How Cisco IT Protects Against Distributed Denial of Service Attacks

Cisco Guard provides added layer of protection for server properties with high business value.

Cisco IT Case Study / < Security and VPN / DDoS Protection: Cisco IT uses a variety of techniques to protect the Cisco network from DDoS attacks. When the attacks originate from a broad range of spoofed addresses and target mission-critical servers, Cisco often uses Cisco Guard, which provides an added layer of protection. This case study describes Cisco IT's internal use of Cisco Guard within the Cisco global network, a leading-edge enterprise environment that is one of the largest and most complex in the world. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

"The threat from low-bandwidth DoS attacks was a hole in our overall security strategy. It wouldn't necessarily be exploited very often, but the risk was significant. We needed a solution to specifically protect servers with high business value."

– John Banner, Network Engineer

BACKGROUND

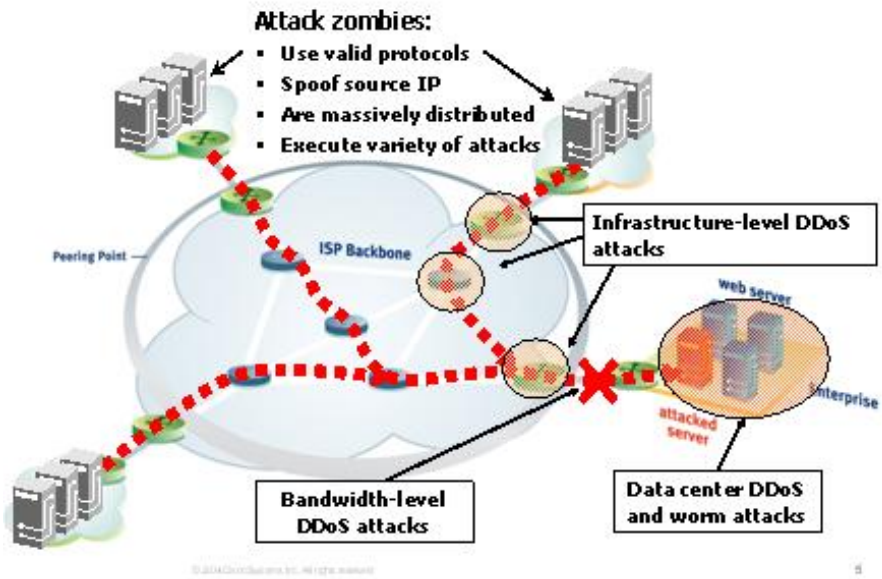
An increase in the rate of network attacks is spurring IT groups to find new efficiencies in protecting network resources. "In the current business climate, it's a much greater effort to detect and prevent attacks, but we don't have more people to do the work," says John Banner, a Cisco® network engineer. "This makes it especially important to automate some portions of network security—to create a self-defending network." Cisco Systems® is highly motivated to automate network defense. Network availability is crucial for business continuity because 93 percent of the company's revenue—more than US$43,000 in sales per minute—is booked online using Cisco Internet connections and internal networks. And more than 80 percent of Cisco products are manufactured by partners that rely on Cisco extranet connections to Cisco campuses.

Cisco successfully uses a variety of technologies to prevent various types of network attacks. The most common attacks originate from a small range of addresses or come in on ports other than HTTP and FTP, such as Windows control ports. To protect against these types of attacks, Cisco uses a technique called "black-holing," which places access control lists (ACLs) at the edge of the Cisco network. This provides coarse filtering of traffic that is clearly unwanted, such as servers spoofing Cisco addresses, or traffic to Windows control ports. In addition, immediately in front of Cisco.com, Cisco IT places another set of ACLs that are much more granular.

CHALLENGE

In 2003, Cisco began experiencing a new kind of threat: low-bandwidth denial of service (DoS) attacks coming from a broad range of spoofed addresses (Figure 1). ACLs are not effective against this type of threat because of the large number of addresses involved. ACLs would block legitimate traffic to Cisco.com as well as malicious traffic. In addition, Cisco IT would need to constantly shift the block as the apparent origin of the attack shifted. The first time this type of attack occurred, Cisco worked with its service providers to block the threat close to the source. Until the remedy was in place, however, approximately one-quarter of IPv4 addresses were prevented from reaching Cisco.com.

Figure 1. Low-Bandwidth DoS Attacks from Spoofed Addresses



ACLs also lack the sophistication to deal with attacks from sites using Network Address Translation (NAT), which makes all traffic from every user at the site appear to come from the same address. Therefore, if one user at a site with NAT is a legitimate user and another is an infected computer participating in a DoS attack, black-holing the address can prevent the legitimate user from conducting important tasks such as downloading Cisco IOS® Software updates or opening a Technical Assistance Center (TAC) case.

