WHITE PAPER

DISTRIBUTED DENIAL OF SERVICE THREATS: RISKS, MITIGATION, AND BEST PRACTICES

Protecting network resources against distributed denial of service (DDoS) attacks is no longer just a concern of companies with high-profile Websites. In fact, Gartner predicts that a full 50 percent of companies without effective mitigation strategies will suffer financial or service loss as a result of botnet attacks by 2007.* In addition to downtime and productivity loss, risks include loss of top-line revenue from Web services, theft of information while IT groups are distracted, and stock price manipulation.

Traditional mitigation solutions such as intrusion prevention systems (IPSs) effectively protect individual servers and subnets from malicious application-layer attacks. However, they do not protect the upstream link, which can be saturated with attack traffic, or even fail completely under the load of a bandwidth-intensive DDoS attack. In this situation, all or most legitimate traffic is blocked even though the services are technically available.

The Cisco® Guard solution mitigates the risk of DDoS attacks by protecting not only individual servers, but also their upstream links. The solution has two parts. The Cisco Traffic Anomaly Detector constantly analyzes traffic destined to protected resources in order to identify anomalous traffic patterns. When an attack is detected, traffic is diverted to the Cisco Anomaly Guard, which applies various mechanisms to drop malicious traffic *while allowing legitimate traffic to pass through to the protected resource that has come under attack*.

IT groups can choose from several deployment options for the Cisco Guard solution. Companies that want the most possible control of the solution can deploy it on premises. However, they need a sufficiently large link between the service provider and the data center to carry both malicious and legitimate traffic. The question for some is, “Is it worth it to pay for a larger pipe to transport malicious traffic, only to drop it at the network edge?” Other companies choose a managed service, if available. In this scenario, the Cisco Guard is deployed within the service provider network, and anomaly detection can occur either on premises or within the service provider network. With a managed service, only legitimate traffic—no DDoS traffic—travels across the service provider link to the data center.

This white paper is intended for enterprise IT professionals. It describes the value of the Cisco Guard solution for DDoS mitigation. It begins by explaining the risks of DDoS attacks and the unique demands of DDoS mitigation. Next, it describes how the Cisco Guard solution works. The paper concludes with deployment considerations, including operational planning and whether an in-house deployment or managed service is better for a given organization.

* Gartner, “Protect Your PCs and Servers from the Botnet Threat,” December 29, 2004

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

WHAT HAPPENS DURING A DDoS ATTACK

During a DDoS attack, multiple hosts send legitimate requests, with malicious intent, for service to a single target. Any resource connected to the Internet can be a target, including DNS servers, e-mail services, online applications, or router interfaces. In the worst case, faced with an onslaught of requests, either the Web server or its upstream router fails and all traffic stops. More often, the link and equipment become saturated, allowing passage to only a portion of traffic—some from legitimate users, some malicious.

Risks of DDoS attacks include:

- **Downtime and productivity loss**.
- **Top-line revenue loss from sales and support services during the outage**. Companies that stand to lose the most from a DDoS attack use their Websites for commerce, vital support services, or the core business, such as a news service or search engine.
- **Damage to company reputation resulting in long-term revenue loss**. If a customer uses a competitor's Website during its preferred supplier's DDoS-related outage, the customer might transfer his or her loyalty to the competitor, resulting in ongoing revenue loss.
- **Theft of information**—Hackers sometimes launch DDoS attacks as a diversion while they snoop through confidential customer or company information, such as credit card numbers or intellectual property.
- **Extortion**—The attacker offers to stop (or not initiate) a DDoS attack for a cash payment. Originally directed against offshore gaming companies, extortion attempts have more recently spread to Fortune 500 companies.**
- **Stock price manipulation**—For certain types of businesses, an unavailable Website sends the stock price down. Attackers sometimes launch a DDoS attack in order to profit from day trading.
- **Malicious competition**—In one recent case, a brick-and-mortar retail establishment hired a computer consultant to launch a DDoS attack against an online competitor

* NetworkWorld, "Extortion via DDoS on the Rise," May 16, 2005

MULTILAYERED APPROACH TO DDoS MITIGATION

Cisco Systems® offers multiple technologies for DDoS mitigation, providing defense in-depth. These include Cisco Security Agent, Cisco Intrusion Prevention System (IPS), Cisco routers, and Cisco Guard. Each has a role in DDoS mitigation.

Cisco Security Agent

Installed on a Web server, Cisco Security Agent can limit the number of connections that any one client can attempt. DDoS attacks can involve more than 200 connections per minute, while a legitimate client typically initiates just a few per minute. If a company specifies that a single client should not attempt to connect more than 15 times a minute, for example, the 16th and subsequent attempts are refused until the timer expires. In this way, Cisco Security Agent slows down DDoS attacks to the degree that they do not prevent the processing of legitimate traffic.

