How Cisco IT Protects Against Distributed Denial of Service Attacks

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

BUSINESS BENEFITS

- Helps ensure business continuity
- Protects mission-critical servers
- Automates response to attacks
- Allows legitimate traffic through during attacks

"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, Cisco Systems

Cisco Systems® successfully uses several different technologies to prevent various types of network attacks. To protect against attacks from a small range of addresses, for example, Cisco® places access control lists (ACLs) at the network edge, a technique called "black-holing".

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. ACLs are not effective against this type of threat because of the large number of addresses involved. The ACLs would block legitimate as well as malicious traffic. Cisco IT wanted a solution that would distinguish between malicious and legitimate traffic and block only the former.

Cisco IT deployed Cisco Guard, which has successfully mitigated attacks against Cisco's mission-critical servers. Cisco Guard is deployed in Cisco Internet points of presence (POPs) around the world as well as in service provider locations. When Cisco IT learns that an attack appears imminent, it decides whether to use Cisco Guard or another mitigation technology.

Cisco Guard drops malicious traffic while allowing legitimate traffic to pass through. It applies sophisticated algorithms to compare traffic against a normal profile developed during a learning period.

The Cisco network experiences no performance degradation when Cisco Guard protection is turned on. During an attack, Cisco customers can continue to use Cisco network resources as they would ordinarily.

Deploying Cisco Guard appliances in the service provider network protects upstream bandwidth. Malicious traffic is intercepted and dropped before it arrives at the Cisco network.

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

Case Study: http://www.cisco.com/web/about/ciscoitatwork/case_studies.html

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.**