



WHITE PAPER

PREVENTING DISTRIBUTED DENIAL OF SERVICE ATTACKS WITH CISCO SELF-DEFENDING NETWORKS

Today's large, sophisticated distributed denial of service (DDoS) attacks target organizations of all sizes. How can you protect your organization from these debilitating attacks both now and in the future?

SUMMARY

The increase in Internet-based transactions and communications offers new opportunities for hackers to disrupt business operations with DDoS attacks. Organizations that are not adequately protected risk losing customers, revenue, and their good reputations. This white paper discusses the challenges of identifying, countering, and avoiding crippling DDoS attacks. With the comprehensive Cisco® Self-Defending Network, organizations can deploy layers of defense to detect and mitigate the effects of DDoS attacks.

THE SECURITY LANDSCAPE

The convenience, efficiency, and global reach of e-business benefit both consumers and businesses. But the accessibility of today's business operations brings increased security challenges. Legions of malicious hackers target e-commerce sites, online banks, partner networks, and Internet or e-mail servers seeking revenge or profit. The problem is serious—countering Internet crime is the U.S. FBI's third-highest priority, behind only countering terrorism and espionage.

Network security is a fairly new discipline. As a result, finding qualified security professionals—and justifying additional security spending—is challenging. Network and IT spending is often justified on return on investment (ROI), whereas network security has been traditionally viewed as a cost center. This perception is changing as well-publicized outages caused by security breaches demonstrate that comprehensive network security actually saves money for organizations.

DDOS PREVENTION CHALLENGES

A DDoS attack quickly overwhelms a company's server, router, firewall or network link with traffic; if successful, the attack floods the network or its resources so completely that legitimate traffic cannot be processed, and the company cannot function. The results are disastrous—frustrated customers place orders elsewhere, service-level agreements are violated, and corporate reputations are damaged. Meanwhile, all IT and security resources focus on responding to the attack. Unfortunately, their efforts are usually too late and only partially effective. A security strategy must instantly identify and respond to DDoS threats, while maintaining the availability of critical network resources for customers, partners, and employees.

DDoS attacks are the second-most costly security incident overall for organizations.* Estimates predict the cost of a 24-hour outage for a large e-commerce company would approach US\$30 million. Smaller organizations are not immune, however, with 12 percent reporting a DDoS attack in the previous 12 months.** Gartner predicts that half of all Internet-connected businesses will feel the impact of a DDoS attack in the next two years.***

* Source: CSI/FBI Computer Crime and Security Survey, 2004

** Source: Yankee Group, Small and Medium Business Infrastructure Survey, December 2004

*** Source: Gartner, December 2004

Identifying and responding effectively to DDoS attacks is becoming increasingly challenging. In the past, filtering specific source addresses was enough to stop basic DoS attacks. Today's DDoS attacks—distributed by definition—often use tens to hundreds of thousands of sources, courtesy of broadband-connected computers that have been infiltrated by hackers and turned into “zombies”. Zombie traffic resembles legitimate user traffic; separating them can be extremely difficult, and often requires large computing resources.

Originally, hackers generated DDoS attacks for mischief or revenge. Today, professionals motivated by profit launch sophisticated DDoS attacks—the deadlier the attack, the higher the gain. Some hackers target large financial institutions or e-commerce sites for extortion, threatening to launch attacks unless their payment demands are met. Others hire themselves out to organizations seeking to bring down a competitor's e-business operations, or launch DDoS attacks to manipulate a company's stock price. These attacks are often timed to produce the maximum negative impact for an organization, such as at the start of a holiday shopping season, or before a major corporate launch.

Sometimes, a DDoS attack is part of another security threat. For example, hackers successfully use DDoS attacks as a diversion while they steal information, such as credit card numbers. The flood of DDoS traffic successfully masks suspicious network activity, diverts security resources, and shuts down security monitoring devices that might otherwise detect and prevent the intrusion.

To prevent DDoS attacks from crippling business operations, organizations must detect and mitigate DDoS attacks automatically; ensure the business can continue to process legitimate traffic while under attack; and create a scalable, adaptable solution that addresses DDoS attacks now and in the future.

Organizations also have a responsibility to protect network endpoints (desktops, servers, and laptops, for example) from becoming zombies that could launch outbound DDoS attacks and use critical network resources. Achieving these goals requires a global systems-based view of network security, where every device connected to the network plays a role in securing the network against unwanted intrusions.

THE CISCO SELF-DEFENDING NETWORK

Today's DDoS attacks are swift and sophisticated. Security systems must react quickly and automatically to detect and mitigate these attacks before the network and its resources become flooded. A security system must be fully integrated into the network from end to end, so it can facilitate a coordinated response to attacks, regardless of location. It must be intelligent, so that it can differentiate potential threats from normal traffic and events. And it must be able to adapt to changing network security conditions. The Cisco Self-Defending Network is Cisco Systems' strategy for network security. By identifying, preventing, and then adapting to both internal and external threats, The Cisco Self-Defending Network allows businesses to maximize their network resources and protect not just their networks, but also their network investments. The results are improved business processes and substantial savings.

