WHITE PAPER

DEFEATING DDOS ATTACKS

Distributed denial-of-service (DDoS) attacks are a real—and growing—threat to businesses worldwide. Designed to elude detection by today's most popular tools, these attacks can quickly incapacitate a targeted business, costing victims thousands, if not millions, of dollars in lost revenue and productivity. By adopting new purpose-built solutions designed specifically to detect and defeat DDoS attacks, businesses can keep their business operations running smoothly.

DDoS attacks are weapons of mass disruption. Unlike access attacks that penetrate security perimeters to steal information, DDoS attacks paralyze Internet systems by overwhelming servers, network links, and network devices (routers, firewalls, etc.) with bogus traffic.

DDoS is emerging as the weapon of choice for hackers, political "hacktivists," cyber-extortionists, and international cyber-terrorists. Easily launched against limited defenses, DDoS attacks not only target individual Websites or other servers at the edge of the network— they subdue the network itself. Attacks have begun to explicitly target the network infrastructure, such as aggregation or core routers and switches, or Domain Name System (DNS) servers in a provider's network. In October 2002, a harbinger of future large-scale attacks was a crude DDoS attack that affected 8 of the 13 root DNS servers, critical systems serving as the roadmap for virtually all Internet communications.

The growing dependence on the Internet makes the impact of successful DDoS attacks—financial and otherwise—increasingly painful for service providers, enterprises, and government agencies. And newer, more powerful DDoS tools promise to unleash even more destructive attacks in the months and years to come.

Because DDoS attacks are among the most difficult to defend against, responding to them appropriately and effectively poses a tremendous challenge for all Internet-dependent organizations. Network devices and traditional perimeter security technologies such as firewalls and intrusion detection systems (IDSs), although important components of an overall security strategy, do not by themselves provide comprehensive DDoS protection. Instead, defending against the current DDoS onslaught threatening Internet availability requires a purpose-built architecture that includes the ability to specifically detect and defeat increasingly sophisticated, complex, and deceptive attacks.

This white paper describes:

- The growing DDoS threat and the severe impact successful attacks have on organizations
- Why current router and perimeter security technologies require complementary solutions to provide comprehensive DDoS protection
- What baseline requirements must be met to defeat DDoS attacks
- How the Cisco Systems® innovative technology and architecture delivers complete DDoS protection

THE DDOS THREAT

A DDoS attack directs hundreds or even thousands of compromised "zombie" hosts against a single target. These zombie hosts are unwittingly recruited from the millions of unprotected computers accessing the Internet through high-bandwidth, "always-on" connections. By planting "sleeper" codes on these machines, hackers can quickly build a legion of zombies, all waiting for the command to launch a DDoS attack. With enough zombie hosts participating, the volume of an attack can be astounding.

