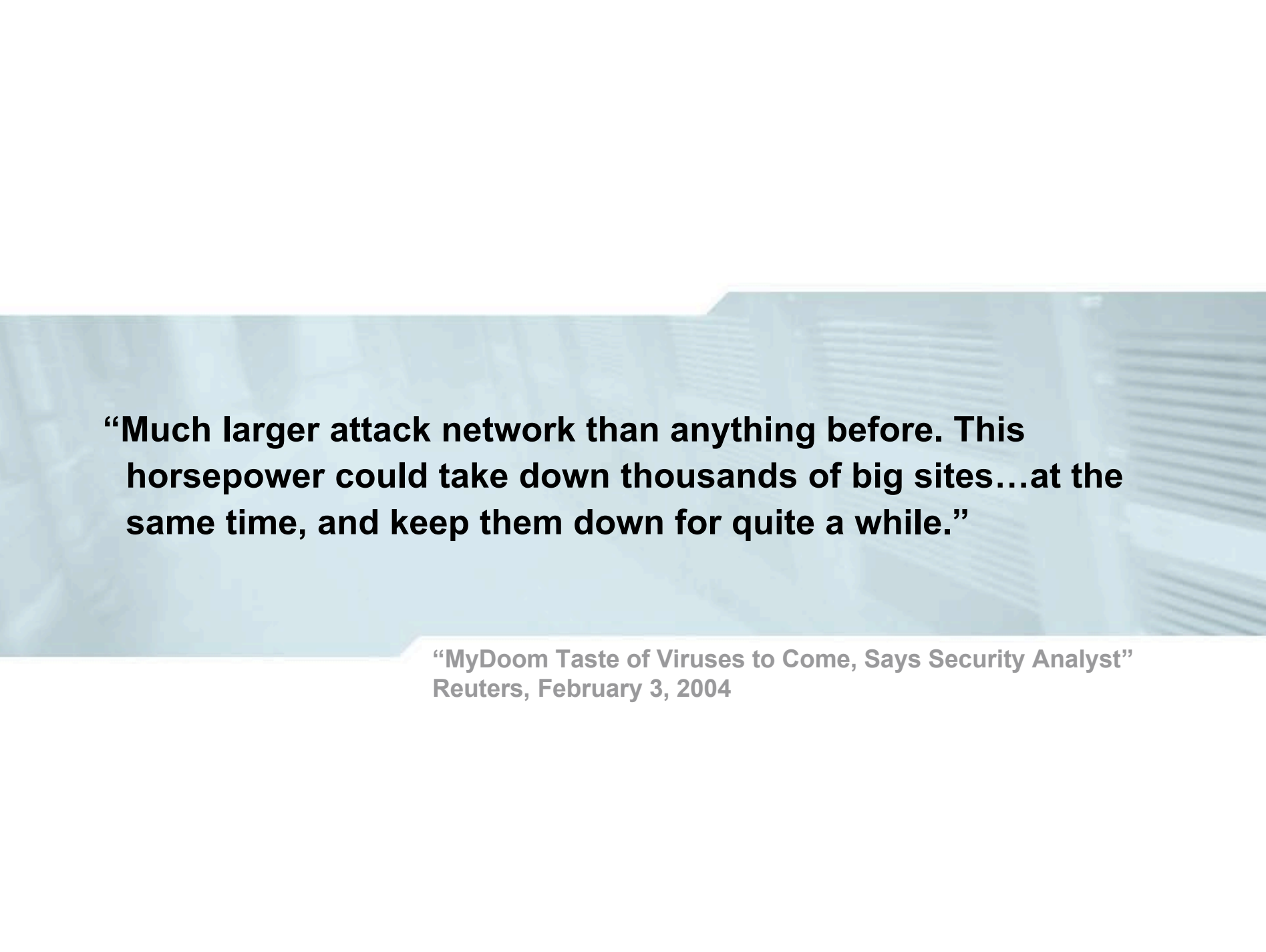
# THE DDoS PROBLEM

# Attack Evolution

## Stronger and More Widespread

**Scale of Attacks** (vertical axis)

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

**Potentially random**

**Mainstream corporations**

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

**Targeted economic**

**Two scaling dimensions:**
- **Millions of packets/second**
- **100Ks of zombies**

**Publicity driven**

**High-profile targets Niche targets**

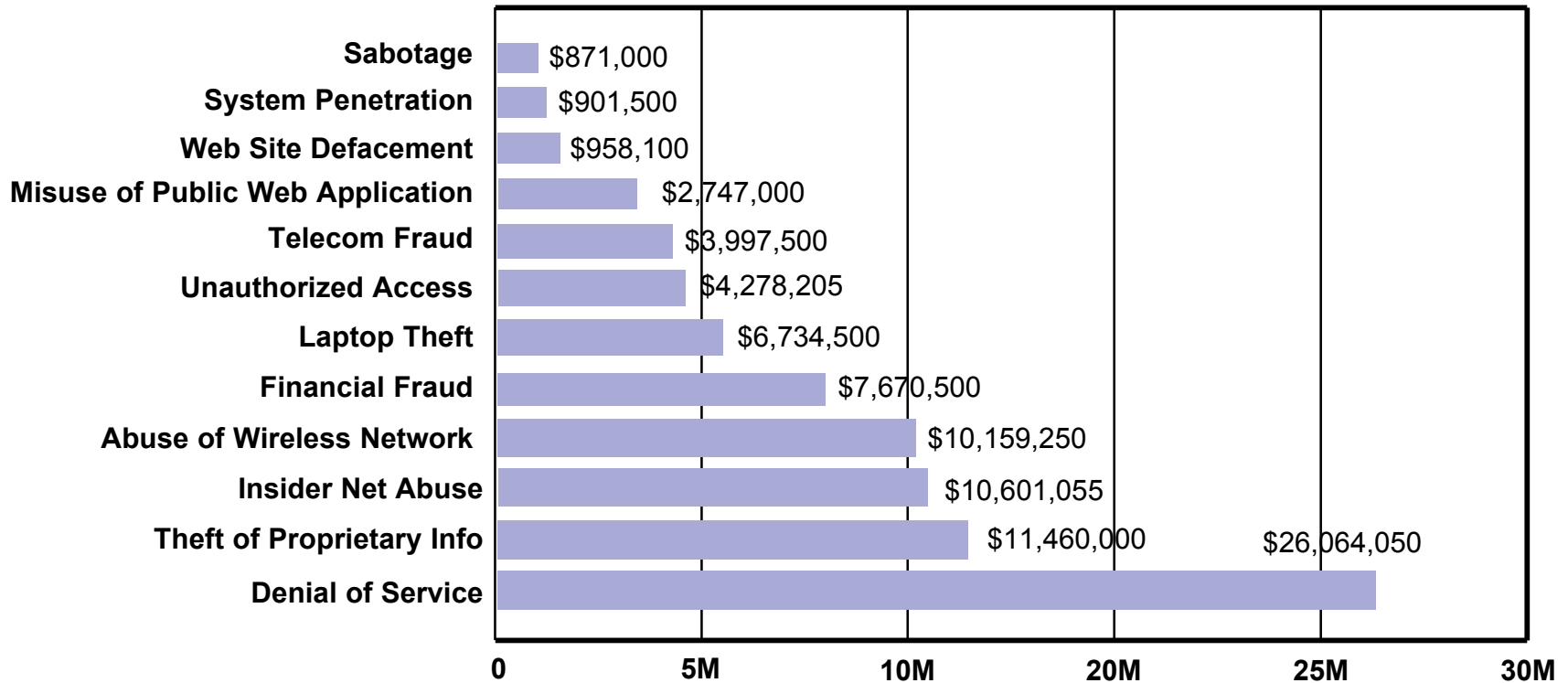**Past** | **Present** | **Emerging**

**Sophistication of Attacks**

**"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)

| Type of Attack | Amount |
|---|---|
| Sabotage | $871,000 |
| System Penetration | $901,500 |
| Web Site Defacement | $958,100 |
| Misuse of Public Web Application | $2,747,000 |
| Telecom Fraud | $3,997,500 |
| Unauthorized Access | $4,278,205 |
| Laptop Theft | $6,734,500 |
| Financial Fraud | $7,670,500 |
| Abuse of Wireless Network | $10,159,250 |
| Insider Net Abuse | $10,601,055 |
| Theft of Proprietary Info | $11,460,000 |
| Denial of Service | $26,064,050 |

X-axis: 0    5M    10M    20M    25M    30M

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 MEDIA

REVIEWS · OPINIONS · TOPICS · INDUSTRIES · RESEARCH · TOOLS · WHITE PAPER

SEARCH [ ] eWEEK

### Security

## DDoS Attack Knocks Out DoubleClick Ads

By Matt Hicks

July 27, 2004

**TalkBack:** Sound off on this article

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.