The Self-Defending Network contains three characteristics that together provide continuous, intelligent, future-proofed security from the network to the application layer:

- **Integrated.** Security defense technology is incorporated across all network elements, including routing, switching, wireless, and security platforms, so that every point in the network can defend itself. These security features include firewalling, virtual private networking, and trust/identity capabilities.
- **Collaborative.** These secure network components work together as a security system that adheres and responds to an organization's security policies. An example of the Collaborative characteristic is Network Admission Control (NAC), a multi-vendor effort only admits endpoints to the network once they have demonstrated their compatibility with various network security policies.
- **Adaptive.** The Self-Defending Network uses several tools to defend against new security threats and changing network conditions. Application awareness defends against security threats entering the network from within Internet-enabled applications. Behavioral recognition defends against worms, viruses, spyware, DDoS attacks, and other threats. Network control intelligently monitors and manages the security infrastructure and provides tools for IT managers to audit, control, and correlate security network episodes.

A LAYERED DEFENSE AGAINST DDOS ATTACKS

DDoS attacks can target many points in an organization's network. Servers (e-commerce, Web, or e-mail, for example) are often the targets of DDoS attacks. These servers are physically located in an organization's data center but logically connected to the Internet. Critical network components, such as firewalls or routers, are other common targets. Hackers can also seek to overwhelm the Internet connection between an organization and the rest of the world, cutting off all access to the organization's critical data centers. An organization may also be indirectly affected by a DDoS attack if its endpoints have been turned into zombies. With so many types of attacks, a multilayered approach to defending and securing an organization is required. A Cisco Self-Defending Network incorporates multiple layers of DDoS defense.

A Proactive Defense

A cost-effective, first-level step to avoiding or minimizing the effects of DDoS attacks is to take advantage of Cisco integrated security features in an existing network infrastructure. Cisco incorporates software capabilities into all routers, switches, and firewalls that protect these network devices from becoming overwhelmed during DDoS attacks, so they can continue to forward legitimate traffic. The Cisco IOS® Software feature set with the advanced security option and the Cisco Catalyst® integrated security software option protect the router or switch processor, control plane, forwarding tables or interfaces from being flooded in a DDoS attack. The integrated security functions that protect Cisco IOS routers and Cisco Catalyst switches use numerous mechanisms to drop or throttle insecure traffic if the network, or the router or switch itself, is under attack. Security managers can place restrictions on the types of traffic that can address the router or switch directly, helping to ensure that the processor is not overloaded by false requests.

However, large-scale DDoS attacks that saturate any device or link capacity, or that result in any defensive throttling action, compromise availability for legitimate users and transactions. If network components are protected from failure but unavailable for legitimate transactions, the DDoS attack has succeeded.

Detect and Contain All DDoS Attacks

Once a DDoS attack is detected, automatic protection should start containing or minimizing the impact of the attack. Cisco integrated security features in switches, routers, and standalone appliances play a role in DDoS detection and containment. Network performance data from routers can be analyzed to detect DDoS attacks. Firewalls can be configured to weed out many types of protocols associated with less sophisticated DDoS attacks.

But firewalls, intrusion prevention systems (IPSs), and integrated router and switch security are not enough to contain large-scale, sophisticated DDoS attacks. Most DDoS attacks generate huge volumes of traffic using cleverly spoofed packets or valid source addresses from large numbers of zombies. This traffic mimics valid transactions and often does not contain abnormal or malicious code, so it will pass through conventional filtering systems in routers, switches, and appliances. These attacks can quickly reach an organization's resources and overwhelm them.

Cisco has an industry-leading, adaptive solution that helps ensure business continuity by detecting and automatically defending against all types of DDoS attacks. The Cisco Traffic Anomaly Detector XT 5600 and the Cisco Guard XT 5650 DDoS Mitigation Appliance are intelligent elements of Cisco's Self-Defending Network solution. The detector and guard are available as either standalone appliances or as integrated services modules for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers. The detector learns what normal traffic looks like, and uses this information to identify abnormal patterns of traffic. Once it recognizes a traffic anomaly destined for a particular server or piece of network infrastructure, it diverts all traffic headed to that destination—not just suspicious packets—to the guard. Traffic destined for other areas of the organization's network is not affected. The guard uses behavioral recognition and multiple layers of defense to identify and remove packets associated with DDoS attacks. A unique combination of active source verification and anomaly recognition is crucial for accurately distinguishing sophisticated attack sources and packets from legitimate transactions. The guard then forwards the legitimate traffic to its intended destination. The attack is eliminated and business continues without interruption.