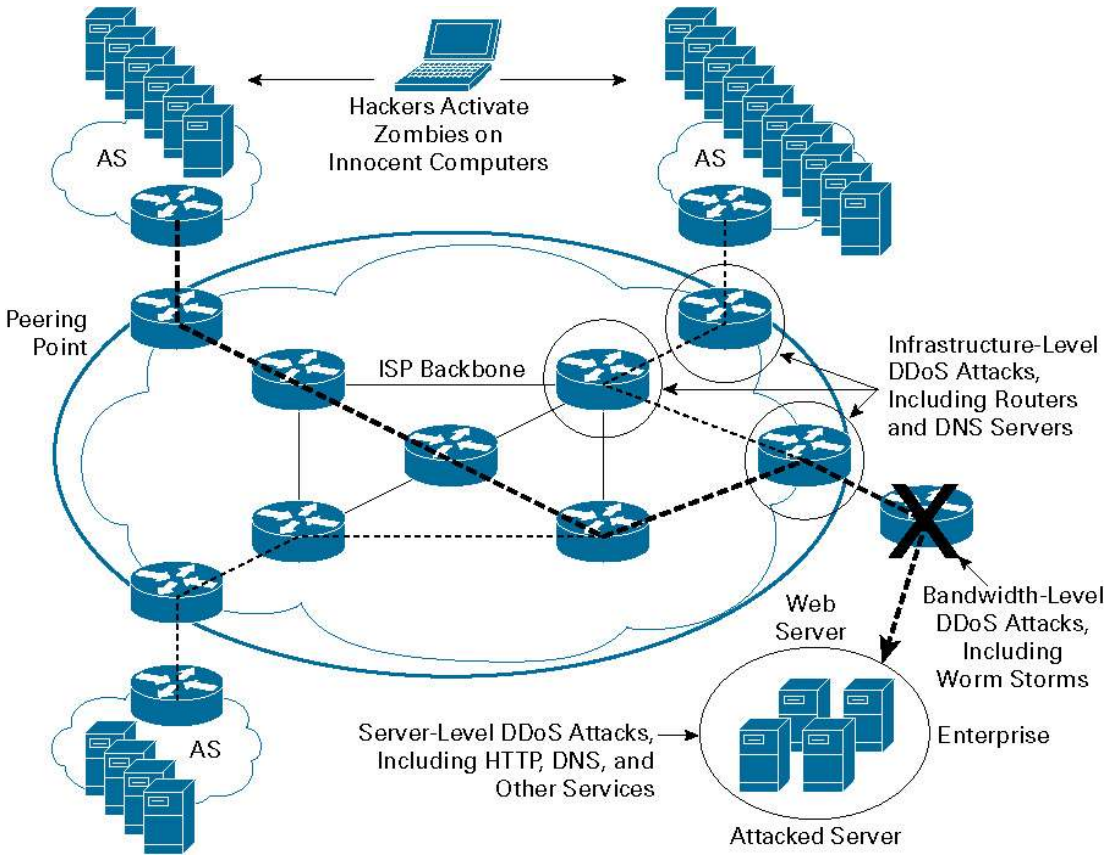
The Impact of DDoS Attacks

The impact of a successful DDoS attack is widespread. Site performance is severely compromised, resulting in frustrated customers and other users. Service-level agreements (SLAs) are violated, triggering costly service credits. Company reputations are tarnished, sometimes permanently. Lost revenue, lost productivity, increased IT expenses, litigation costs—the losses just keep mounting.

The numbers are staggering. Estimates from Forrester, IDC, and the Yankee Group predict the cost of a 24-hour outage for a large e-commerce company would approach US$30 million. A spate of DDoS attacks against Amazon, Yahoo, eBay, and other major sites in February 2000 caused an estimated cumulative loss of US$1.2 billion, according to the Yankee Group. And in January 2001, Microsoft lost approximately US$500 million over the course of a few days from a DDoS attack on its site. Clearly, businesses must take steps to protect themselves from these malicious attacks by shoring up defenses at their multiple points of vulnerability (refer to Figure 1).

Figure 1

Multiple Points of Vulnerability and Failures



Inside DDoS Attacks

How do DDoS attacks work? By taking advantage of Internet protocols and the fundamental benefit of the Internet—delivering data packets from nearly any source to any destination, without prejudice.

Essentially, it is the behavior of these packets that defines the DDoS attack: either there are too many, overwhelming network devices as well as servers, or they are deliberately incomplete to rapidly consume server resources. What makes DDoS attacks so difficult to prevent is that illegitimate packets are indistinguishable from legitimate packets, making detection difficult; typical "signature" pattern matching, performed by IDSs, do not work. Many of these attacks also use spoofed source IP addresses, thereby eluding source identification by anomaly-based monitoring tools looking for unusually high volumes of traffic coming from specific origins.

The two most basic types of DDoS attacks follow:

- Bandwidth attacks—These DDoS attacks consume resources such as network bandwidth or equipment by overwhelming one or the other (or both) with a high volume of packets. Targeted routers, servers, and firewalls—all of which have limited processing resources—can be rendered unavailable to process valid transactions, and can fail under the load.

