



WHITE PAPER

## CISCO DISTRIBUTED DENIAL OF SERVICE PROTECTION SOLUTION: LEADING DDoS PROTECTION FOR SERVICE PROVIDERS AND THEIR CUSTOMERS

Today, service providers and their customers are exposed to a growing number of distributed-denial-of-service (DDoS) attacks, which can damage revenues and reputations. Therefore, service providers' offerings must include advanced security solutions. This paper explains the Cisco® DDoS Protection solution, part of the IP Next-Generation Network (NGN) from Cisco Systems®. The Cisco DDoS Protection solution helps enable service providers to sell customers "clean pipes" connectivity services while at the same time hardening and protecting their own infrastructure to ensure resilient service delivery. The solution includes new service modules for the Cisco 7600 Series Router and Cisco Catalyst® 6500 Series Switch, and a comprehensive set of system architectures that have been validated in different service provider infrastructure and managed security service implementations.

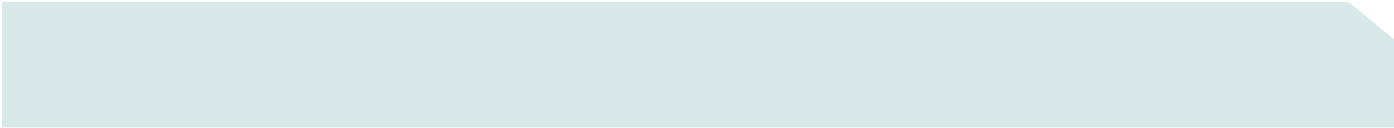
### EXECUTIVE SUMMARY

DDoS attacks have evolved from random hacker exploits into organized criminal activities aimed at extorting ransom money from targeted businesses and government entities. DDoS attacks against host systems or network infrastructure disrupt services to customers, limit access to servers and other critical network resources, and can block legitimate network traffic flows by absorbing all available bandwidth.

It has become trivial to launch DDoS attacks through process automation, and traditional network security mechanisms located at the customer premise are not designed to mitigate them. The effective way to mitigate these attacks is to clean the packet traffic before it reaches the customer site by dropping bad traffic and allowing only legitimate traffic to the destination, protecting the bandwidth-limited connection from service provider to customer. Combating attacks requires a purpose-built system-level architecture that detects and mitigates increasingly sophisticated, complex, and deceptive attacks.

The Cisco DDoS Protection solution enhances the security profile of service provider networks, enabling them to deliver "clean pipes" capabilities to their customers. Its premise is to find and deal with anomalies in the network infrastructure closest to the source of the attack. By enabling greater visibility into malicious traffic and providing the means to better control it, Cisco promotes business continuity and service availability, allowing service operators to meet their service-level agreements. By installing these security capabilities in the operational layer in the Cisco IP NGN architecture, service providers are also able to deploy a new class of security services, effectively turning security from a cost center to a profit center.

The Cisco DDoS Protection solution leverages the Cisco Network Foundation Protection (NFP) technology embedded in Cisco switches and routers, which hardens the data, control, management, and service planes of the infrastructure against various security threats. Then it combines several functional elements including detection, mitigation, and traffic diversion and injection to protect networks from DDoS attacks. Unlike other DDoS defense techniques, which generally drop all traffic to the affected target network, the Cisco solution distinguishes legitimate traffic from harmful traffic, then filters the bad traffic while passing the good traffic.



The Cisco DDoS Protection solution is not simply a collection of security point products, but a tightly integrated system ready for defending against today's most damaging DDoS attacks. Moreover, the typical implementations and architectures that service providers use to defend their networks and offer DDoS protection services to their customers have already been validated.

## **TAXONOMY OF DDoS ATTACKS AND BUSINESS RISK**

### **A DDoS Primer**

DDoS attacks disrupt service to customers and users by slowing or even completely blocking legitimate network traffic flows due to excessive packet flooding of the IP bandwidth. Typically, the network resource under attack is sent far more traffic than it can manage.

Traditional security mechanisms located at the customer premise are not designed to identify and protect against such attacks. A DDoS attack can be created by a botnet, or network of compromised machines (bots) that can be remotely commandeered by an attacker. Before a DDoS attack occurs, the attacker compromises and installs a daemon on a number of hosts. To start an attack, the attacker instructs the daemon on the compromised hosts to begin flooding a target host with various types of packets. The ensuing massive stream of data overwhelms the victim's hosts or routers.