**RELATED LINKS**

▶ 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**

# The Register

## 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 Solution
# Completes Security in Depth

**AVAILABILITY**

**Authenticated Access**

**Data Integrity**
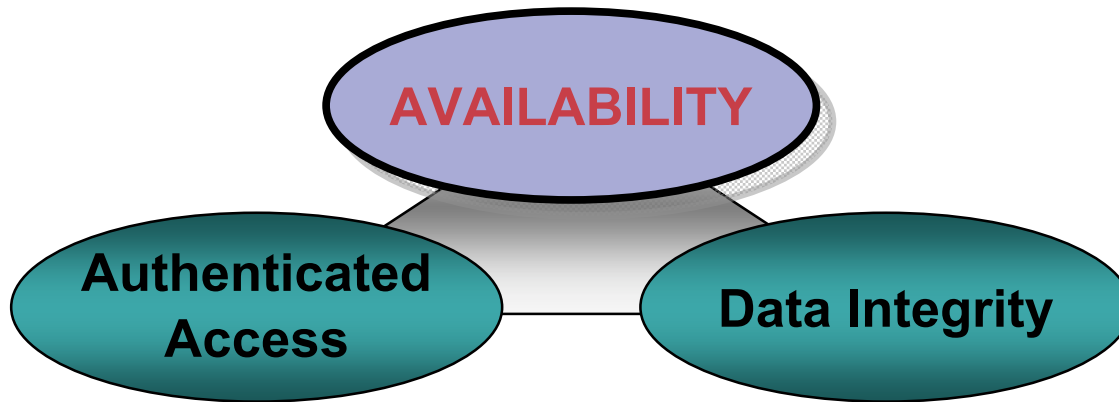
- **Addresses need to "secure availability" of infrastructure**

  Network behavior-based solution required to stop DDoS

  Does not use attack signatures—catches day-zero attacks

- **Complements and strengthens overall security solution**

  Firewall, IPS, SSL, and antivirus as well as content switching

  Efficient sequential elimination of different levels of threats

# DDoS Protection
# Cisco Service Modules

## 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**

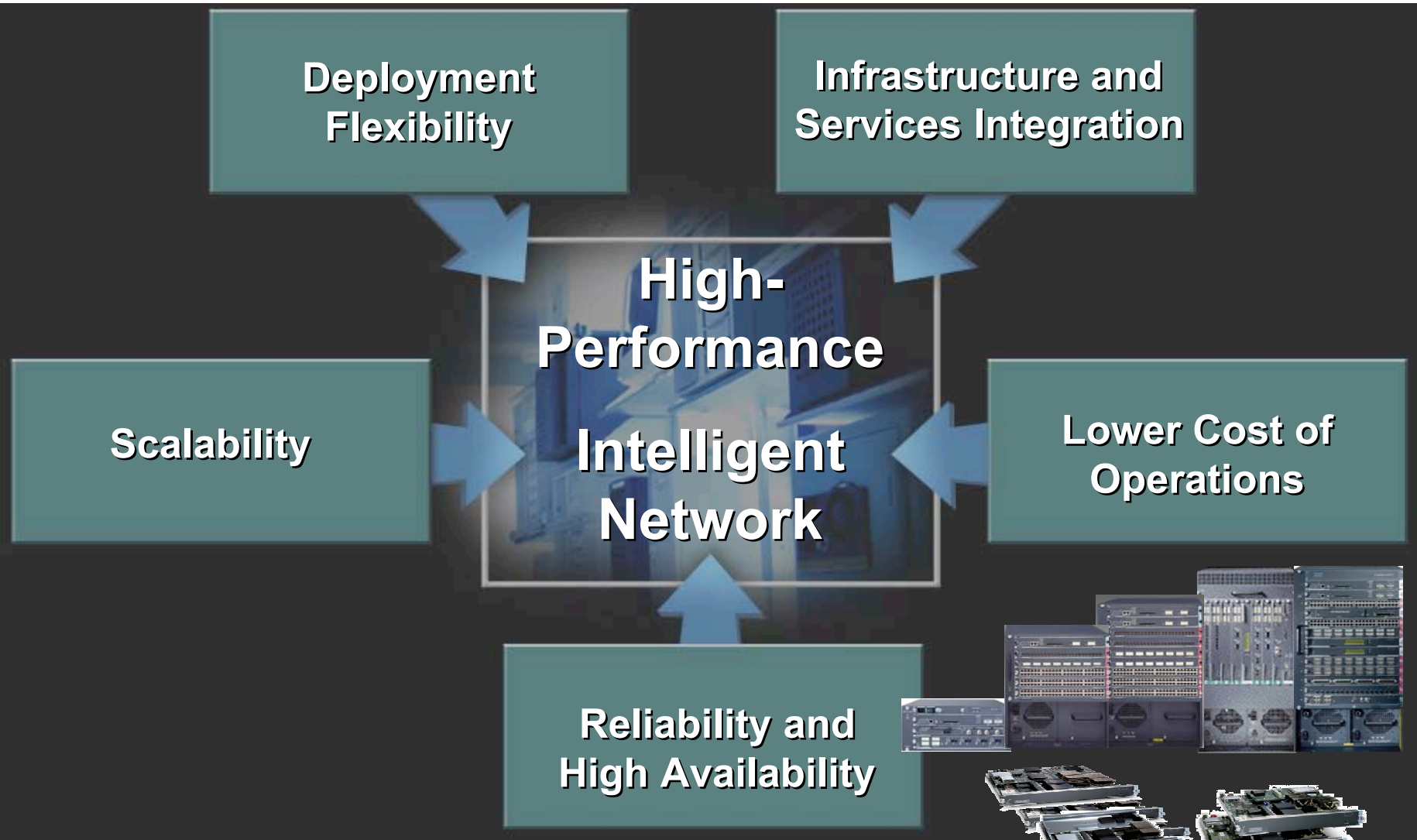**Cisco Traffic Anomaly
Detector Module**

# 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**

**Scalability**

**High-Performance**

**Intelligent Network**

**Lower Cost of Operations**

**Reliability and High Availability**

# Layer 4–7 Services Modules Family

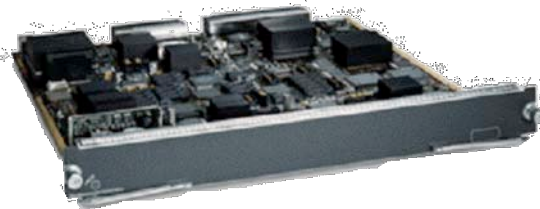**NAM-1 and NAM-2 Module**

**Firewall Module**

**IDSM-2 Module**

**CSM  Module**

**VPN Module**

**SSL Module**

**Cisco Anomaly Guard Module**

**Cisco Traffic Anomaly Detector Module**

# Flexible Deployment Options

Cisco.com

**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**

Guard Module
Detector Module

Cisco DDoS Mitigation
Enterprise Solutions

© 2005 Cisco Systems, Inc. All rights reserved.

18
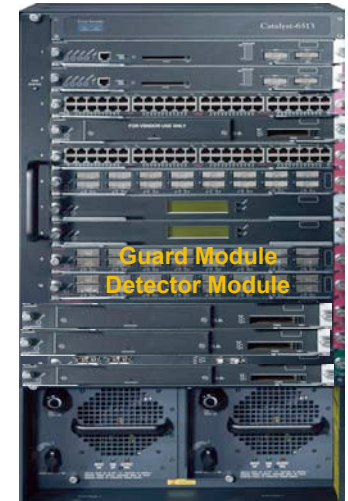
# Flexible Deployment Options (cont.)