  The most common form of bandwidth attack is a packet-flooding attack, in which a large number of seemingly legitimate TCP, User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP) packets are directed to a specific destination. To make detection even more difficult, such attacks might also spoof the source address—that is, misrepresent the IP address that supposedly generated the request to prevent identification.
- Application attacks—These DDoS attacks use the expected behavior of protocols such as TCP and HTTP to the attacker's advantage by tying up computational resources and preventing them from processing transactions or requests. HTTP half-open and HTTP error attacks are just a couple examples of application attacks.

The DDoS Threat Grows Ever More Disruptive

A growing trend among DDoS attackers is to use sophisticated spoofing techniques and essential protocols (instead of nonessential protocols that can be blocked) to make DDoS attacks even more stealthy and disruptive. These attacks, which use legitimate application protocols and services, are very difficult to identify and defeat; employing packet-filtering or rate-limiting measures simply completes the attacker's task by shutting everything down, causing denial of legitimate users.

TODAY'S INSUFFICIENT DDOS DEFENSES

Regardless of the type of DDoS attack, current techniques used to deal with them fall short in terms of mitigation and ensuring business continuity. Some of the more popular DDoS responses—such as "blackholing" and router filtering—are not optimized to deal with the increasingly sophisticated attacks being seen today. IDSs offer some excellent attack-detection capabilities, but cannot mitigate the impact of the attacks. Firewalls offer a rudimentary level of protection but, like blackholing and router filtering, they were not designed to protect against the types of advanced attacks that are so common today. Still other strategies, such as overprovisioning, do not provide adequate protection against ever larger attacks, and they are far too costly as a DDoS prevention strategy.

Blackholing

Blackholing describes the process of a service provider blocking all traffic destined for a targeted enterprise as far upstream as possible, sending the diverted traffic to a "black hole" where it is discarded in an effort to save the provider's network and its other customers. Because legitimate packets are discarded along with malicious attack traffic, blackholing is not a solution. Victims lose *all* their traffic—and the attacker wins.

Routers

Many people assume that routers, which use access control lists (ACLs) to filter out "undesirable" traffic, defend against DDoS attacks. And it is true that ACLs can protect against simple and known DDoS attacks, such as ping attacks, by filtering nonessential, unneeded protocols.

However, today's DDoS attacks generally use valid protocols that are essential for an Internet presence, rendering protocol filtering a less effective defense. Routers can also stop invalid IP address spaces, but attackers typically spoof valid IP addresses to evade detection. In general, although router ACLs do provide a first line of defense against basic attacks, they are not optimized to defend against the following sophisticated types of DDoS attacks:

- SYN, SYN-ACK, FIN, etc. floods—ACLs cannot block a random, spoofed SYN attack or ACK and RST attacks on port 80 of a Web server, where the spoofed source IP addresses are constantly changing, because manual tracing would be required to identify all the individual spoofed sources—a virtual impossibility. The only option would be to block the entire server, completing the attacker's goal.
- Proxy—Because ACLs cannot distinguish between legitimate and malicious SYNs coming from the same source IP or proxy, it would, by definition, have to block all the victim's clients coming from a certain source IP or proxy when attempting to stop this focused spoofed attack.
- DNS or Border Gateway Protocol (BGP)—When these types of randomly spoofed DNS server or BGP router attacks are launched, ACLs—as with SYN floods—cannot track the rapidly changing volume of random spoofed traffic. In addition, they have no way of identifying which addresses are spoofed and which are valid.
- *Application-level (client) attacks*—Although ACLs could theoretically block client attacks such as HTTP error and HTTP half-open connection attacks (provided the attack and individual nonspoofed sources could be accurately detected), it would require users to configure hundreds and sometimes thousands of ACLs per victim.

Another router-based DDoS prevention strategy—using Unicast Reverse Path Forwarding (uRPF) to stop spoofed attacks on the outbound side—is generally ineffective against today's DDoS attacks because the underlying principle of uRPF is to block outbound traffic if the IP address does not belong to the subnet. However, because attackers can spoof source IP addresses from the same subnet they are sitting behind, such a strategy can be easily defeated. Additionally, for uRPF to be truly effective, it would have to be implemented in front of every potential attack source—an implementation that would be difficult, if not impossible, to accomplish.