While Cisco Security Agent effectively protects individual servers from malicious attacks, it does not protect the upstream link. And if the upstream link is saturated, traffic cannot pass through to the servers. Organizations can augment the Cisco Security Agent by using the Cisco Guard solution, discussed later in this paper, to protect upstream links and devices.

Cisco Intrusion Prevention System

Deployed on a subnet, a Cisco Intrusion Prevention System (IPS) can mitigate DDoS threats downstream from the sensing device. It recognizes various flood signatures and then automatically executes the response that IT has specified for that signature. Actions include resetting the connection, dropping packets at the sensor so they do not reach the intended target, or modifying the access control list (ACL) on the edge router or switch near the affected area. The IPS can also create a rate-limiting policy on the edge router. For example, upon detecting a SYN flood attack, the IPS device can define a policy in the router that that limits the number of SYN packets forwarded, thereby decreasing the load on the internal network and targeted device.

Like Cisco Security Agent, Cisco IPS protects the subnet and its hosts from many malicious threats but cannot completely eliminate the impact of many of today's sophisticated DDoS attacks.

Cisco Routers

Cisco routers at the network edge help mitigate certain types of DDoS attacks by using ACLs, blackhole routing, rate limiting, and traffic-flow reporting:

- ACLs coarsely filter traffic that is clearly unwanted, such as traffic that spoofs the company addresses or is destined for Windows control ports. When DDoS attacks originate from a broad range of spoofed addresses, however, ACLs alone cannot prevent a large-scale DDoS attack because of the large number of addresses involved and the inability to distinguish between legitimate and malicious users. ACLs also lack the sophistication to deal with network address translation (NAT). If multiple people at a single NATed site try to access resources, all traffic might appear to come from the same address.
- Blackholing can effectively block all traffic from a given source or destined to a given address. However, it cannot distinguish between bad and good traffic in cases when Web traffic from the source is good but DNS traffic is bad, for example.
- Rate limiting is effective in reducing the impact of DDoS attacks but not in eliminating the threat entirely.
- Traffic-flow reporting entails an ongoing comparison of network traffic with the normal network baseline.

Traffic-flow reporting is available through Cisco NetFlow technology, which collects information about traffic flows and then sends it to a threat-detection correlation tool for anomaly detection. The industry's most widely deployed DoS identification and network traffic flow analysis technology, Cisco NetFlow is available in hardware, Cisco IOS® Software, and Cisco Catalyst® Operating System Software.

Cisco NetFlow classifies packets according to flows, where each flow is defined by seven unique characteristics: the ingress interface, IP protocol type, type-of-service (ToS) byte, source and destination IP addresses, and source and destination port numbers. These characteristics provide enough data to create a baseline profile of normal traffic patterns. By producing detailed accounting of traffic flows, Cisco NetFlow allows IT users to identify deviations from typical traffic patterns, an early sign of potential DDoS attacks.

Cisco NetFlow is usually deployed at the network edge and can also be implemented by service providers to monitor edge and peer interfaces, which are the typical ingress points for most attacks. The router maintains a live Cisco IOS NetFlow cache to track the current flows. Companies can export IP flow information from the cache to an external collector for further analysis. Analysis of this exported data helps administrators determine the threat classification and apply appropriate mitigation techniques available in Cisco IOS Software, such as ingress ACLs, Network-Based Application Recognition (NBAR), and Unicast Reverse Path Forwarding (uRPF).

To analyze Cisco NetFlow data, companies can use freeware tools such as cflowd, flow-tools, and autofocus. In addition, vendors such as Arbor Networks provide a GUI-based collector application tool for large-scale data collection, analysis for DoS and DDoS attack detection, and centralized reporting. When Arbor Networks Peakflow software detects an anomaly in its analysis of Cisco NetFlow statistics, it can signal the Cisco Anomaly Guard to "scrub" malicious traffic. For more information on the traffic classification and identification capabilities integrated into Cisco IOS Software, visit http://www.cisco.com/web/about/ac123/ac114/about_cisco_packet_issues_list.html.

CISCO DDoS MITIGATION SOLUTION: CISCO GUARD

The Cisco Guard solution complements, rather than replaces, ACLs, firewalls, remote-triggered blackholes, traffic-flow reporting, IPSs, and other tools for policy enforcement and mitigation. It protects not only the targeted server and its subnet, but also all upstream bandwidth between the Cisco Guard and the targeted host. Designed specifically to protect resources with high business value against DDoS attacks, Cisco Guard allows legitimate traffic to pass, blocks malicious traffic, and prevents downstream resources from being overwhelmed with malicious traffic. The Cisco Guard is not an inline solution that remains always on. Instead, it is a diversion-based, on-demand solution.