**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**


Anomaly Guard Modules

# 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**

# Dynamic Diversion At Work

Cisco.com

**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**

27

# Dynamic Diversion At Work

**4. Identify and filter malicious traffic**

**3. Divert only target's traffic**

**6. Non-targeted traffic flows freely**

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**

# Cisco Catalyst Service Module

## Solution Overview

**Dynamic route diversion**

Line Card Module

**Anomaly Guard Module**

Switch Fabric

Supervisor Engine 2 or 720

**Alert**

Firewall Service Module

**Traffic Anomaly Detector Module**

Line Card Module

**Cat6K/7600**

Internal Network

# 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**

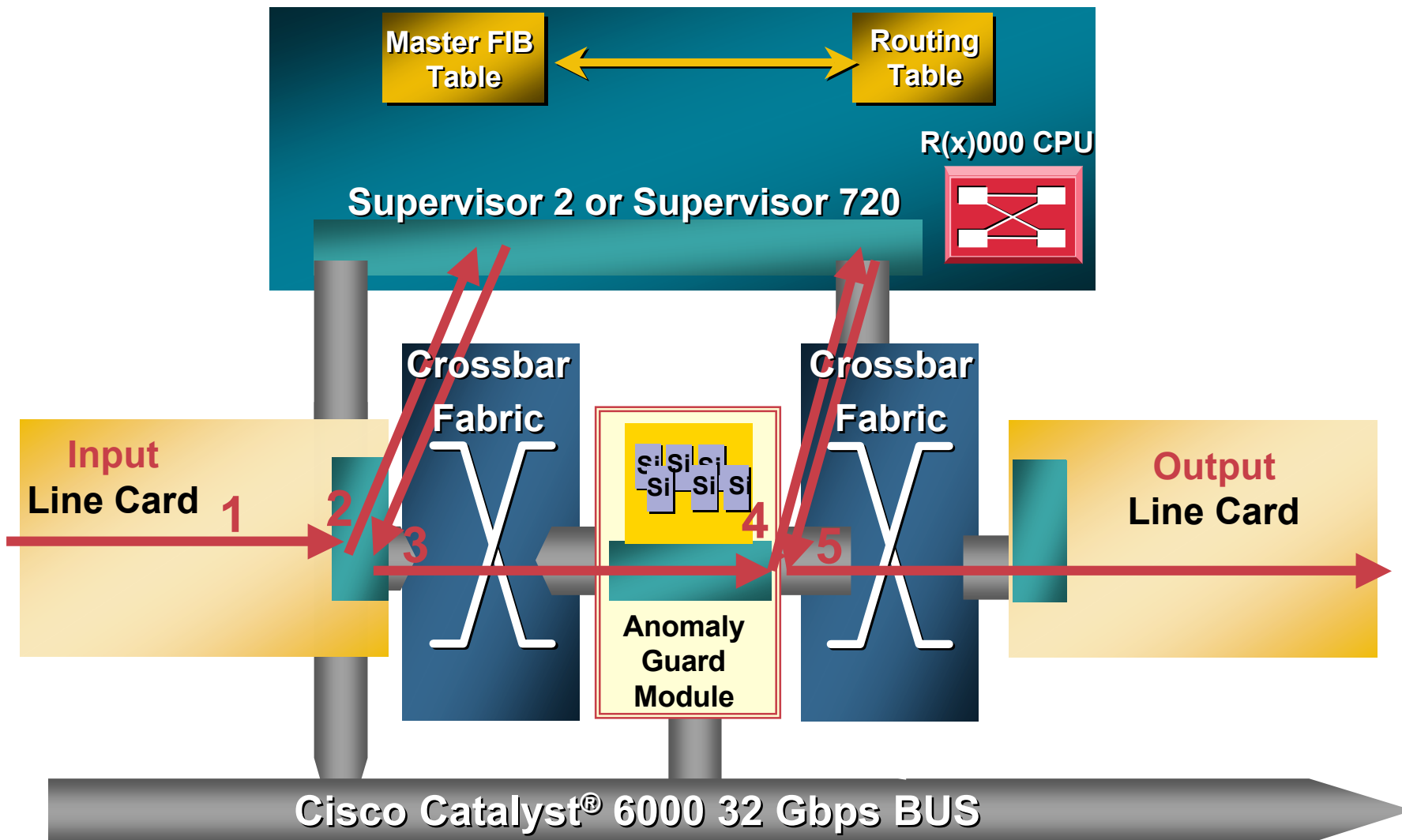  - **Supervisor redistributes route update**

- **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**

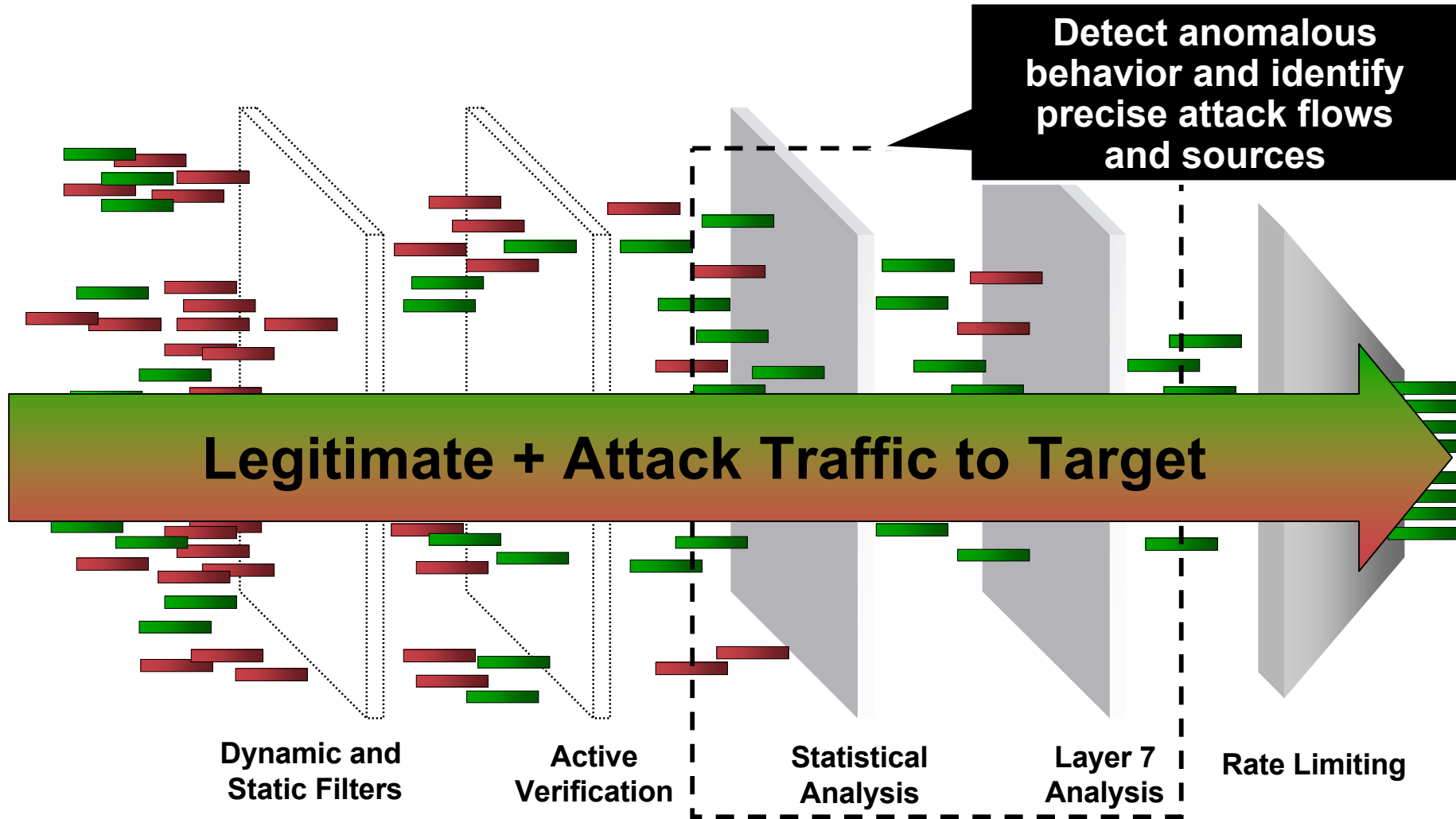# Anomaly Guard Module Packet Flow
## Supervisor 2/SFM or Supervisor 720

