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

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

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

Past
- Publicity driven
- High-profile targets
- Niche targets

Present
- Targeted economic

Mainstream corporations
- Potentially random

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

- Stronger and More Widespread
“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)

- 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

Total Losses for 2004—$141,496,560

Source: Computer Security Institute

2004 CSI/FBI Computer Crime and Security Survey
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

Not just downtime:

• Lost customers
• Damaged reputations
• Contractual liabilities

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

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
- Lower Cost of Operations
- High-Performance Intelligent Network
- 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

1. Detect

Protected Zone 1: Web
Protected Zone 2: Name Servers
Protected Zone 3: E-Commerce Application

Cisco Anomaly Guard Module
Cisco Traffic Anomaly Detector Module

Target
Dynamic Diversion At Work

1. Detect


Target

Protected Zone 1: Web
Protected Zone 2: Name Servers
Protected Zone 3: E-Commerce Application

Cisco Traffic Anomaly Detector Module
Cisco Anomaly Guard Module

Protected Zone 1: Web
Protected Zone 2: Name Servers
Protected Zone 3: E-Commerce Application
Dynamic Diversion At Work

1. Detect
3. Divert only target’s traffic

Route update: RHI internal, or BGP/other external

Protected Zone 1: Web
Protected Zone 2: Name Servers
Protected Zone 3: E-Commerce Application

Cisco Anomaly Guard Module
Cisco Traffic Anomaly Detector Module

Target
Dynamic Diversion At Work

1. Detect


3. Divert only target’s traffic

4. Identify and filter malicious traffic

Traffic Destined to the Target

Protected Zone 1: Web
Protected Zone 2: Name Servers
Protected Zone 3: E-Commerce Application

Cisco Traffic Anomaly Detector Module
Cisco Anomaly Guard Module

Target
Dynamic Diversion At Work

1. Detect
3. Divert only target’s traffic
4. Identify and filter malicious traffic
5. Forward legitimate traffic

Protected Zone 1: Web
Protected Zone 2: Name Servers
Protected Zone 3: E-Commerce Application

Traffic Destined to the Target
Legitimate Traffic to Target

Cisco Traffic Anomaly Detector Module
Cisco Anomaly Guard Module

192.168.3.0/24 [110/2] via 10.0.0.3, 2d11h, GigabitEthernet2
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

1. Detect


3. Divert only target’s traffic

4. Identify and filter malicious traffic

5. Forward legitimate traffic

6. Non-targeted traffic flows freely

Protected Zone 1: Web

Protected Zone 2: Name Servers

Protected Zone 3: E-Commerce Application

Cisco Traffic Anomaly Detector Module

Cisco Anomaly Guard Module

Target

Legitimate Traffic to Target

Traffic Destined to the Target

Non-targeted traffic flows freely
Solution Overview

- Dynamic route diversion
- Alert
- Anomaly Guard Module
- Traffic Anomaly Detector Module
- Supervisor Engine 2 or 720
- Line Card Module
- Firewall Service Module
- Cat6K/7600
- Internal Network

Cisco Catalyst Service Module
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

Master FIB Table → Routing Table

R(x)000 CPU

Supervisor 2 or Supervisor 720

Input Line Card → Crossbar Fabric → Crossbar Fabric → Anomaly Guard Module → Crossbar Fabric → Output Line Card

Cisco Catalyst® 6000 32 Gbps BUS
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
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

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

Dynamically insert specific filters to block attack flows and sources
Apply rate limits
Intelligent Countermeasures

Benefits:
- Accuracy
- Maximized performance
- Maximum transparency
- Automated response

1. **DETECTION**
   - Passive copy of traffic monitoring

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

3. **BASIC PROTECTION**
   - Basic antispoofing applied
   - Analysis for continuing anomalies

4. **STRONG PROTECTION**
   - Strong antispoofing (proxy) if needed
   - Dynamic filtering of zombie sources

Benefits:
- Accuracy
- Maximized performance
- Maximum transparency
- Automated response

Anomaly Sources Identified
Anomaly Verified
Attack Detected

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 total 1.5 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, authentication 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#)
- ack(c#,s#)
- Redirect(c#,s#)
- Syn(c’)
- Synack(c’,s’)
- request(c’,s’)
- Target

Hash-function(SrcIP,port,t)

Verified connections

SrcIP, port#
Brodest 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
Brodest 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
Hosting or Service Provider Data Center with Service Modules in “Integrated Mode”

Cisco.com

Catalyst® 6K or 7600

ISP 1

Sup720 or Sup2 w MSFC

ISP 2

RHI Route Update

Anomaly Guard Module

Traffic Anomaly Detector Module

Attack Alert

Firewall Service Module

Catalyst Switch

Target

Internal Network

Web, Chat, E-mail, etc.

DNS Servers

Guard/Detector Device Manager

Cisco DDoS Mitigation Service Provider Solutions © 2005 Cisco Systems, Inc. All rights reserved.
Service Provider
Distributed or Edge Protection

- Distributed, dedicated Guards
- Detector CPE for monitoring and optionally activation
Managed DDoS Service
Centralized Protection
Clustering Topology

ISP Upstream

ISP Upstream

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

Cat 6k/7600

Load-Leveling Router

Mitigation Cluster

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
  Commercial 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:

- DDoS Defense Option for Internet Protect managed services
- IP Defender managed service
- PrevenTier DDoS Mitigation service
- SureArmour DDoS protection service

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

- Protects last-mile bandwidth and all enterprise infrastructure
- Provider can protect against largest attacks
- Provision and pay only for bandwidth for legitimate traffic
- Upstream protection can cover multiple data centers
- DDoS protection can be efficiently offered as managed service
- Leverage focused security operations team

Enterprise Deployment at Data Center

- Last-mile bandwidth and edge router not protected
- Can only defend against attacks that don’t exceed last-mile bandwidth
- Must overprovision for largest potential attacks and/or pay burst charges
- Must replicate protection at all data centers
- CPE infrastructure only protects locally and cannot be shared
- Difficult to maintain staff skill on DDoS attacks