Proactive Mitigation At a Glance

The Cisco Guard solution for DDoS protection consists of two components: the Cisco Traffic Anomaly Detector and the Cisco Anomaly Guard (Figure1). Both are available as appliances or as modules for Cisco Catalyst 6500 Series switches or Cisco 7600 Series routers. When the Cisco DDoS solution is first deployed, an administrator creates a behavior profile of normal traffic—a process called learning. The company uses its applications as usual for 24 hours to one week, and application traffic runs through the Cisco Traffic Anomaly Detector. During the learning period, the Traffic Anomaly Detector collects baseline information to understand the normal operation of the network, including:

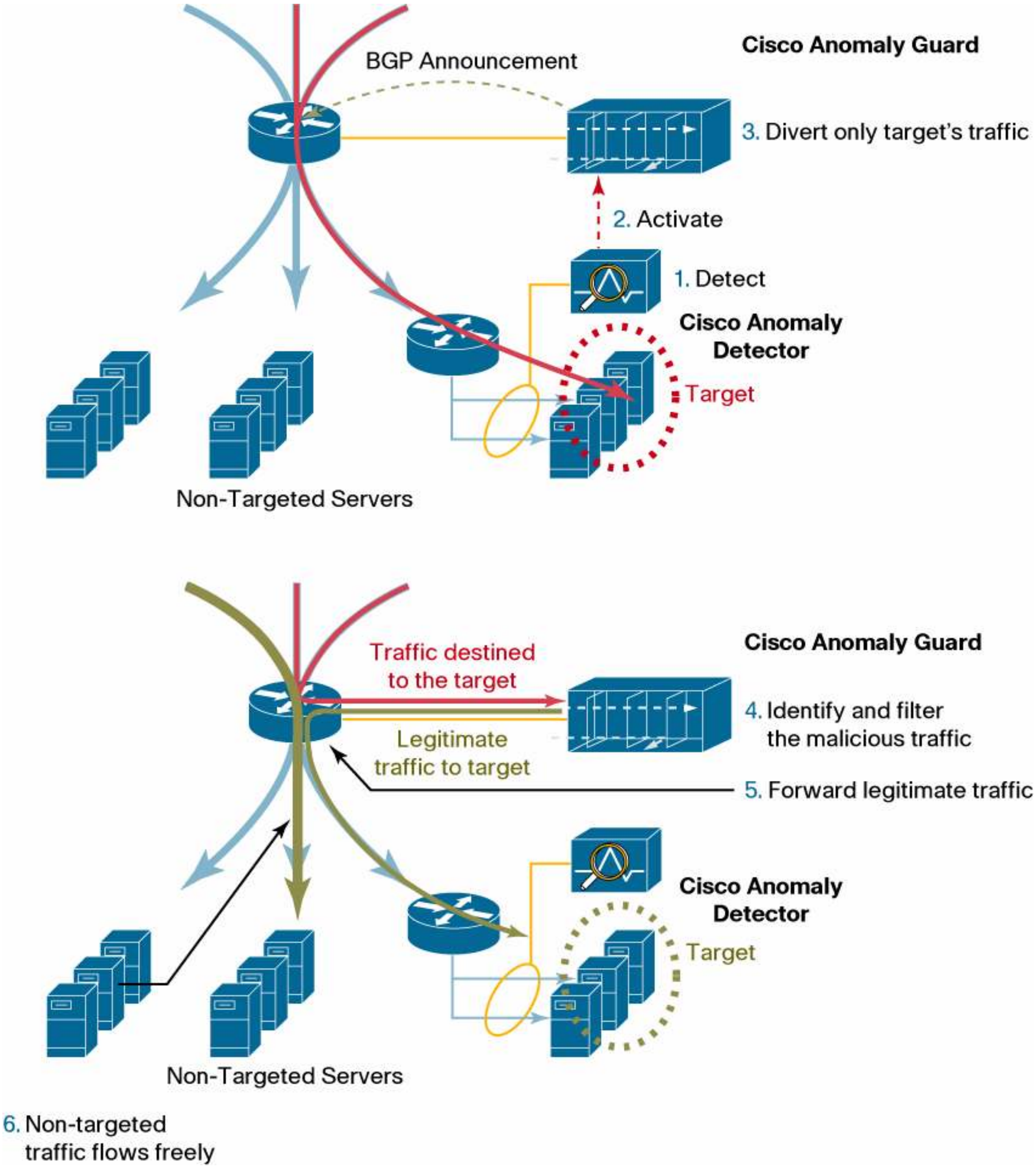
- Packet rates for each type of packet, measured in packets per second (pps)
- Packet ratios, such as the ratio of SYN packets to FIN packets
- The number of simultaneous TCP connections opened by a single source

Baseline information is collected for each destination host address, destination subnet, source host address, and source subnet.