Firewalls

Although firewalls play a critical role in any organization's security solution, they are not purpose-built DDoS prevention devices. In fact, firewalls have certain inherent qualities that impede their ability to provide complete protection against today's most sophisticated DDoS attacks.

First is location. Firewalls reside too far downstream on the data path to provide sufficient protection for the access link extending from the provider to the edge router at the fringe of the enterprise, leaving those components vulnerable to DDoS attacks. In fact, because firewalls reside inline, they are often targeted by attackers who attempt to saturate their session-handling capacity to cause a failure.

Second is a lack of anomaly detection. Firewalls are intended primarily for controlling access to private networks, and they do an excellent job of that. One way this is accomplished is by tracking sessions initiated from inside (the "clean" side) to an outside service and then accepting only specific replies from expected sources on the ("dirty") outside. However, this does not work for services such as Web, DNS, and other services, which must be open to the general public to receive requests. In these cases, the firewalls do something called opening a conduit—that is, letting HTTP traffic pass to the IP address of the Web server. Although such an approach offers some protection by accepting only specific protocols for specific addresses, it does not work well against DDoS attacks because hackers can simply use the "approved" protocol (HTTP in this case) to carry their attack traffic. The lack of any anomaly-detection capabilities means firewalls cannot recognize when valid protocols are being used as an attack vehicle.

The third reason firewalls cannot provide comprehensive DDoS protection is a lack of antispoofing capabilities. When a DDoS attack is detected, firewalls can shut down a specific flow associated with the attack, but they cannot perform antispoofing on a packet-by-packet basis to separate good or legitimate traffic from bad—action that is essential for defending against attacks using a high volume of spoofed IP addresses.

IDS

Although IDSs provide excellent application layer attack-detection capabilities, they do have a weakness: they cannot detect DDoS attacks using valid packets—and most of today's attacks use valid packets. Although IDSs do offer some anomaly-based capabilities, which are required to detect such attacks, they require extensive manual tuning by experts and do not identify the specific attack flows.

Another potential issue with IDSs as a DDoS defense platform is that they only detect—they do nothing to mitigate the effects of an attack. IDS solutions may recommend filters for routers and firewalls, but, as described earlier, these are not entirely effective for mitigating today's sophisticated DDoS attacks. What IDSs require is a complementary mitigation solution that provides the next level of specific attack flow identification, integrated with immediate enforcement capabilities.

In summary, IDSs are optimized for signature-based application layer attack detection. Because sophisticated DDoS attacks are defined by anomalous behavior at Layers 3 and 4, current IDS technology is not optimized for DDoS detection or mitigation.

Manual Responses to DDoS Attacks

Manual processes used as part of a DDoS defense are a case of too little, too late. A victim's first response to a DDoS attack is typically to ask the closest upstream connectivity provider—an Internet service provider (ISP), a hosting provider, or a backbone carrier—to try to identify the source. With spoofed addresses, this can be a long and tedious process that requires cooperation among many providers. And though a source might be identified, blocking it would mean blocking all traffic—good and bad.

Other Strategies

In order to withstand DDoS attacks, enterprise operators may have considered various strategies such as overprovisioning—that is, buying excess bandwidth or redundant network devices to handle any spikes in demand. Such an approach is not particularly cost effective, especially because it requires the addition of redundant network interfaces and devices. And regardless of the initial effect, attackers merely need to increase the volume of the attack to defeat the extra capacity.

THE CASE FOR SECURING AVAILABILITY

Any business with an online presence has any number of reasons—economic and otherwise—to invest in DDoS protection. Large enterprises, government organizations, service providers—all need to protect the components of their infrastructure (Web servers, DNS servers, e-mail and chat servers, firewalls, switches, and routers) to preserve the integrity of business operations and make more efficient use of technical staff.

ROI Models of DDoS Defense

Of course, implementing complete DDoS protection carries its own costs. However, the return on investment (ROI) for implementing such a program is compelling.

