Q & A

CISCO DDoS PROTECTION SOLUTION

Q. What is a distributed denial of service (DDoS) attack?

A. A denial of service attack is defined as a malicious attempt to deny service to a victim. Some sample targets could be an individual user, a server farm, or a router that carries Internet traffic. When the DoS attack is launched from multiple, compromised sources that are centrally coordinated, the result is an attack with greater size and much larger magnitude of damage inflicted which constitutes a distributed DOS.

To further understand the anatomy of a DDoS attack, refer to:

http://www.cisco.com/en/US/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html.

Q. Why are DDoS attacks growing on the Internet?

A. The motivation behind launching attacks, especially in the case with DDoS, is taking a turn for the worse. In the past, the attacker would create the security threat to gain fame or create havoc. Times have changed where DDoS attacks are now motivated by money and the activity has increased, especially targeting corporations. A typical scenario occurs where a massive attack is launched on a corporation and delivered through the service provider network. The attack can bring operations to a halt for that corporation. A phone call ensues with instructions from the extortionist behind the attack to wire funds into an account or the attacks will continue. Many in the industry who track this criminal activity claim this scenario is becoming more commonplace.

Q. What is impacted by DDoS attacks?

A. The primary effect of DDoS attacks on corporations is service disruption—business downtime leading to customer dissatisfaction and loss of credibility and possibly revenue. The service provider network can be overwhelmed, impacting the ability to deliver connectivity. Even worse, collateral damage can be inflicted on other elements of the network that were not the original target of the attack, but overwhelmed in the process of the attack.

With the growing regulations placed upon corporations, the connectivity required to access data is critical. Any compromise on the ability to exchange data could violate regulations. One such act is the Gramm-Leach-Bliley Act Protection of 1999 which states the need for disaster recovery and business continuity processes to be in place. More regulations are appearing and they imply that corporations and service providers should proactively manage security threats.

Q. What can I do about it?

A. Taking a proactive approach to security is the first step to addressing this problem. Service providers must design an operational process throughout their business to address security. To view a process model, visit:

http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac253/packet_service_provider_solution0900aecd800e015e.html.

If you are a customer of the service provider, call your provider to determine if they support a service to address this problem. To address the DDoS threat, Cisco Systems® has created a DDoS Protection solution.

Q. What is the Cisco® DDoS Protection solution?

A. The Cisco DDoS Protection solution delivers a set of system architectures validated by Cisco, with market-proven implementations. The solution integrates industry-leading Cisco 12000, 10000, 7600, 7500, and 7200 Series routers with the Cisco Guard and the Cisco Traffic Anomaly Detector product lines to form a defense system that proactively detects and mitigates DDoS anomalies. The Guard and Detector both use network behavior analysis to identify and mitigate DDoS attacks. The Cisco Traffic Anomaly Detector provides precise anomaly tracking and Cisco Guard provides detailed, scalable, and granular scrubbing of the traffic anomalies. Based on an alert from a Detector, the Guard provides flow-based analysis and mitigation to distinguish between legitimate sources and malicious sources. The Cisco Guard provides scalable, real-time, and granular scrubbing of the traffic anomalies. The Cisco routers use the NetFlow feature in Cisco IOS® Software to monitor trends in the network. Netflow data used in conjunction with Arbor Networks, a Cisco Technology Developer Program (CTDP) Partner, empowers service providers with the knowledge they need to manage security attacks when they arise.

Q. What are "clean pipes" capabilities?

A. "Clean pipes" is a phrase used to describe the capability of delivering data connections and services unhindered by security threats. The goal is to remove the malicious traffic from the data pipe and only deliver the legitimate traffic. The major threats impacting the carriers today include DDoS, worms, and viruses, but the threats are evolving on a daily basis. The attributes of clean pipes help deliver information along the pipe removed of the threat and alleviates the bandwidth saturation which creates the choke point leaving the data pipe vulnerable.

Q. What steps are required in the Cisco DDoS Protection solution?

A. There are several critical steps required in the solution:

1. **Detection**—The process to identify an anomaly can take place in the network or at the customer premises. The detection involves identifying the type of attack and the source of the attack. When the attack is detected, the Guard gets notified through an out-of-band connection to ensure that the alarms are received. A service provider with greater visibility into its network and its customers' networks can detect anomalies more precisely. To achieve this visibility, the Cisco Traffic Anomaly Detector learns normal traffic flows on the customers' network, so it can quickly identify abnormal behavior.

2. **Mitigation**—This critical step in the process precisely removes the malicious traffic. The Cisco Guard delivers very detailed and granular traffic analysis that facilitates per-flow analysis and blocking. The mitigation process is very rapid with unnoticeable packet delay and is highly scalable to withstand the largest attacks. The learning process during peacetime gives the mitigation process much greater accuracy.