After the learning period, the Cisco Traffic Anomaly Detector is placed in monitoring mode and the Cisco Anomaly Guard in standby mode. As long as no attack is in progress, inbound traffic from the Internet flows through the switch without any involvement from the Cisco Anomaly Guard. A copy of inbound traffic is sent to the Cisco Traffic Anomaly Detector for analysis via a Switched Port Analyzer (SPAN) or virtual ACLs. If the Cisco Traffic Anomaly Detector identifies anomalous traffic behavior compared to the baseline, the mitigation process begins:

- The Cisco Traffic Anomaly Detector commands the Cisco Anomaly Guard to start the diversion process.
- The Anomaly Guard then diverts (“hijacks”) traffic destined for the IP address under attack to itself.
- The Anomaly Guard subjects the traffic to multiple layers of analysis and countermeasures to distinguish legitimate sources from attack sources, a process called cleaning or scrubbing.
- The Anomaly Guard drops the attack traffic and forwards the legitimate traffic back into the normal traffic path to the target, a process called injection.

Figure 1. The Cisco Guard Solution


Cisco Anomaly Guard
BGP Announcement
3. Divert only target's traffic
2. Activate
1. Detect
Cisco Anomaly Detector
Target
Non-Targeted Servers
Cisco Anomaly Guard
Traffic destined to the target
4. Identify and filter the malicious traffic
Legitimate traffic to target
5. Forward legitimate traffic
Cisco Anomaly Detector
Target
Non-Targeted Servers
6. Non-targeted traffic flows freely

Cisco Traffic Anomaly Detector

The Cisco Traffic Anomaly Detector is a passive monitoring device that constantly looks for indications of a DDoS attack against a protected destination, also called a zone, such as a server, firewall interface, or router interface. The Cisco Traffic Anomaly Detector analyzes copies of all inbound traffic destined for the protected zones via SPAN or a passive network tap. This analysis involves comparing the current traffic behavior to the baseline thresholds, also called a zone policy, to detect anomalous traffic behavior. If anomalous behavior is seen and appears to be a possible attack, the Cisco Traffic Anomaly Detector signals the Cisco Anomaly Guard via an out-of-band Ethernet management network to begin analysis and mitigation of the attack.

Cisco Anomaly Guard

The Cisco Anomaly Guard is a self-contained traffic analysis and filtering device. When it begins receiving traffic destined for a particular zone that appears to be under attack, it conducts a rigorous analysis of that traffic. If analysis confirms that the traffic is malicious, the Cisco Anomaly Guard applies countermeasures such as anti-spoofing mechanisms and various levels of filtering (Table 1). The end result is that traffic from malicious sources is dropped, while traffic from legitimate sources is forwarded to the intended destination.

DDoS Attacks Detected and Mitigated

Table 1 lists the types of DDoS attacks that the Cisco Guard solution detects and mitigates.

Table 1. Categories and Specific Types of DDoS Attacks

Attack Category	Specific Types of Attacks
Bandwidth Consumption Attacks	Spoofed and non-spoofed flood attacks: □ TCP Flag (SYN, SYN-ACK, ACK, FIN) □ Internet Control Message Protocol (ICMP) □ User Datagram Protocol (UDP) Examples include SYN flood, smurf, LAND, and UDP flood attacks.
	Zombie/botnet attacks, in which each zombie or bot source opens multiple TCP connections, and sometimes issues repetitive HTTP requests.
	DNS attacks, such as DNS request flood.
Resource Starvation Attacks	Packet size attacks, characterized by fragmented or large packets. Examples include teardrop and ping-of-death.
	Low-rate zombie/botnet attacks, which are similar to bandwidth consumption attacks except that each attack source sends multiple requests at a low rate.
	DNS attacks, with DNS recursive lookup.

For a comprehensive description of DDoS attacks, see “The Internet Protocol Journal” at: http://www.cisco.com/en/US/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html

Traffic Diversion Options

IT groups can select from the following options for traffic diversion from the upstream network to the Cisco Anomaly Guard, a process also called traffic hijacking:

- Border Gateway Protocol (BGP) announcements from the Cisco Anomaly Guard to upstream routers, stating that traffic to the protected destination will be routed instead to the Cisco Anomaly Guard.
- Use of external traffic diversion mechanisms such as remote BGP update routers.
- Route Health Injection (RHI) announcements from Cisco Anomaly Guard to the routing process of the Cisco Catalyst 6500 Series or Cisco 7600 Series supervisor engine. These announcements place a static route in the global routing table that points to the Cisco Anomaly Guard module as the next hop.