- E-commerce—DDoS protection for e-commerce sites can pay for themselves within a matter of hours when compared to the cost of potential losses associated with a DDoS attack. The transactional volumes of an e-commerce site, average revenue per transaction, advertisement revenue, intangibles such as brand equity and legal liabilities, as well as technical staff time required to restore an attacked site should all be considered when determining the fiscal impact of any DDoS-related downtime. Add the possibility that DDoS protection might allow downgrading to less-expensive bandwidth links, and the ROI figures grow even more impressive.
- Service providers—For service providers, keeping their own network operational has huge ROI ramifications. If a provider's infrastructure is attacked (routers, DNS, etc.), all services to customers fail, resulting in SLA violations. The cost of DDoS protection is insurance against catastrophic failures that would cost the business orders of magnitude more in terms of both revenue and negative customer relations.

Cost-avoidance, however, is not the only motivation for hosting, transit, and service providers to implement a complete DDoS solution. For these users, DDoS protection can also be offered as a value-added service that creates new revenue streams and provides competitive differentiation.

MITIGATING THE DDOS THREAT

Taking on DDoS attacks requires a new approach that not only detects increasingly complex and deceptive assaults but also mitigates the effects of the attack to ensure business continuity and resource availability.

Complete DDoS protection is built around four key themes:

1. Mitigate, not just detect.
2. Accurately distinguish good traffic from bad traffic to preserve business continuity, not just detect the overall presence of an attack.
3. Include performance and architecture to deploy upstream to protect all points of vulnerability.
4. Maintain reliable and cost-efficient scalability.

A DDoS defense built on these concepts delivers the following protection attributes:

- Enables immediate response to DDoS attacks through integrated detection and blocking mechanisms, even during spoofed attacks when attacker identities and profiles are changing constantly
- Provides more complete verification capabilities than either static router filters or IDS signatures can provide today
- Delivers behavior-based anomaly recognition to detect valid packets sent with malicious intents to flood a service
- Identifies and blocks individual spoofed packets to protect legitimate business transactions
- Offers mechanisms designed to handle the huge volume of DDoS attacks without suffering the same fate as protected resources
- Enables on-demand deployment to protect the network during attacks without introducing a point of failure or imposing the scaling costs of an inline solution
- Processes (with built-in intelligence) only contaminated traffic streams, helping ensure maximum reliability and minimum scaling costs
- Avoids reliance on network device resources or configuration changes
- Uses standard protocols for all communications, helping ensure maximum interoperability and reliability

COMPLETE CISCO SYSTEMS DDOS PROTECTION SOLUTION

Cisco Systems delivers a complete DDoS protection solution based on the principles of detection, diversion, verification, and forwarding to help ensure total protection. When a DDoS attack is launched against a victim protected by the Cisco solution, business continuity is maintained by:

- *Detecting* the DDoS attack
- *Diverting* the data traffic destined for the target device to a Cisco appliance for treatment
- *Analyzing and filtering* the bad traffic flows from the good traffic flows packets, preventing malicious traffic from impacting performance while allowing legitimate transactions to complete
- *Forwarding* the good traffic to maintain business continuity

The Cisco Solution Set

The Cisco solution provides complete protection against all types of DDoS attacks, even those that have never been seen before. Featuring active mitigation capabilities that rapidly detect attacks and separate malicious traffic from legitimate traffic, the Cisco solution delivers a rapid DDoS response that is measured in seconds, not hours. Easily deployed adjacent to critical routers and switches, the Cisco solution offers a scalable option that eliminates any single points of failure and does not impact the performance or reliability of the existing network components.

The Cisco solution set includes two distinct components—the Cisco Traffic Anomaly Detector (TAD) XT and the Cisco Guard XT—that, working together, deliver complete DDoS protection for virtually any environment.