3. **Diversion and Injection**—When the attack has been detected, the dirty traffic (both legitimate and malicious) is to be diverted to a scrubbing center where the Guard performs the mitigation process to remove anomalies. When the anomalies are removed, the legitimate traffic is injected back into the network toward the original destination. There are many forms of diversion and injection designed in the Cisco solution to support Layer 2 and Layer 3 networks and IP/Multiprotocol Label Switching (MPLS) networks.

Q. What are the service models for the Cisco DDoS Protection solution?

A. The service models are as follows:

- **Managed Network DDoS Protection**—Helps enable service providers to offer their customers effective protection against DDoS attacks on their last-mile connections and internal infrastructure
- **Managed Hosting DDoS Protection**—Helps enable hosting providers to protect their Web hosting and other hosting services from DDoS attacks
- **Peering Edge DDoS Protection**—Helps enable service providers to provide DDoS-free wholesale connections to their ISP customers
- **Infrastructure DDoS Protection**–Helps enable a service provider to protect their own network assets from the impacts of DDoS to maintain availability and service delivery.

Q. What are the products that make up the Cisco DDoS Protection solution?

A. The following products make up the Cisco DDoS Protection solution:

- The Cisco IOS® NetFlow feature, supported on Cisco devices including Cisco CRS-1, 12000, 10000, 7600, 7500, and 7200 Series routers focuse on network telemetry in the service provider network.
- Leading Network Foundation Protection (NFP) security features found on Cisco routers. Refer to www.cisco.com/go/nfp for more information.
- The Cisco Traffic Anomaly Detector XT 5600 appliance and the new Cisco Traffic Anomaly Detector Module for the Cisco 7600 Series Router and Cisco Catalyst® 6500 Series Switch.
- The Cisco Guard XT 5650 appliance and the new Cisco Anomaly Guard Module for the Cisco 7600 Series Router and Cisco Catalyst 6500 Series Switch for anomaly mitigation are highly scalable to provide anomaly mitigation for the largest attacks.
- Arbor Networks' Peakflow SP option for networkwide monitoring and detection. Arbor Networks is a Cisco Technology Developer Program Partner and provides a solution that monitors NetFlow data from Cisco devices for detecting DDoS attacks in the provider network and alerting the Cisco Guard-based scrubbing centers.

Q. What are the benefits of the Cisco DDoS Protection solution?

A. The Cisco DDoS Protection solution includes the following attributes:

- **Scalable**–Mitigation tools have high performance as well as mitigation capacity to grow and cope with the increasing size of the DDoS attacks.
- **Resilient** –The system architecture delivers a highly reliable, distributed design to troubleshoot unforeseeable fault situations that may occur. Devices are easily brought inline when necessary and removed just as easily.
- **Economical**–Supports multiple deployment models to offer a "pay-as-you-grow" structure to meet your customers' requirements.
- **Flexible**–The system design meets rigorous requirements on topological and operational models that best serve the customer.

Q. Who has deployed DDoS protection today?

A. The following global service providers are amongst those that have launched their offering of DDoS protection services to their customers:

- AT&T—Internet Protect
- Sprint—IP Defender
- MCI—WAN Defense
- COLT—IP Guardian
- Rackspace—PrevenTier DDoS Mitigation Service
- Datapipe—SureArmour DDoS Protection Service

Q. What is the greatest impact of DDoS on the service provider, enterprise, small and medium-sized business (SMB), and consumer?

A. Service providers risk a potentially huge impact on connectivity to their end users. Loss of connectivity translates to loss of revenue. The Cisco DDoS Protection solution can protect their infrastructure and enable new security service offerings to their customers.

The enterprise, SMB, and consumer markets have been increasing their dependence on the service provider to do business, to gain access to entertainment, and to conduct multiple forms of communication. Blockage of the connectivity from a DDoS event impacts day-to-day operations. Having a service from the carrier to alleviate these worries and achieve a DDoS-free environment helps maintain the connectivity they need and expect.

Q. Why is the service provider best suited to deal with DDoS attacks?

A. A primary reason is that service providers own the data connections that exchange Internet traffic from peering points and broadband subscribers. These places in the network are the primary sources for DDoS attacks that target a specific destination, usually a corporation. The best prevention is to mitigate the attack closest to the source of origination to reduce traffic impacts across the network. A secondary reason is the likelihood to saturate the last-mile bandwidth between the service provider and the customer. So while the customer might protect its own assets by placing a mitigation device on its own facility, the choke point becomes the connectivity between the service provider and the customer. For these reasons and more, the service provider is best suited to deliver a DDoS protection service.

The enterprise can still maintain control of the situation. By placing an anomaly detector on the customer premises, the enterprise gains visibility into the traffic patterns and attacks that happen on its network. Also, the enterprise can decide when to activate mitigation through the Guard scrubbing centers and notify the service provider at those times.

Q. Where can I get more information about the Cisco DDoS Protection solution?

A. For more information about the Cisco DDoS Protection solution, visit: http://www.cisco.com/go/cleanpipes.

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

Printed in USA