Traffic Injection Options

Traffic injection is the process that Cisco Anomaly Guard uses to forward cleaned, legitimate traffic to the destination under attack. The Cisco Guard solution supports multiple traffic injection options. In the Layer 2 topology option, cleaned traffic is forwarded from Cisco Anomaly Guard to a statically configured, next-hop address that resides on a downstream router attached to the same VLAN or subnet as the Cisco Guard traffic injection interface/VLAN. Layer 2 traffic injection is the simplest to configure because it does not require any significant configuration changes on the downstream router.

Layer 3 topology options for traffic injection include:

- VPN Routing and Forwarding (VRF)
- Policy-Based Routing (PBR)
- VLAN Trunking
- Generic Routing Encapsulation (GRE) or IP Encapsulation Within IP (IPIP) Tunnel

Results: False Positives, False Negatives

Attacks That the Cisco Guard Stops

The Cisco Guard intercepts and stops more than 95 percent of malicious traffic. The few false negatives have little potential for harm because legitimate, non-malware packets, such as the SYN packets commonly used in DDoS attacks, cause little or no damage. Note that malware packets or application-layer exploits, which can cause damage, can be stopped by the Cisco IPS.

Why the Cisco Guard Does Not Stop Legitimate Packets

The Cisco Guard affects less than five percent of legitimate traffic—a lower false-positive rate than typical of intrusion detection systems (IDSs) or other signature-based solutions. The reason for the low false-positive rate is that the Cisco Guard solution subjects individual sources to multiple levels of inspection before classifying them as malicious DDoS sources. Types of inspection include:

- Per-destination analysis
- Anti-spoofing engaged based on per-destination analysis
- Per-source analysis
- Source-based drop filters engaged based on per-source analysis

DEPLOYMENT OPTIONS

Organizations can deploy the Cisco Guard solution entirely on premises, entirely at the service provider location, or with the Cisco Traffic Anomaly Detector on premises and the Cisco Anomaly Guard at the service provider (Table 2).

Table 2. Comparing Cisco Guard Deployment Options

Deployment Option	Advantages	Disadvantages
In-House	□ Provides IT with the most control. □ Is the only option available if service provider does not offer a managed service.	□ Link to service provider must be large enough to carry both malicious and legitimate traffic during a DDoS attack. □ IT staff must be available 24x7.
Managed Service: Cisco Traffic Anomaly Detector on Customer Premises	□ Protects service provider link in addition to data center bandwidth and resources. □ Enables IT to monitor its own traffic. □ Provides access to experts at service provider, available 24x7.	□ More complex—provider equipment must communicate with Cisco Traffic Anomaly Detector module at the data center.
Managed Service: Cisco Traffic Anomaly Detector at Service Provider Point of	□ Protects service provider link in addition to data center bandwidth and resources. □ Provides access to experts at service provider, available 24x7. □ Avoids communication between Cisco Guard	□ IT cannot monitor traffic because Cisco Traffic Anomaly Detector is offsite.

Deployment Option	Advantages	Disadvantages
Presence (POP)	components at POP and data center.	

In-House Deployment Considerations and Best Practices

Companies that deploy the Cisco Guard solution at the data center typically install both the Cisco Anomaly Guard and Cisco Traffic Anomaly Detector in a Cisco Catalyst 6500 Series switch that is the first point of entry for inbound Internet traffic.

The Cisco Guard can only protect the upstream link if it is deployed in the service provider network. Therefore, before deciding to deploy the Cisco Guard solution on-premises, the IT group must determine if the link from the data center to the service provider has sufficient capacity to withstand a DDoS attack. The link to the service provider is typically low-bandwidth, and is therefore especially vulnerable to DDoS attacks. Many Fortune 500 companies, for example, rely on multiple DS-3 links (45 Mbps) to create a link of 200 Mbps. DDoS attacks, which range from sub-gigabit to multi-gigabit, can quickly saturate or bring down these links. Cisco recommends 500 Mbps minimum for in-house deployments, with 1 GB preferred. However, certain organizations might conclude that a lower-capacity link to the service provider is adequate for their business needs.