Botnets can consist of several tens of thousands of compromised machines. Even relatively small botnets can aggregate a combined bandwidth that exceeds the "last-mile" connection of most corporate systems. The IP distribution of the bots makes it difficult to construct, maintain, and deploy ingress filters. Also, botnets can act stealthily by sending small data streams from each compromised host but still deliver a sizable attack to its target. Incident response is hampered by the large number of separate organizations that may be involved in a distributed botnet. As a result, tracing an attack back to its source is extremely difficult.

### **Service and Business Risk Implications**

Attack schemes have become streamlined extortion operations and a component of organized crime activities, threatening to attack a target business if it does not pay a ransom. Some attackers offer DDoS attack services, reportedly renting out their botnets for US\$0.10 to US\$0.40 per bot. The purpose of an attack can be for a monetary payoff or merely for spite.

Any business that relies on its Website to do business transactions is a target, especially during important events like a major sports game, a new product launch, or a quarterly earnings conference call. These are opportunities for attackers to extort vulnerable targets. While online businesses were early victims, now all sectors including financial, retail, media and entertainment, manufacturing, services, and governments are potential victims of DDoS attacks.

Network security has become a critical part of business success. A secure infrastructure forms the foundation for service availability and delivery. Operations and core business functions are conducted over the Internet and IP networks, and converged IP networks are becoming a major part of all businesses. An attack that results in any downtime will have a negative effect on profits. Even if the direct impact of the attack on the network is insignificant, the perception of the network being vulnerable can have financial repercussions that are significant indeed.

## **CISCO DDoS PROTECTION SOLUTION**

The Cisco DDoS Protection solution is not simply a collection of security point products, but a tightly integrated system ready for defending against today's most damaging DDoS attacks. As a part of the operational layer in the Cisco IP NGN architecture, the Cisco DDoS Protection solution enables service providers to sell connectivity services with "clean pipes" attributes to customers, while hardening and protecting their own infrastructure to ensure resilient service availability and delivery—e.g., VPN, IP communications, video—without disruption, despite DDoS attacks.

Because only secure networks are available networks, the network has to be hardened at its foundation. Network elements need inherent and comprehensive security features to lock down services and routing protocols, secure access for management and instrumentation, and protect data forwarding through the device.

### **Deploying Network Infrastructure Security with Cisco NFP**

While the Cisco DDoS Protection solution provides a comprehensive solution against DDoS threats for service providers and their customers, we strongly recommend that service providers make full use of the Cisco Network Foundation Protection (NFP). Cisco NFP is a part of Cisco IOS® Software that protects network devices, routing and forwarding of control information, and management of traffic bounded to the network devices. In effect, NFP is built into the fabric of Cisco routers and switches.

Cisco NFP hardens the data, control, and management planes of the network infrastructure against a wide variety of security threats. The advantages of deploying Cisco NFP include the following:

- Provide network devices protection not only from DDoS attacks but also from threat vectors like reconnaissance, network device break-ins, and theft of service.
- Help minimize vulnerability of critical services such as Domain Name System (DNS), e-mail, Web access, and VoIP to network attacks.
- Make use of network telemetry, such as NetFlow, to study traffic patterns in real time, create traffic baselines, detect anomalies and miscues, and characterize affected interfaces. Anomalies can be compared across the network to provide traceback and determine an attack's point of ingress.
- Complement the Cisco DDoS Protection solution—NFP mitigates primitive DDoS attacks, thus freeing the capacity of the Cisco Guard to fight more sophisticated attacks.

For more information about Cisco NFP, visit: <http://www.cisco.com/go/nfp>.