- Cisco Traffic Anomaly Detector XT—Acting as an early warning system, the Cisco TAD XT provides in-depth analysis of the most complex DDoS attacks. The Cisco TAD XT passively monitors network traffic, looking for any deviation from “normal” or baseline behavior that indicates a DDoS attack. When an attack is identified, the Cisco TAD XT alerts the Cisco Guard XT, providing detailed reports as well as specific alerts to quickly react to the threat. For example, the Cisco TAD XT can observe that the rate of UDP packets from a single source IP is out of range, even if overall thresholds are not exceeded.
- Cisco Guard XT—The Cisco Guard XT is the cornerstone of the Cisco DDoS solution set—a high-performance DDoS attack-mitigation device that is deployed upstream at either the ISP data center or at the perimeter of a large enterprise to protect both the network and data center resources.

  When the Cisco Guard XT is notified that a target is under attack (whether from a Cisco TAD XT or some other security-monitoring device such as an intrusion detector or firewall), traffic destined for the target is diverted to the Guard (or Guards) associated with the targeted device. The traffic is then subjected to a rigorous five-stage analysis and filtering process designed to remove all malicious traffic while allowing good packets to continue flowing uninterrupted.

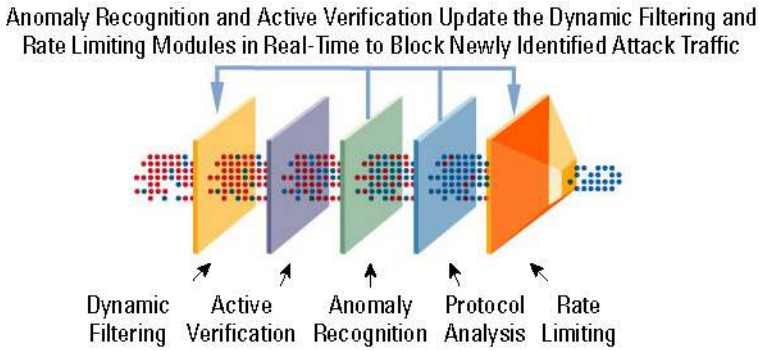
  The Cisco Guard XT resides adjacent to a router or switch on a separate network interface, helping enable on-demand protection without impacting data traffic flow of other systems. Depending on its location, the Cisco Guard XT can concurrently protect multiple potential targets, including routers, Web servers, DNS servers, and LAN and WAN bandwidth.

The Cisco Systems MVP Architecture

The next-generation Cisco Guard XT DDoS defense solution is based on a unique, patent-pending Multiverification Process (MVP) architecture that integrates a variety of verification, analysis, and enforcement techniques to identify and separate malicious traffic from legitimate traffic (refer to Figure 2). This purification process consists of five modules or steps:

- Filtering—This module includes both static and dynamic DDoS filters. Static filters, which block nonessential traffic from reaching the victim under attack, are user-configurable, and they come from Cisco with preset default values. Dynamic filters are inserted by the other modules based on observed behavior and detailed analysis of traffic flows, delivering real-time updates that either increase the level of verification applied to suspicious flows or block sources and flows that have been verified as malicious.

Figure 2
Cisco Systems MVP Architecture



- Active verification—This module verifies that packets entering the system have not been spoofed. The Cisco Guard XT uses numerous unique, patent-pending source-authentication mechanisms to stop spoofed packets from reaching the victim. The active verification module also has several mechanisms to help ensure proper identification of legitimate traffic, virtually eliminating the risk of valid packets being discarded.
- Anomaly recognition—This module monitors all traffic that was not stopped by the filter or the active verification modules and compares it to baseline behavior recorded over time, looking for deviations that would identify the source of malicious packets. The basic principle behind the operation of this module is that the pattern of traffic originating from a "black-hat" daemon residing at a source differs dramatically from the pattern generated by legitimate sources during normal operation. This principle is used to identify the attack source and type, as well as to provide guidelines for blocking traffic or performing more detailed analysis of the suspected data.
- Protocol analysis—This module processes flows that anomaly recognition finds suspicious in order to identify application-specific attacks, such as HTTP error attacks. Protocol analysis then detects any misbehaving protocol transactions, including incomplete transactions or errors.
- Rate limiting—This module provides another enforcement option and prevents misbehaving flows from overwhelming the target while more detailed monitoring is taking place. The module performs per-flow traffic shaping, penalizing sources that consume too many resources (for example, bandwidth or connections) for too long a period.