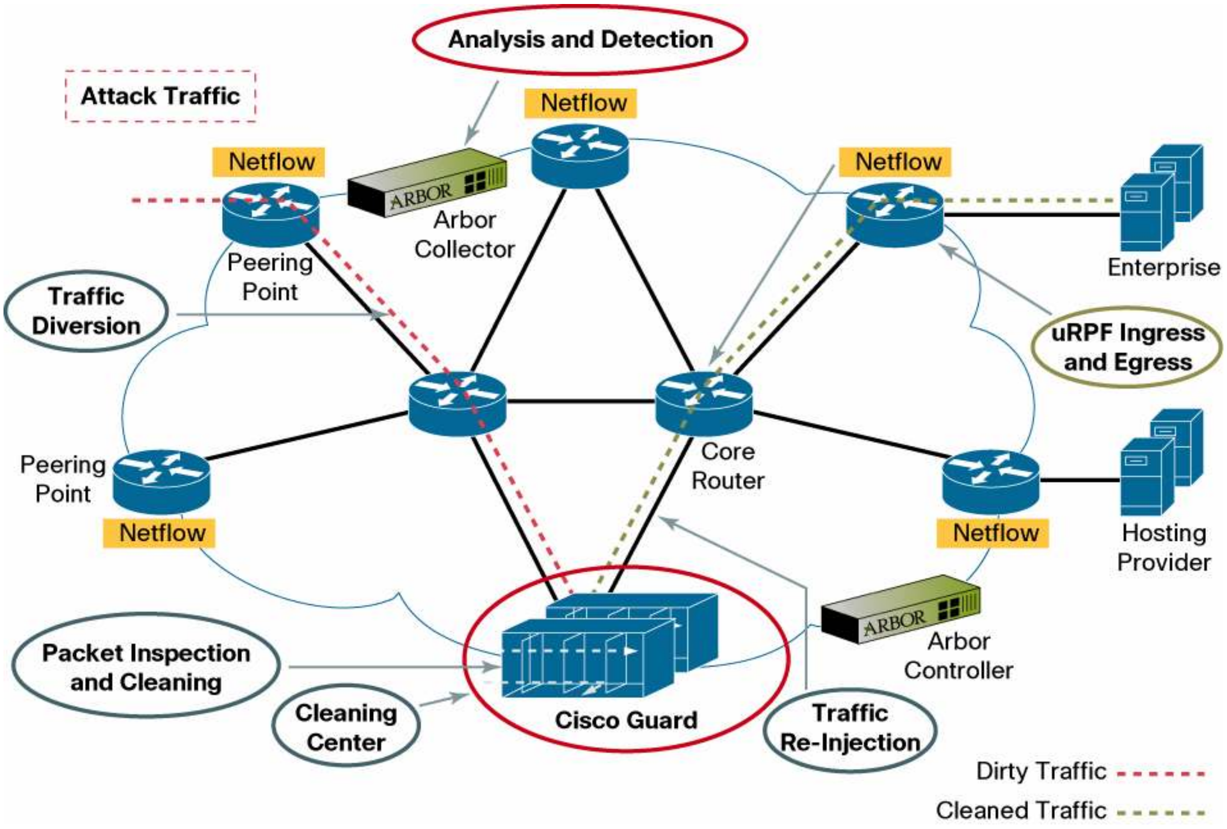
Other best practices for in-house deployments are:

- Consider the business risk of loss of service when determining incoming bandwidth requirements. If the attack does not exceed available bandwidth, the Cisco Anomaly Guard lets in all legitimate traffic. If the attack exceeds available bandwidth, the Anomaly Guard only cleans traffic that makes it past the congested link. This traffic could contain no legitimate traffic or very little, making the Anomaly Guard less effective as a DDoS traffic scrubber.
- Be sure that the upstream devices used to divert traffic to the Cisco Anomaly Guard can handle the attack volume. Use Cisco Catalyst 6500 Series switches or Cisco 7600 Series routers. Do not use Cisco 7200 Series routers for this purpose.
- Deploy the Cisco Anomaly Guard as close to the edge as possible. The Anomaly Guard only protects what is behind it. Therefore, deploy it far enough upstream to drop the attack traffic before it can saturate network infrastructure components such as firewalls, IPSs, switches, and routers.

Managed Service: In-Network DDoS Mitigation

Certain service providers offer DDoS protection as a managed service to complement their Internet connectivity service offerings. In a managed service, the Cisco Anomaly Guard is deployed in the service provider network to clean malicious traffic. The service provider uses Arbor Peakflow software to analyze Cisco NetFlow traffic from the routers. Upon detecting anomalous traffic, the Arbor Peakflow system redirects the offending traffic to the Cisco Guard, which scrubs the attack traffic and then forwards the cleaned traffic to its destination (Figure 2).