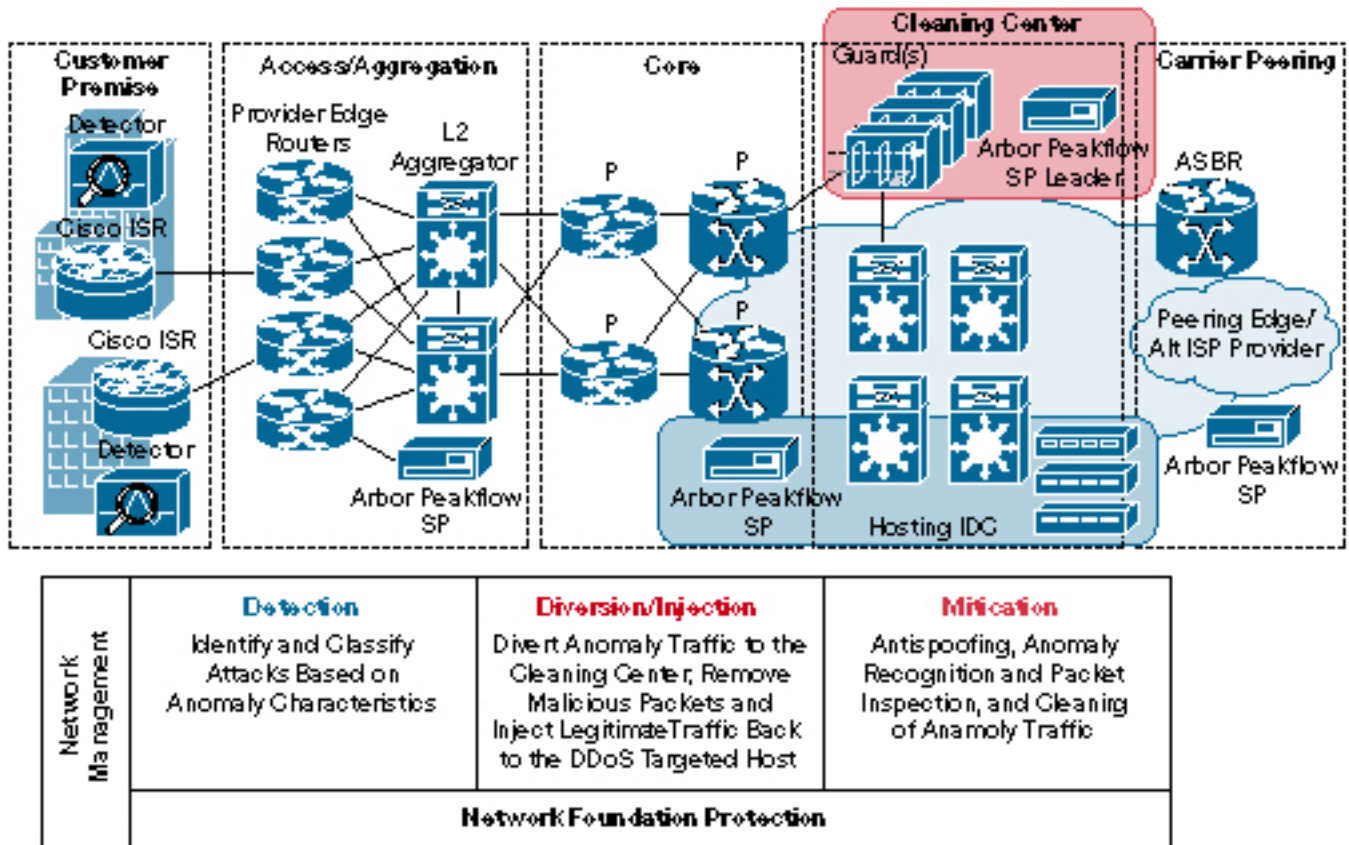
Unlike other DDoS defense techniques, which generally drop all traffic, good and bad, to the target network, the mitigation function of the Cisco DDoS Protection solution accurately distinguishes legitimate traffic from malicious traffic, then filters out harmful traffic while allowing legitimate traffic to pass.

## Cisco DDoS Protection Solution Highlights

Figure 1 depicts the architecture of the Cisco DDoS Protection solution.

Figure 1

Architecture of Cisco DDoS Protection Solution



The solution incorporates new Cisco products in the infrastructure, along with partner-developed products from Arbor Networks, including:

- The NetFlow feature, supported on Cisco devices including the Cisco CRS-1 Carrier Routing System and the Cisco 12000, 10000, and 7600 Series routers focused on network telemetry in the service provider network
- The Cisco Traffic Anomaly Detector XT 5600 and the new Cisco Traffic Anomaly Detector Module for the Cisco 7600 Series Router and Cisco Catalyst® 6500 Series Switch for precise anomaly detection, including deployment at the customer premise with APIs to managed service
- The Cisco Guard XT 5650 and the new Cisco Anomaly Guard Service Module for the Cisco 7600 Series Router and Cisco Catalyst 6500 Series Switch for precise anomaly analysis and mitigation
- Arbor Networks Peakflow SP—including infrastructure security, managed services, and traffic and routing functions—as an option for intelligent traffic and routing analysis for DDoS and worm protection

Cisco Systems, Inc.

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Page 4 of 7

Arbor Networks, a Cisco Technology Developer Program Partner, provides a solution that uses NetFlow data from Cisco devices for networkwide relational modeling, anomaly detection, and intelligent mitigation management that alerts the Cisco Guard in the cleaning centers.