It is important to note that, between attacks, the Cisco Guard XT is in "learning" mode, passively monitoring traffic patterns and flow for each of the different resources it protects to understand normal behavior and establish a baseline profile. This information is later used to fine-tune policies for recognizing and filtering both known and unknown, never-before-seen attacks in real-time network activity.

CISCO DDOS DEFENSE DEPLOYMENT

Cisco DDoS protection offers flexible, scalable deployment scenarios to protect data centers (servers and network devices), ISP links, and backbones (routers and DNS servers).

Providers

The Cisco Guard XT can be deployed at strategic points in the provider's infrastructure, such as at each peering point, to protect core routers, downstream edge devices, links, and customers (refer to Figure 3). Deployment also can be at the edge router for dedicated customer protection. The detection mechanisms can be near the provider edge or on the customer premises. The scalable Cisco solution for protecting the network itself and multiple customer data centers from upstream deployment supports provider requirements.

Enterprises and Data Centers

In enterprise data centers, the Cisco Guard XT is deployed at the distribution layer in the data center, protecting lower-speed links downstream and the servers. The Cisco Guard XT can be connected to the distribution switch, and it can support a redundant configuration (refer to Figure 4).

Figure 3

Cisco Protection in an ISP Environment. Traffic Destined for Targeted Device Is Diverted to Cisco Guard XTs; Clean Traffic Is Returned to the System.