# MULTISTAGE VERIFICATION PROCESS

# Multiverification Process (MVP)
## Integrated Defenses in the Guard

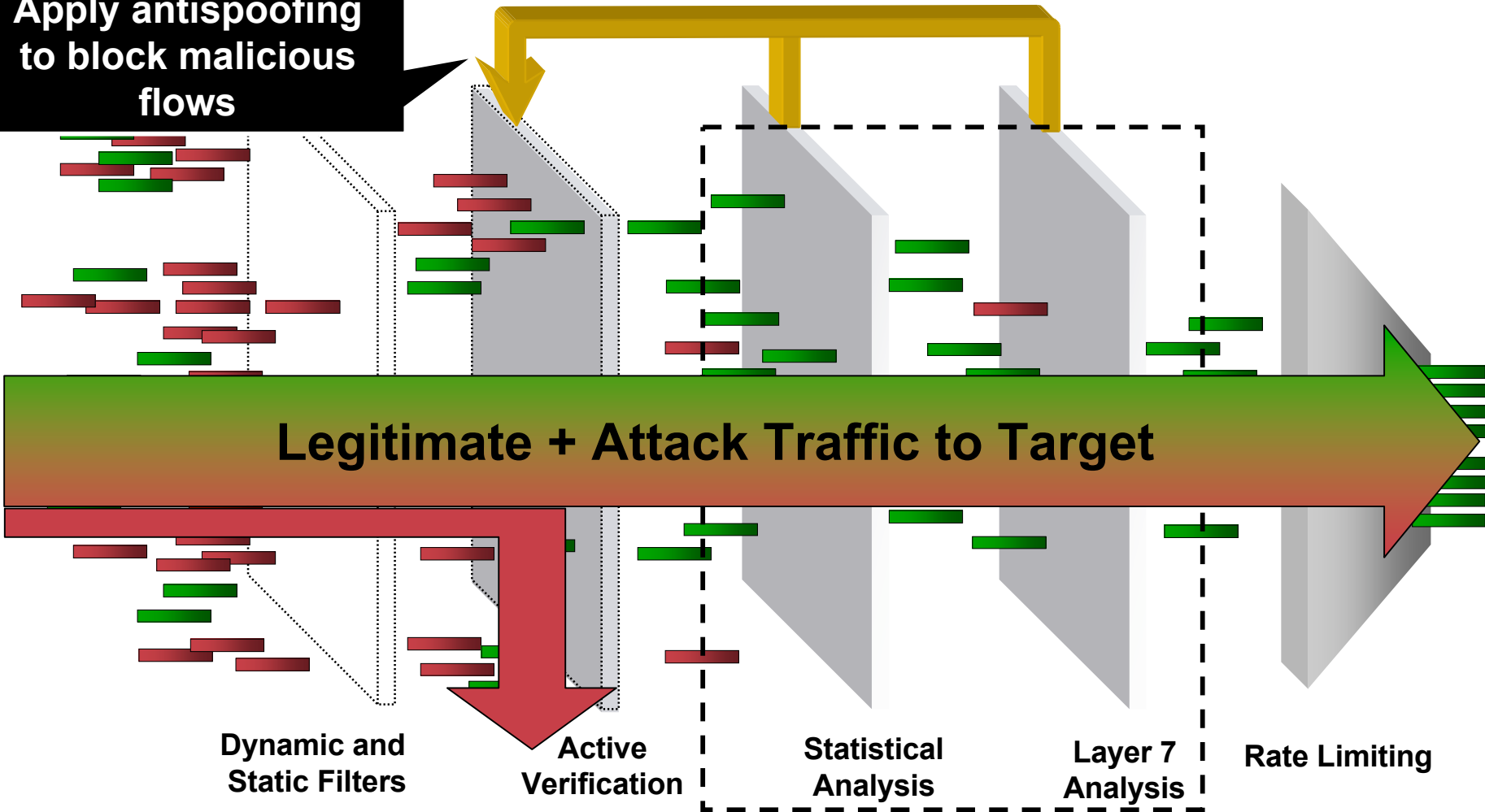**Detect anomalous behavior and identify precise attack flows and sources**

**Legitimate + Attack Traffic to Target**

| Dynamic and Static Filters | Active Verification | Statistical Analysis | Layer 7 Analysis | Rate Limiting |
|---|---|---|---|---|