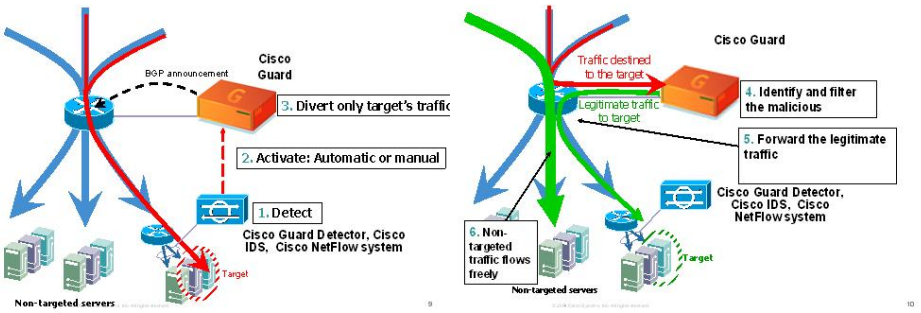
“Our challenge was to distinguish between malicious and legitimate traffic and to block only the former,” says Banner. “The threat from low-bandwidth DoS attacks was a hole in our overall security strategy. It wouldn’t necessarily be exploited very often, but the risk was significant. We needed a solution to specifically protect servers with high business value.”

SOLUTION

Cisco IT found the solution in Cisco Guard, a product developed by a company called Riverhead, which Cisco aquired in April 2004. Cisco Guard is deployed in Cisco’s major ISP points of presence (POPs) around the world to provide an added layer of protection for mission-critical servers, including e-commerce servers, e-mail servers, and Domain Name System (DNS) servers.

Each Cisco Guard mitigation appliance sits on the server’s traffic path. During ordinary operations, traffic follows its ordinary path through the network (Figure 2).

Figure 2. Cisco Guard Solution

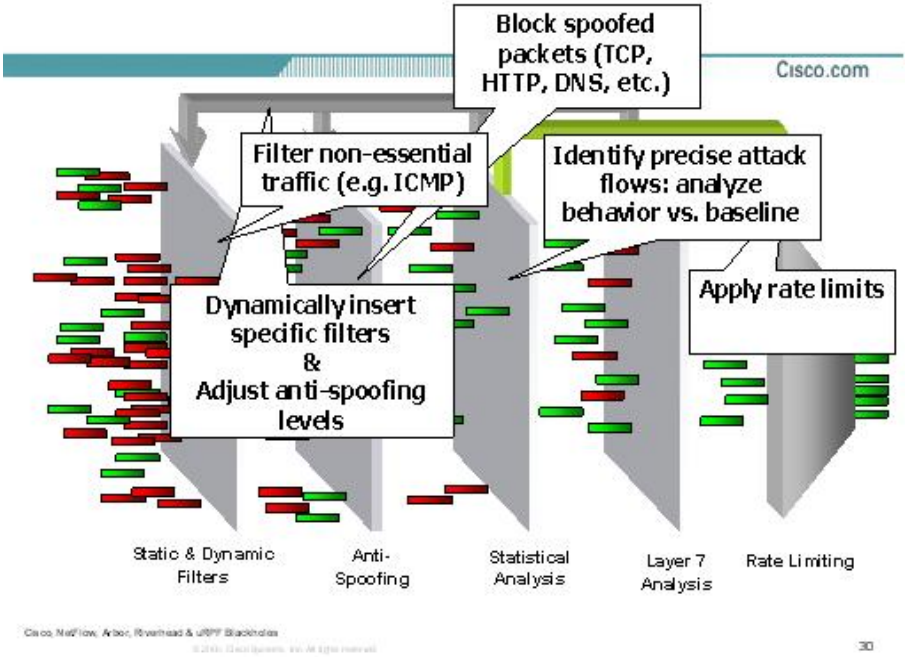


When Cisco IT learns that a potential attack appears imminent—usually by notification from Arbor PeakFlow DoS system, which interprets data collected from Cisco NetFlow technology—Cisco engineers analyze the data to determine the nature of the attack and the most effective mitigation technology. If the attack is small and originates from few IP addresses, one option is to use black-hole technology or simply shut down specific devices. If the attack is large and originates from dozens or hundreds of IP addresses, Cisco IT frequently turns on Cisco Guard to protect the servers under attack. Cisco Guard can be turned on manually or automatically, by an internal detector or an external system such as Arbor PeakFlow DoS or Cisco Intrusion Detection System (IDS).

After Cisco Guard is turned on, it uses dynamic routing to divert traffic headed for the protected properties, based on destination addresses and netblocks. To differentiate malicious from legitimate traffic, Cisco Guard compares it to the normal traffic profile for that server developed during a "learning period" (Figure 3). "The Cisco Guard applies a series of algorithms to distinguish between good and bad traffic, and allows the good traffic to pass through," says Banner. During an incident, Cisco can dynamically tune parameters for protected properties in order to maximize protection against shifting attack profiles.