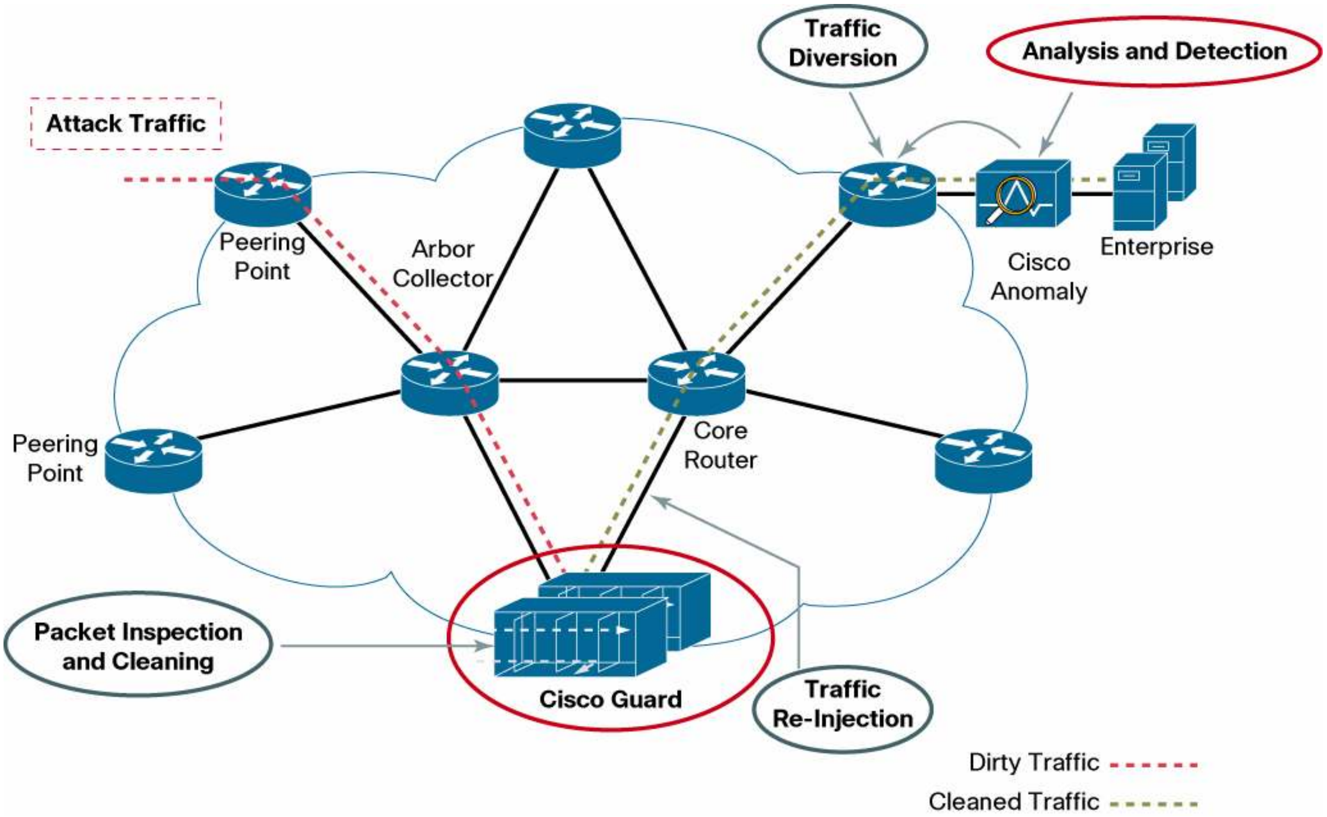
Figure 2. Managed Service Using Cisco NetFlow, Arbor Peakflow, and the Cisco Guard



Managed Service: Cisco Traffic Anomaly Detector at the Customer Premise

Many service providers realize that enterprises do not have the bandwidth necessary to withstand a large scale DDoS attack but want more control over the detection of an attack targeted at their critical resources. Either the service provider or the enterprise can install a Cisco Anomaly Detector at the enterprise location to monitor and analyze the traffic destined to enterprise resources. Upon detecting an attack, the Cisco Anomaly Detector can redirect the traffic stream to the Cisco Guard hosted at the service provider facility. The Cisco Guard eliminates the malicious traffic and forwards legitimate the legitimate data back to the enterprise resources (Figure 3).

Figure 3. Managed Service, with Cisco Traffic Anomaly Detector at Customer Premise



PREVENTING OUTBOUND DDoS

Malware, including viruses, worms, and spyware, can corrupt desktops or servers so that they generate malicious outbound traffic. Typically, the user is unaware that someone else is using the desktop or server to perpetrate an attack. While outbound DDoS does not threaten revenue, it is an embarrassment and potential liability that IT groups should take due diligence to avoid.

Cisco Systems offers several technologies at different levels of the network to help prevent companies from unwitting participation in outbound DDoS attacks. For example, Cisco Intrusion Detection Systems deployed on a subnet, mitigates against DDoS threats downstream from the sensing device, including outbound DDoS attacks.

Similarly, Cisco Security Agent can prevent malware from being installed on desktops or servers. One type of malware, zombie programs, causes a computer to participate in a DDoS attack against a target outside the company. Another type of malware, spyware, produces what amounts to a DoS attack against the system on which it resides—it slows down the computer to the extent that it becomes unusable. Cisco Security Agent prevents all types of malware from being installed on a desktop without the user’s explicit permission.

OPERATIONAL PLANNING

This section of the white paper provides the decisions and actions that Cisco advises IT groups to make prior to deploying the Cisco Guard solution.