# Multi-Verification 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

# Multi-Verification Process (MVP)
## Integrated Defenses in the Guard

**Dynamically insert specific filters to block attack flows and sources**

**Apply rate limits**

**Legitimate Traffic**

**Dynamic and Static Filters**

**Active Verification**

**Statistical Analysis**

**Layer 7 Analysis**

**Rate Limiting**
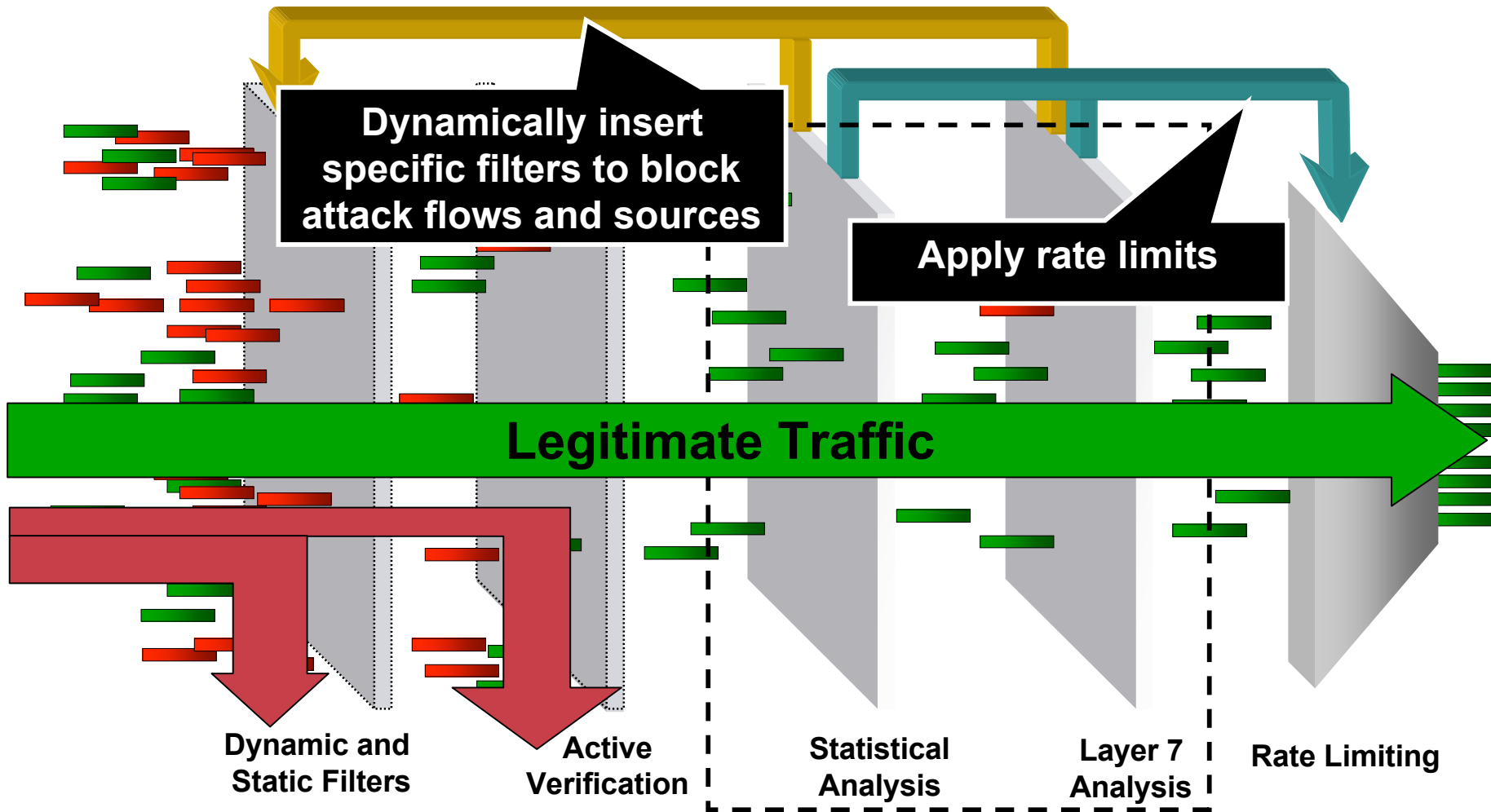
# Intelligent Countermeasures

**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**

**Anomaly Sources Identified**

**Anomaly Verified**

**Attack Detected**

# 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

## 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
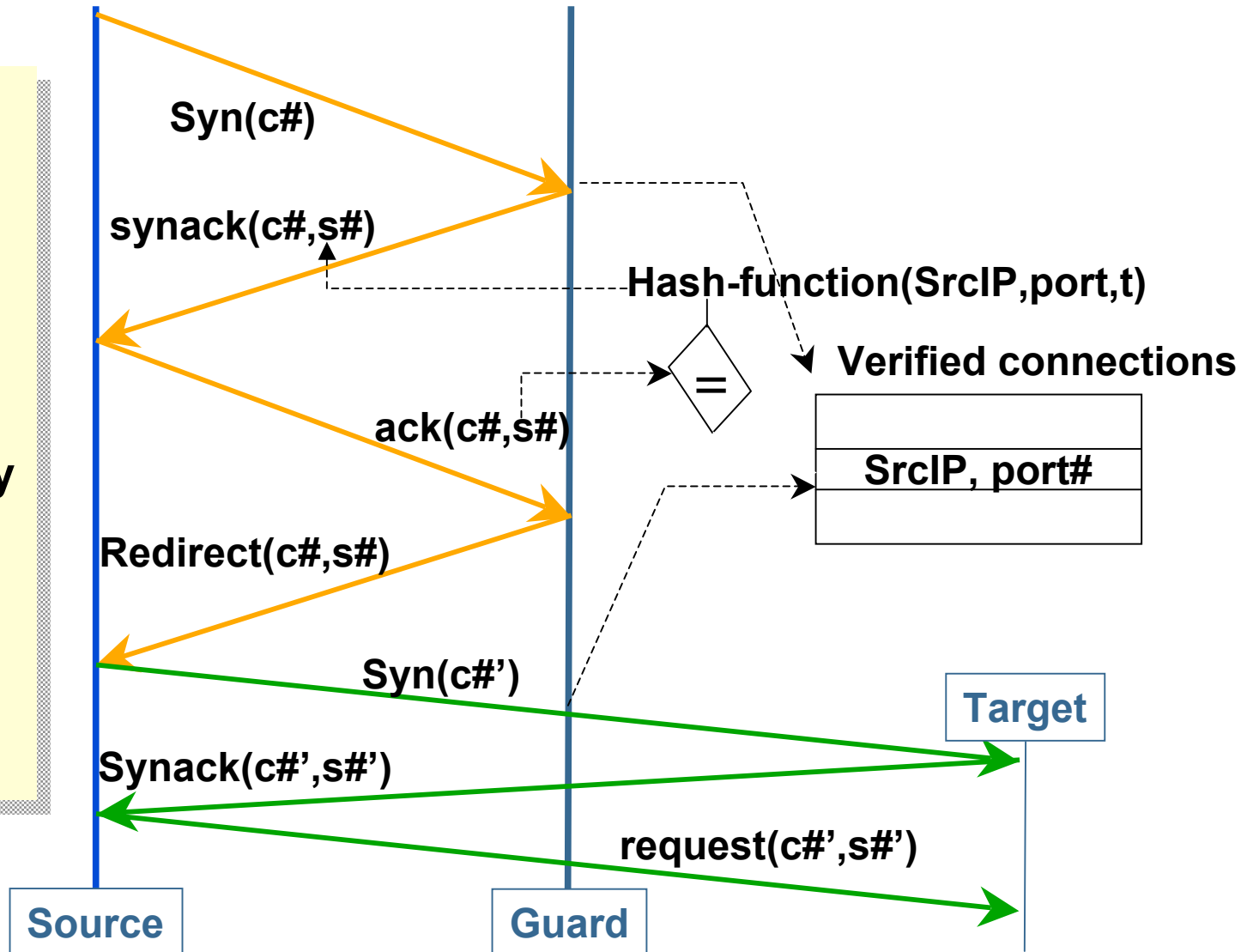
- **Authenticates**

  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**