Managed DDoS Services

From both a technical and economic viewpoint, it makes the most sense to repel DDoS attacks before they reach an organization's data center. Typical "last-mile" bandwidth connecting enterprises to the Internet cannot withstand today's large DDoS attacks. Rather than spend money over-provisioning their connection to the outside world, organizations find it more economical to partner with service providers that repel DDoS attacks at the service provider network. The Cisco Guard and Detector solution delivers the performance, scalability, and architecture necessary for a managed DDoS service. Many of the world's leading service providers are already offering managed DDoS protection services based on the Cisco Guard and Detector solution, preventing DDoS attacks from ever reaching their customers' data centers and last-mile connections. Deployment options vary and depend on an organization's needs and traffic patterns. A comprehensive DDoS protection service can be securely shared between several organizations or can be dedicated to a single enterprise. A DDoS service can be offered on its own, or combined with a Web hosting or e-commerce solution. Cisco detectors can also be deployed as customer premises equipment (CPE), giving organizations more control over DDoS prevention management and administration. Some large enterprises that operate their own backbones or maintain high-bandwidth connections may choose to operate the solution directly.

Ensure Business Continuity

Even when under attack, organizations seek to minimize disruption, maintain business productivity, and continue to serve customers. A business continuity plan identifies risks and potential security threats, and defines technological and business processes to detect and mitigate real-time incidents such as DDoS attacks. A business continuity plan is mandatory in some regulated industries, such as finance. However, all organizations can benefit from a properly executed plan.

Together, the Cisco Traffic Anomaly Detector and Cisco Guard are a unique DDoS defense solution that helps ensure business continuity during DDoS attacks. They continue to deliver legitimate traffic to a targeted device during an attack, while accurately detecting and removing DDoS traffic. Diverting traffic to the guard also ensures that links from the service provider to the organization do not remain clogged, as they would during a typical attack. The Cisco Traffic Anomaly Detector and Cisco Guard can scale to protect even the largest organizations, with the most amount of online traffic, from the consequences of DDoS attacks.

Protect Against Attacks on Others

Compromised endpoints are unable to perform productively. Organizations that fail to properly secure their desktops and laptops from malicious mobile code can be unwitting participants in a DDoS attack against their own or another organization. Some worms and viruses create a "back door" into computers, allowing hackers to send huge amounts of traffic to a targeted organization via infected computers. Other worms or viruses include automatic instructions to start sending requests to a certain server at a certain date and time.

Cisco Security Agent uses behavior-based assessment to identify and prevent malicious behavior on endpoints. It analyzes behavior of the system, and can eliminate both known and unknown ("day zero") security risks based on this behavior. Cisco Security Agent aggregates multiple security functions by providing host intrusion prevention, distributed firewall capabilities, malicious mobile code protection, operating system integrity assurance, and audit log consolidation in a single powerful software package.

MONITORING AND MANAGING THE SECURITY STATE OF THE NETWORK

In a large, distributed network, it can be difficult to see the big picture. Firewalls, IPS appliances, routers, switches, and secure endpoints continuously send large amounts of security-related network intelligence to management stations. The IT staff needs intelligent tools in order to analyze and act on this information.

The Cisco Security Monitoring, Analysis and Response System (CS-MARS) is a family of high-performance, scalable appliances that monitors the enterprise security infrastructure and correlates network and security device information, application logs, and security events. Through graphical network representations, the Cisco Security Monitoring, Analysis and Response System provides a consolidated view of all security devices,

enabling IT staff to identify, track, analyze, and mitigate incidents and attacks in real time from a central location. The Cisco Security Monitoring, Analysis and Response System also provides reports and stores information on network security status, which can help enterprises meet regulatory compliance and audit requirements.

PROTECT YOUR NETWORK FROM DDOS ATTACKS WITH CISCO SELF-DEFENDING NETWORKS

Organizations need to avoid the disruption caused by DDoS attacks, while controlling the costs of deploying and maintaining a secure network. A Cisco Self-Defending Network identifies, prevents, and adapts to changing security threats; protects corporate assets; helps ensure business continuity; and contains the total cost of network ownership. With a multilayered security approach, a Cisco Self-Defending Network provides the broadest defense against DDoS attacks threatening an organization's servers, network elements, or Internet connections.

Cisco is the industry leader in networking and security solutions. Only Cisco offers a unique, systemic approach to business security based on the intelligent collaboration of networking and security technologies and services. Cisco provides the most comprehensive range of integrated, intelligent, adaptable security solutions to best protect organizations of all sizes from disruptive and expensive DDoS attacks.

For more information on protecting your organization from DDoS attacks and on the Cisco Self-Defending Network strategy, please visit:

<http://www.cisco.com/go/ddos>



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website** at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R) 204053.P_ETMG_KM_8.05