To minimize the possibility of dropping legitimate traffic along with malicious traffic, the algorithms are conservative in characterizing traffic as malicious. If good traffic is dropped, Cisco IT can add specific hosts to a "white list." This might occur, for example, if the Cisco Guard protection is turned on during an attack, and a customer calls to say he cannot access Cisco.com. "If this occurs because the Cisco Guard thinks the source looks malicious, we can simply add the customer's host to the white list and allow the traffic," says Banner.

Figure 3. Cisco Guard Verification Process



The Cisco network experiences no performance degradation when Cisco Guard protection is turned on. And if the Cisco Guard becomes unavailable for any reason, it simply stops advertising its route, which it ordinarily advertises using Border Gateway Protocol (BGP). This “graceful failure” avoids disruption to business continuity. “At worst we might experience a brief disruption in traffic while the route is removed,” says Banner. Cisco deployed redundant Cisco Guard appliances so that Cisco IT can eliminate the possibility that a bug in an individual Cisco Guard appliance is causing problems, and can upgrade the Cisco Guards without having to turn off protection.

Cisco is collaborating with its global ISPs to deploy the Cisco Guard in their facilities as well, to protect Cisco’s upstream bandwidth from becoming clogged with distributed DoS (DDoS) traffic. “Deploying Cisco Guards in Cisco’s own POPs protects our e-commerce servers from attacks originating from computers within Cisco,” says Talukdar. “Deploying Cisco Guards in the public Internet protects Cisco servers and upstream bandwidth from large-scale attacks originating from locations outside of the Cisco network.”

Cisco selected Cisco Guard over several public domain tools. “The main advantages of Cisco Guard are that it processes more packets per second than other options, and is not inline,” says Banner. “Because it is not inline, upgrades or other outages on the server do not cause network problems, and bugs in the Cisco Guard do not cause outages on protected services when protection is not turned on.”

RESULTS

“Cisco Guard has been successful in mitigating attacks directed toward Cisco’s e-commerce applications,” says William Ku, project manager for the Cisco INS product team. Following are some of the instances in which Cisco has prevented interruptions to the business by using Cisco Guard.

Ruling out a SYN Flood Attack

When Arbor’s PeakFlow DoS revealed an excessive number of SYN packets at the same time Cisco wasexperiencing problems with the Cisco.com servers, Cisco IT suspected a SYN flood attack, and turned on Cisco Guard to filter SYN packets. The SYN packet is the first packet of a TCP handshake. Whenever a host receives a SYN packet it sets up a new session. But if the SYN packet is not eventually followed by a packet to end the session,

the host can quickly run out of memory and other resources. Cisco Guard used its sophisticated algorithms to analyze the traffic, and concluded that the traffic was legitimate, although it was, indeed, out of spec. Armed with this information, Cisco IT turned its attention to other potential sources of the problem, eventually identifying the cache engines in front of Cisco.com. “Whether or not Cisco Guard identifies the problem as an attack, it’s a useful tool,” says Banner. “In this case it helped us narrow our scrutiny to more quickly identify the source of the network trouble.”

Preventing Spamming of a Customer Website

In January 2004, a new worm was released that was scheduled to begin spamming the website of a major company (and Cisco customer) on a particular date, an event that was widely publicized. To ensure that no Cisco hosts were going to participate in the attack, Cisco IT set up Cisco Guard with that company as a victim, monitoring traffic between Cisco and the company. “As it happens, the infected hosts were remediated before the attack started,” says Banner. “But had our antivirus measures been less effective, Cisco Guard would have enabled us to block any malicious traffic originating from our servers without blocking legitimate traffic to the other company.”

LESSONS LEARNED

Banner notes that IT staff need to let each other know when Cisco Guard is turned on. Cisco inadvertently validated the effectiveness of Cisco Guard when someone turned on protection on the Cisco load test network without informing other staff members. This network is used to test applications before they are put into production on Cisco.com. When a single PC sent application traffic, it arrived at its destination as expected, but when the application generators sent the traffic in higher volumes, it was dropped. “Cisco Guard determined that the traffic was coming in too quickly for normal patterns, making it look like an automated attack,” says Banner.

It is also important to check profile information periodically during learning. If a real attack started while Cisco Guard was in learning mode, Cisco Guard would consider the malicious traffic normal. Therefore, if the attack occurred on the last day of a seven-day learning cycle, the learning cycle would have to be restarted—and Cisco Guard would not be effective for mitigating the attack. Cisco avoids this problem by checkpointing profile information at various times during the learning cycle.

Similarly, it is advisable to periodically repeat the learning cycle for protected hosts. Otherwise, changing traffic patterns can also invalidate the profile.

NEXT STEPS

Cisco has begun working with service providers to offer the Cisco Guard solution to other enterprise customers. The “Clean Pipes” solution will drop malicious traffic before it arrives at the company that is the target of the attack. “When Clean Pipes becomes part of every ISP’s service infrastructure, DDoS attacks can be contained at the ISP site so that they do not affect a company’s Internet connection,” says Ku.

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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