**Syn(c#)**

**synack(c#,s#)**

**Hash-function(SrcIP,port,t)**

**=**

**Verified connections**

**SrcIP, port#**

**ack(c#,s#)**

**Redirect(c#,s#)**

**Syn(c#')**

**Target**

**Synack(c#',s#')**

**request(c#',s#')**

**Source**

**Guard**

40

# 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**
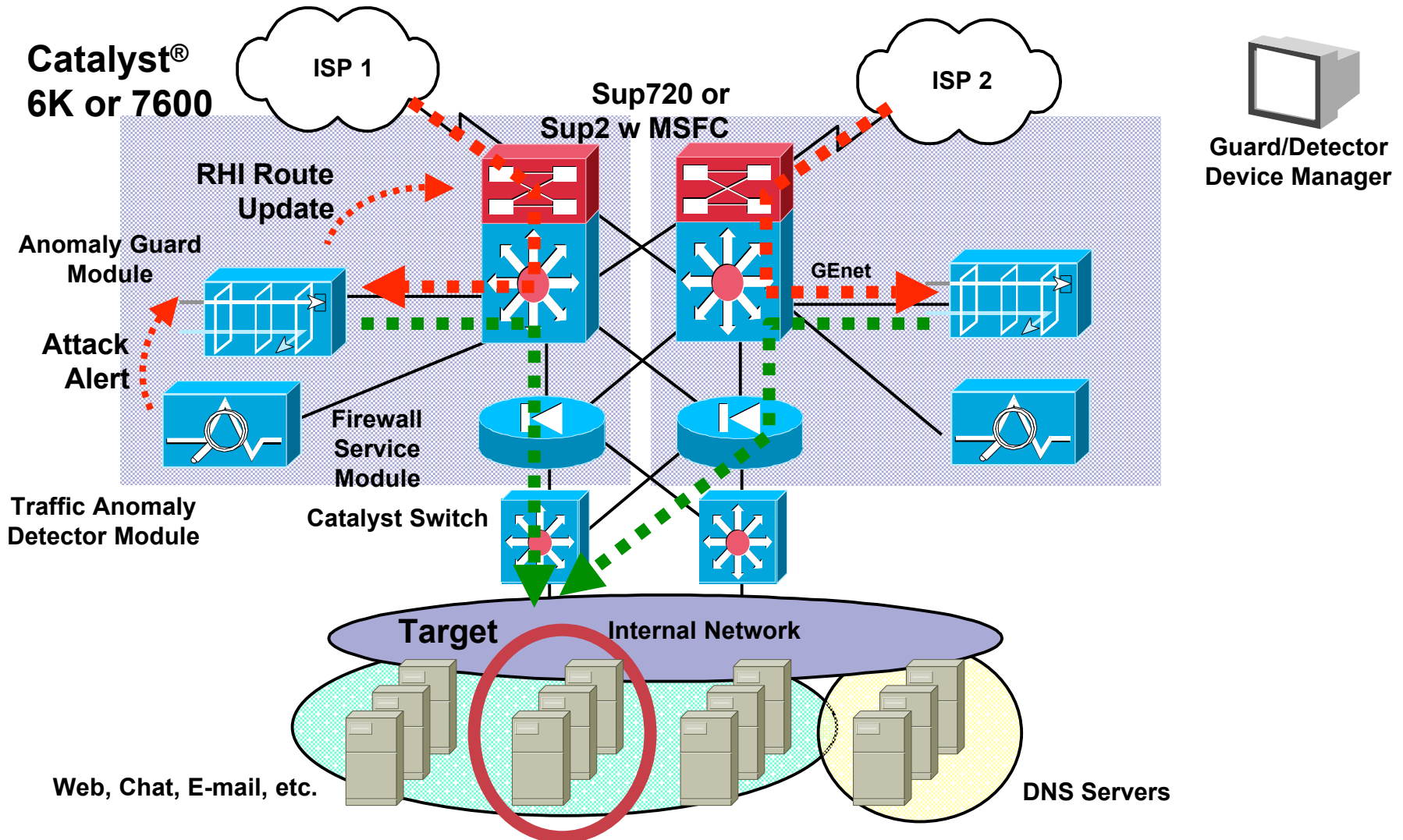
# Management Features

- **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**

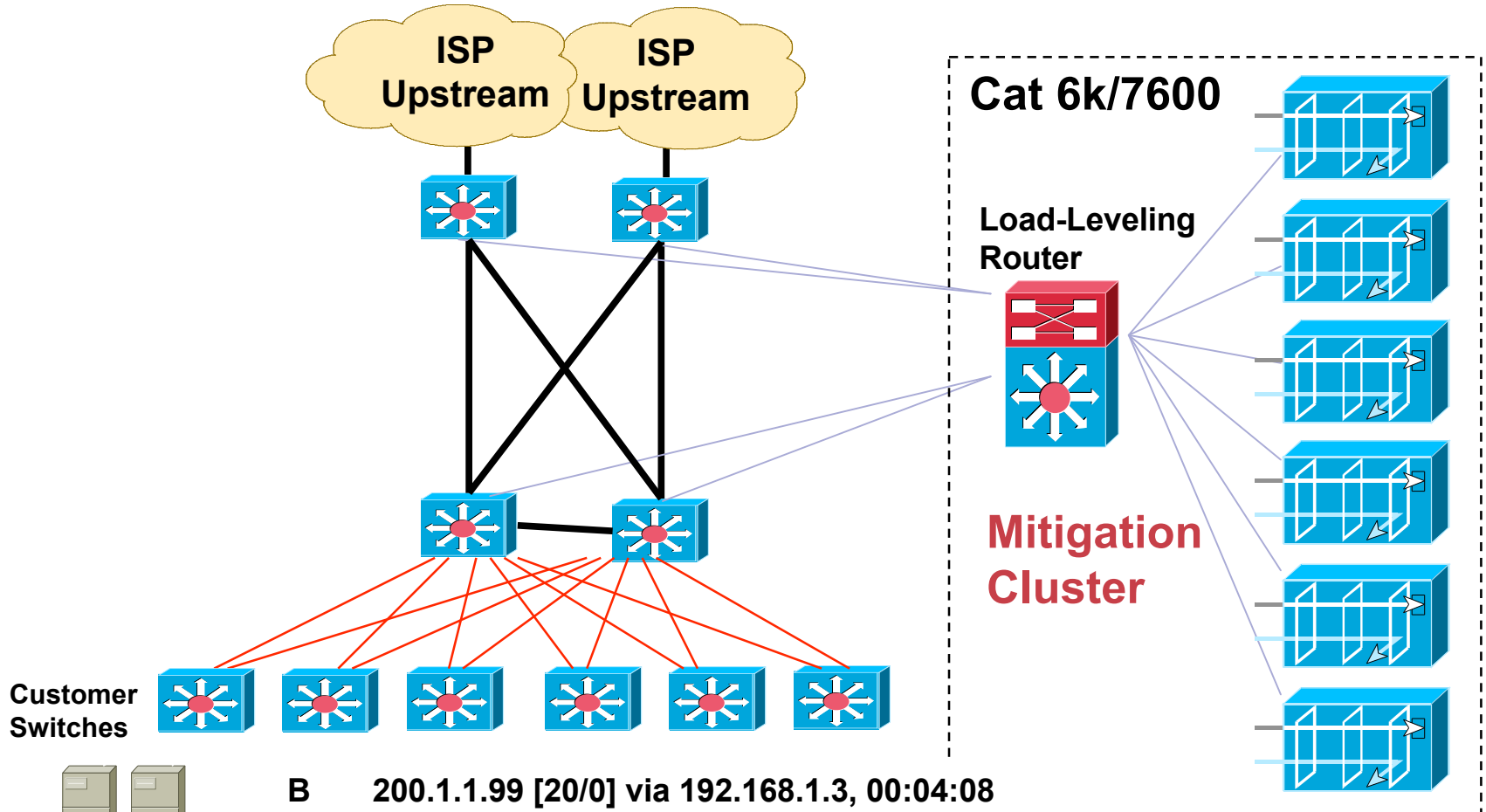- **Future CVDM for Cisco Catalyst® 6K support**
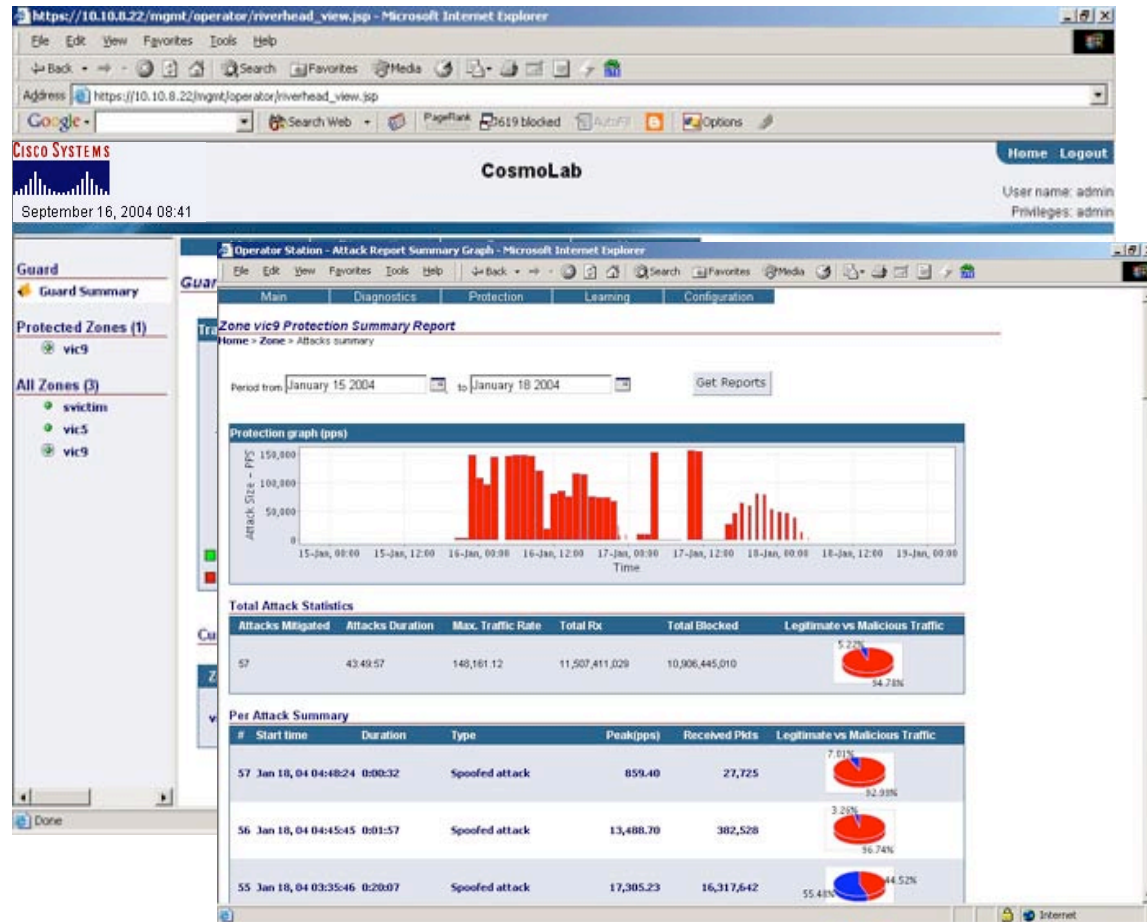
# DEPLOYMENT SCENARIOS

# Enterprise or Hosting Data Center
## with Service Modules in "Integrated Mode"

Catalyst® 6K or 7600

ISP 1

Sup720 or Sup2 w MSFC

ISP 2

Guard/Detector Device Manager

RHI Route Update

Anomaly Guard Module

GEnet

Attack Alert

Traffic Anomaly Detector Module

Firewall Service Module

Catalyst Switch

Target

Internal Network

Web, Chat, E-mail, etc.