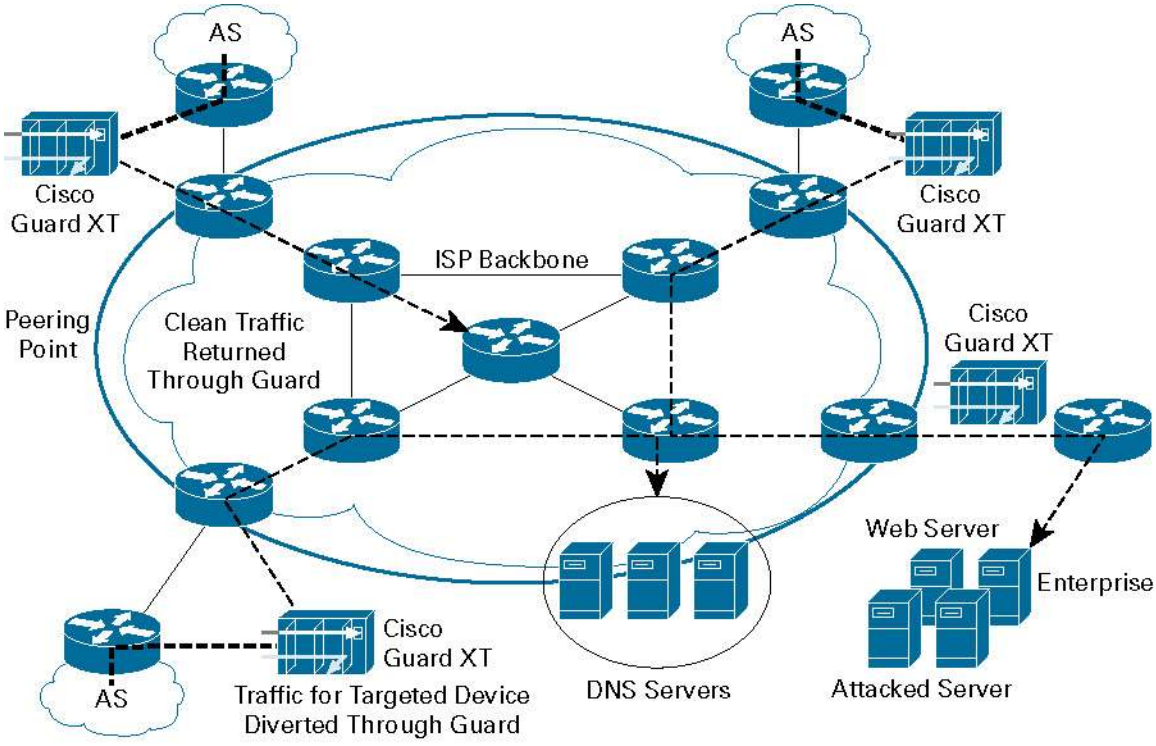
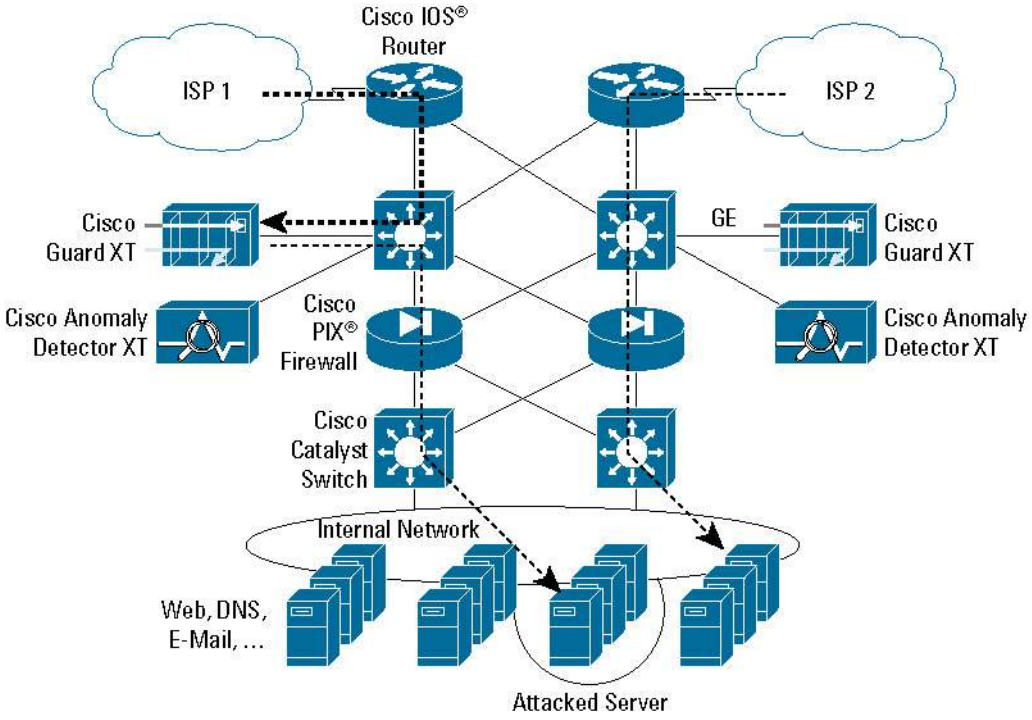


Figure 4

Cisco Protection in an Enterprise Environment. Only Traffic Destined for the Targeted Device Is Diverted to the Cisco Guard XT, Which Returns "Clean" Transactions Back to the System.



CONCLUSION

DDoS attacks will continue to grow in scale and severity thanks to increasingly powerful (and readily available) attack tools, the multiple points of vulnerability of the Internet, and business' increasing dependence on the Internet. As the cost of these attacks rise, providers, enterprises, and governments must respond to protect their investments, revenue, and services.

What is required is a new type of solution that complements existing security solutions such as firewalls and IDSs by not only detecting the most sophisticated DDoS attacks, but also delivering the ability to block increasingly complex and difficult-to-detect attack traffic without impacting legitimate business transactions. Such an approach demands more granular inspection and analysis of attack traffic than today's solutions can provide.

The Cisco Systems technology and architecture delivers an innovative, new approach that subjects traffic to the most detailed scrutiny available today, helping ensure that DDoS attacks fail to achieve their objective of halting business operations. Going beyond simple filtering, the Cisco solution "cleans" data to remove malicious traffic while allowing good packets to pass, helping ensure business continuity and preserving business integrity.

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

BG/LW6616 0604