Management Considerations

Security management is an important factor in a company's ability to detect and prevent threats to the network and valuable resources. To be effective, security management must provide visibility into the state of the end-to-end security solution, gather and analyze information in real-time and provide the response necessary to quickly mitigate the threat. The Cisco Security Monitoring, Analysis and Response System (CS-MARS) aggregates information about security incidents from hosts, network devices, firewalls, and IPS devices. Alerts and logs from multiple sources, including NetFlow, are correlated and analyzed in real time resulting in a definition of the anomalous behavior, allowing immediate verification and response.

By utilizing the discovered network device topology and device configuration information, attackers are identified to the level of MAC address, workstation and user name, etc. and the full attack path from the source to the destination is mapped. CS-MARS dashboard dynamically presents prioritized incidents with full drill-down investigation capability. Operators can readily identify, examine, investigate, exclude and respond to incidents at the push of a button. Graphic presentation includes network attack hotspots, enterprise visualization, prioritized incidents with attack path details and replay, as well as full incident disclosure (consisting of depicting associated rules, the raw event data and the correlation that caused the incident to fire). Incidents range from known sequence of common attacks and company-specific watch lists to correlated anomalous network behavior exhibited by existing and day-zero worms and network management issues.

Ensuring That Routers Remain Operational During an Attack

A router can be a direct target of an attack or can suffer collateral damage. If a router fails during a DDoS attack, users cannot access Web, DNS, or e-mail servers, even if they are technically available. Therefore, IT groups need to take special care to protect routers associated with the services that the Cisco Guard solution protects.

The following precautions help ensure that the network infrastructure remains operational and available during DDoS attacks:

- Deploy an appropriate router in vulnerable positions. Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers, used with a Supervisor Engine 720, provide hardware-based rate limiting.
- Deploy the Control Plane Policing feature to protect the control plane based on policies for acceptable traffic types according to sender, receiver, protocol, and more. Control plane policing is performed in hardware to not drain processing resources during a DDoS attack.
- Ensure use of best practices for end-to-end defense in depth.

Defining Zones on the Cisco Anomaly Guard and Cisco Traffic Anomaly Detector

First define the entities needing protection: destination IP addresses for servers, other hosts, router interfaces, and firewall interfaces. Next, create zones of destinations and entities that exhibit similar behavior. Companies with high bandwidth usage or variable usage generally classify entities by their activity, such as all Web servers. Companies with low total bandwidth can group unlike entities—for example, Web, e-mail, and DNS servers—with similar bandwidth usage, such as "10 to 100 Mbps" or "more than 100 Mbps." The more similar the behavior of entities in a group, the easier it is to detect anomalous behavior. A zone can contain from 1 to 100 destination IP addresses.

Planning Packet-Processing Capacity

Each Cisco Anomaly Guard can process up to one million 64-byte packets per second. Companies with very high bandwidth requirements can cluster up to eight Cisco Anomaly Guard modules using Cisco Express Forwarding-based load sharing. This provides a capacity of up to 8 Mpps/8 Gbps for processing zone traffic.

Planning Zone Capacity

Each Cisco Anomaly Guard accepts up to 500 zones, with 30 protected simultaneously. Deploy the needed number of Cisco Anomaly Guards.

Deciding How Often to Change Baseline Zone Policies

Each zone has a baseline policy that defines normal behavior. Companies should periodically redefine the policy. The frequency depends on two factors:

- **Variability of traffic behavior**. Companies whose traffic behavior changes weekly or monthly should consider relearning at this frequency. If traffic behavior is static, less frequent changes are needed.
- **Addition of new applications**. After deploying a new application, IT should capture normal application behavior for 24 hours to one week so that the Cisco Traffic Anomaly Detector can later identify anomalous application behavior.

IT groups can change the baseline policy either by placing the zone in learning mode or by manually tuning thresholds. Generally, manual tuning is used only when an attacker is continually adjusting a DDoS attack based on the countermeasures that the Cisco Anomaly Guard applies.

Establishing Access Control and Change Control

Use the TACACS+ authentication, authorization, and accounting (AAA) feature to establish access controls for the Cisco Guard solution. TACACS+ can also create an audit trail, recording actions taken by individual users.

CONCLUSION

As the threat of DDoS attacks spreads to more companies, effective mitigation has become increasingly important to protecting top-line revenue and company reputations. While traditional DDoS mitigation solutions such as IPSs protect individual properties, they fail to protect upstream bandwidth, rendering the "protected" server unreachable. The Cisco Guard solution is the first line of defense for high-value business services—it protects not only the server, but also its upstream network infrastructure and bandwidth. When companies use the Cisco Guard solution in conjunction with other Cisco Self-Defending Network solutions such as Cisco Security Agent and Cisco IPS, they acquire a multilayer defense that is far more effective than any single solution.

For more information on Cisco DDoS mitigation solutions, visit 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.