DNS Servers

# Clustering Topology

ISP Upstream

ISP Upstream

Cat 6k/7600

Load-Leveling Router

Mitigation Cluster

Customer Switches

**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**
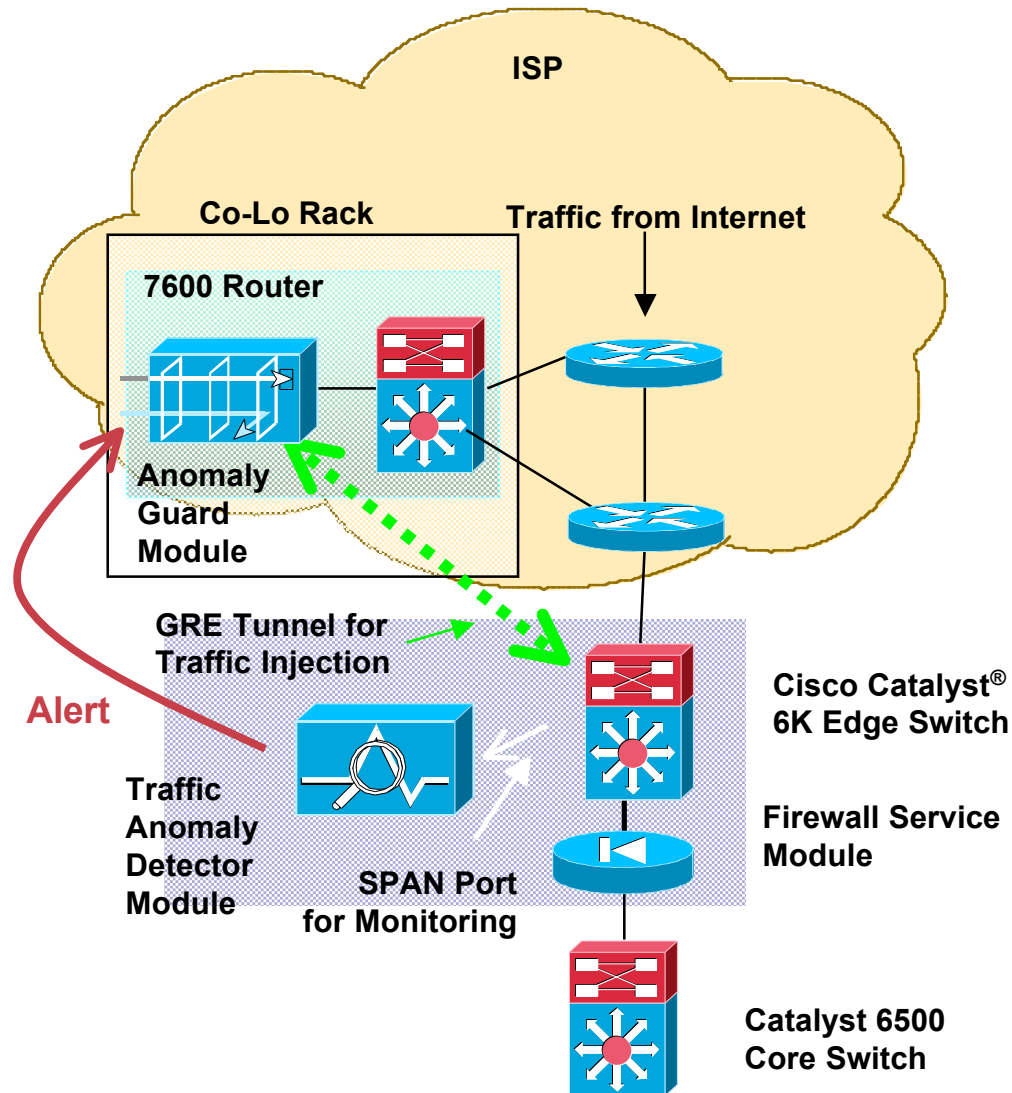**200.1.1.99 = zone   192.168.1.1-5 = Guards**

**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**

# Enterprise Deployment
## Provider Edge via Colocation

ISP

Co-Lo Rack

Traffic from Internet

7600 Router

Anomaly Guard Module

GRE Tunnel for Traffic Injection

Alert

Traffic Anomaly Detector Module

SPAN Port for Monitoring

Cisco Catalyst® 6K Edge Switch

Firewall Service Module
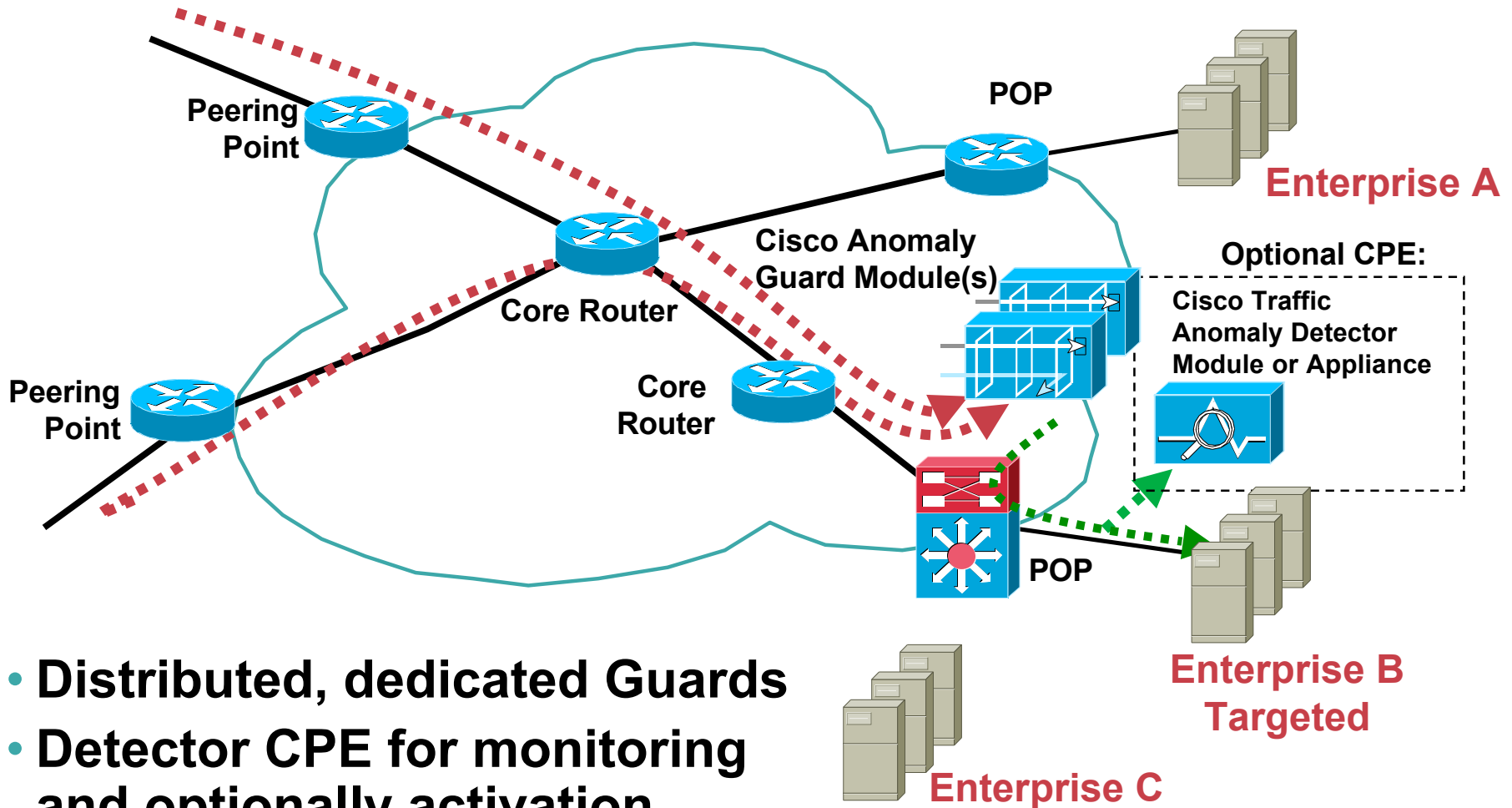
Catalyst 6500 Core Switch