For more information about the Peakflow SP, visit: [http://arbor.net/products\\_sp.php](http://arbor.net/products_sp.php).

### Cisco DDoS Protection Solution Deployment Models

The Cisco DDoS Protection solution has been tested and validated in the four most common deployment models that service provider customers have implemented, as indicated in Table 1.

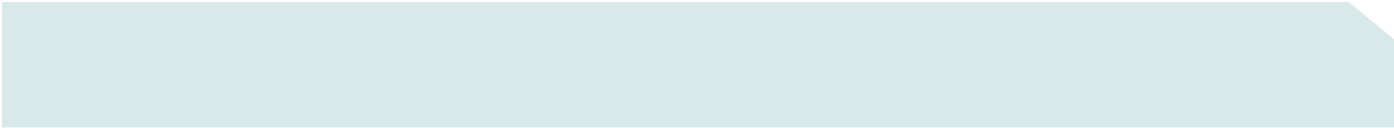
**Table 1.** Validated Deployment Models for Cisco DDoS Protection Solution

DDoS Protection Model	Core Function(s)	Key Capabilities
<b>DDoS infrastructure protection</b>	Protection model for service provider to defend networks and protect service delivery	<ul style="list-style-type: none"> <li>• Protect critical assets in the data center</li> <li>• Mitigate attacks on critical routing infrastructure (peering points, provider edge and core routers)</li> <li>• Reduce operating expense by reducing unwanted traffic across expensive links</li> <li>• Reduce collateral damage impacts</li> </ul>
<b>Managed network DDoS protection</b>	“Last-mile” bandwidth protection for service provider customers	<ul style="list-style-type: none"> <li>• New revenue model for service providers</li> <li>• Primary function to enhance business continuance for customers</li> <li>• Protection of critical bandwidth</li> <li>• Ensure continual delivery of enhanced services offered over data connections</li> </ul>
<b>Managed hosting DDoS protection</b>	Protection of data center assets hosted by providers	<ul style="list-style-type: none"> <li>• New revenue model for service providers</li> <li>• Ensure uptime of critical assets hosted by service providers</li> <li>• Differentiation of the hosting service</li> </ul>
<b>Managed peering point DDoS protection</b>	Provide DDoS-free wholesale connections for downstream ISPs	<ul style="list-style-type: none"> <li>• New revenue model for service providers</li> <li>• Provide clean wholesale connections</li> <li>• Better promote a DDoS-free environment</li> </ul>

The Cisco DDoS Protection solution offers notable benefits to both service providers and their customers.

Service provider benefits include:

- Ability to enhance protection or harden infrastructure to enable IP service delivery despite DDoS attacks
- Ability to add a new revenue stream on top of existing service
- Ability to become a trusted partner that understands security implications to the business
- Ability to better utilize core assets for new service and differentiation
- Ability to start delivering protection services without large capital investment



Business customer benefits include:

- Proactive, real-time DDoS mitigation in which service provider detects attacks in real time and mitigates impacts on the network rapidly, grounding the attack before network resources are overwhelmed
- Protection of critical assets in the data center including Web servers, DNS and Dynamic Host Configuration Protocol (DHCP) servers, and other mission-critical elements
- Better assurance of business continuity through upstream protection that keeps network resources remaining active and usable
- Compliance with new laws and regulations such as Sarbanes-Oxley in the financial and accounting fields

## **CONCLUSION**

The Cisco DDoS Protection solution, inscribed in the operational layer of the Cisco IP NGN architecture, delivers “clean pipes” capabilities to service providers. The solution leverages the Network Foundation Protection elements of Cisco IOS Software, which embed comprehensive security features in Cisco switches and routers to lock down services and routing protocols, secure access for management and instrumentation, and protect data forwarding through the devices. Additionally, the solution uses the Cisco DDoS Protection products and partner products to perform the detection, mitigation, and traffic diversion and injection functions to protect networks from increasingly complex DDoS attacks

The Cisco DDoS Protection solution enables service providers to sell connectivity services to customers while hardening their own network infrastructure to help ensure resilient service delivery despite DDoS attacks. This Cisco solution is not simply a collection of individual security products, but a tightly integrated system ready for defending against today’s most damaging DDoS attacks. In fact, it is already validated in the most common typical DDoS protection implementations and architectures.

**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](http://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

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks or 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) DMLW8643 06/05