# Enterprise Deployment
## Provider Edge via Colocation (cont.)

- **Enterprise-controlled, but upstream mitigation protects link and enterprise-edge router**

- **Enterprise-located Detector activates the Guard via separate management circuit**

- **Additional router isolates routing updates to enterprise-owned devices**

- **GRE tunnel is configured from Guard to enterprise edge router for traffic injection**

- **Managed service alternative saves bandwidth costs for carrying attack traffic**
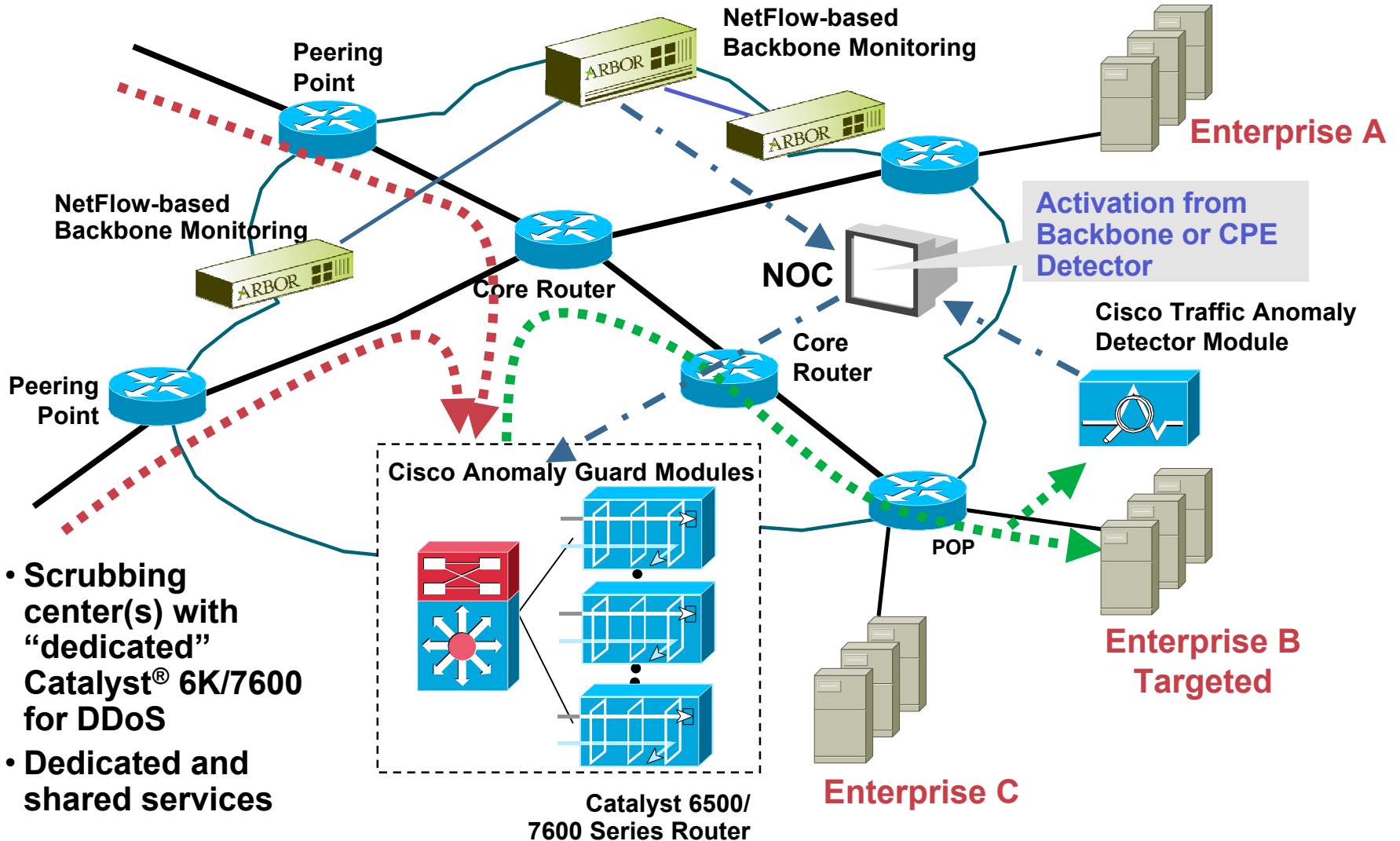
# Managed DDoS Service
## Provider Edge Protection

Peering Point

POP

Enterprise A

Cisco Anomaly Guard Module(s)

Optional CPE:

Cisco Traffic Anomaly Detector Module or Appliance

Core Router

Peering Point

Core Router

POP

Enterprise B Targeted

Enterprise C

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

# Managed DDoS Service
## Centralized Protection

**Peering Point**

**NetFlow-based Backbone Monitoring**

ARBOR

ARBOR

**Enterprise A**

**NetFlow-based Backbone Monitoring**

ARBOR

**Core Router**

**NOC**

**Activation from Backbone or CPE Detector**

**Peering Point**

**Core Router**

**Cisco Traffic Anomaly Detector Module**

**Cisco Anomaly Guard Modules**

**POP**

- **Scrubbing center(s) with "dedicated" Catalyst® 6K/7600 for DDoS**
- **Dedicated and shared services**

**Catalyst 6500/ 7600 Series Router**

**Enterprise B Targeted**

**Enterprise C**

# MANAGED DDoS SERVICE

# Managed DDoS Services Are Widely Available

**Compelling solution both technically and economically**

**Cisco DDoS deployed by most providers**

Advantages*:*

- **Protects last-mile bandwidth as well as data center—typical last-mile bandwidth cannot withstand attack without significant upgrade**

- **Protection against largest attacks, not limited by size of last mile-bandwidth—attacks have reached up to 5 Gbps**

- **Allows economical provisioning of last-mile bandwidth and edge-device capacity only for legitimate traffic rates (No burst charge surprises for DDoS attacks)**

- **Upstream protection economically covers multiple data centers**

- **Leverage provider SOC instead of trying to maintain in-house expertise on DDoS attacks**

# Managed DDoS Services
# Cisco Powered Providers

**Largest carriers offering "clean pipes" services to F500 enterprises:**

- **Full managed services offered:**

  Service agreement and multiyear contract typical

  Gigabit+ dedicated capacity with shared overage

  Customized policies

  Customer-approved or automatic response (backbone or CPE Detector alert or activation)

  Service and attack reporting

**AT&T** — DDoS Defense Option for Internet Protect Managed Services

**CABLE & WIRELESS** — IP Defender Managed Service

**and many others** — **Sprint.**

# Managed DDoS Services
## Cisco Powered Providers

## Managed hosting providers are offering DDoS protected services:

- **Protection offered with hosting:**

  A la carte option, bundled with premium services or included with hosting

  Capacity matched to hosting

  Standardized or customized policies

  Service and attack reporting

**DataPipe** am

SureArmour DDoS Protection service

**rackspace** ™ MANAGED HOSTING

PrevenTier DDoS Mitigation Service

THE PLANET

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