SOLUTION OVERVIEW

PROVIDING SERVICE SECURITY WITH CISCO SERVICE CONTROL TECHNOLOGY

The ubiquity of the Internet coupled with the increasing number of unprotected and unsophisticated residential users threatens the operational integrity of service provider networks. Malicious software such as worms, viruses, and spam zombies can cripple a provider network by creating network gridlock, increasing operating costs, consuming provider storage capacity, and disabling the subscriber universe. Service security can be enhanced by deploying Cisco® Service Control technology, which identifies an attack, protects the network, and notifies or redirects subscribers to support sites to facilitate resolution and minimize overall impact.

CHALLENGE

As the number of "always-on" residential broadband connections grows, coupled with the lack of security-conscious residential users, the open nature of the Internet creates a breeding ground for network security threats impacting both service providers and subscribers. Subscribers are under a constant threat of denial-of-service (DoS) attacks, worms, and virus infections. Recent threats have created "security storms" resulting from such popular viruses as Sasser, myDoom, Slammer, or Blaster. Meanwhile, spam zombies create a different set of issues for service providers.

Although infected computers and laptops cause obvious problems for subscribers, ensuring the integrity of the service network or service security is a paramount issue for network operators. It is expected that as intelligent mobile handsets become increasingly prevalent, security threats to the mobile network will become more evident. Distributed DoS (DDoS) attacks include SYN floods, connection floods, packet floods, and difficult-to-identify attacks coming from spoofed and nonspoofed sources. Many broadband users are not sufficiently educated about the dangers of unprotected Internet access resulting in, for example, worm infection.

Using encrypted attachments to infiltrate subscriber systems with worms and viruses ultimately impacts service provider operations and profits. PCs in the home network left continually connected to the Internet can be easily infected. Casual residential users may not even be aware that their machine has been compromised. Although causing obvious damage to the infected subscriber, the costs to the service provider of increased network traffic from the broadband edge and the customer support associated with troubleshooting an infected subscriber system can be significant. However, each can be dramatically reduced if the providers could only identify and mitigate against the attack in the first place—doing so before it is broadly disseminated across their network.

Multiple infected hosts generating spikes in traffic result in congestion, degraded user performance, and a big administrative burden for operators, because they must use additional cycles to troubleshoot their network, respond to calls for technical assistance, and work to reestablish levels of service. To overcome malicious attacks, operators must track, disable, and block their spread.

Beyond DoS, worm, and virus attacks, spam zombies offer a different type of threat to service providers. Once considered little more than an annoyance, spam has become an enormous headache affecting Internet users and broadband service providers. Big-name viruses, worms, and Trojan horses get the headlines, but spam is arguably a more pervasive and insidious threat because it affects every Internet user, directly or indirectly, and it lacks a comprehensive solution analogous to antivirus software programs. Spam can cause disruptions to service when service providers are blacklisted as spam sources because of the activities of their users, real or spoofed.

Protecting the service network from these operational threats translates into profit-line savings for service providers. Security solutions have traditionally focused on the workstation or enterprise network. However, security threats to a provider’s network are just as viable, but few proactive tools that provide diagnosis, troubleshooting, and resolution are available, escalating operational cost and reducing profit for service providers. Service control complements existing solutions and can mitigate the impact of these threats to service security and facilitate the restoration of service levels.

SOLUTION

The Cisco Service Control solution from Cisco Systems® enhances IP networks with an application-aware service control point that enables the network to identify and classify application traffic by subscriber at multigigabit speeds. By tracking all network activity, the Cisco Service Control Application for Broadband can identify malicious attack patterns and contain their effect.

Cisco Service Control technology comprises both hardware and software integrated into a state-of-the-art, dedicated network device, providing detection and control capabilities. Using a Layer 7 stateful deep packet inspection capability, the solution can accurately identify application use by individual subscriber. Only the Cisco Service Control solution has a unique set of characteristics and architectural attributes purpose-built to perform real-time traffic classification, accounting, and control. In order to undertake stateful deep packet inspection at multigigabit speeds, a specific hardware architecture is required that is capable of maintaining the state of each network conversation, while executing deep and detailed inspection of each data packet through the application or Layer 7 network layer. The result is a solution that can detect specific protocol signatures and classify all traffic for a given network session.

Mitigating Against DoS Attacks, Viruses, and Spam Zombies Using a Three-Phased Approach

The Cisco Service Control Application for Broadband uses a three-phased approach to reduce the operational costs associated with DoS flood attacks, worms, or viruses and is equipped to help service providers stop spam from reaching subscribers. Cisco Service Control helps service providers proactively reduce the impact of malicious attacks on their network and their subscribers by blocking malicious traffic, reducing overall network congestion and technical support calls from subscribers seeking assistance.

In the case of viruses, worms, or DoS attacks, Cisco Service Control can detect and monitor, for example, virus-related traffic. The solution can identify the source of such attacks from within the provider network and implement traffic control policies to prevent the spread of a virus by identifying the port numbers and the protocols used and then blocking further propagation across a provider’s network.

Using the example of how a spam zombie attack is thwarted using Cisco Service Control can further demonstrate how application and subscriber awareness can alert providers to such threats, identify and isolate infected subscribers from malicious attacks, and direct them to support centers for resolution. Spam zombie-based attacks constitute one of the most difficult problems for service providers to defend against, creating support challenges for meeting customer satisfaction. As spammers use more sophisticated techniques, providers can adapt by taking advantage of the programmable, intelligent network infrastructure offered by Cisco Service Control to respond to threats in real time. Addressing the spam zombie challenge requires a multidimensional approach that includes the ability to map traffic to a particular subscriber and classify it to the Simple Mail Transfer Protocol (SMTP). This is just one example of how Cisco Service Control technology helps reduce security threats in service provider networks.

Cisco Service Control solutions employ deep packet inspection at Levels 4 through 7, as well as the ability to maintain “state” to identify and redirect anomalies in network traffic generated by spam zombies. Adding state to the solution is the key that allows Cisco Service Control technology to differentiate, for example, between 1000 1-KB messages generated as 1000 independent sessions or a single 1-MB mail session. Less-effective or “stateless” service control offerings can only count packets and cannot easily differentiate between a multitude of small sessions or a single large one. In the case of spam zombie attacks, the Cisco Service Control solution uses the following critical detection and notification capabilities:

Phase One: Identification:

- In the case of spam, Cisco Service Control detects the characteristics of a zombie attack in the early phases, often in the first few thousand messages, and quickly identifies the source of the suspected spam attack.
- The solution can just as easily identify and track DoS flood, virus, and worm attacks at the session level. When identified, the Cisco Service Control Application for Broadband generates an alarm indicating the exact origin of an attack, automating the process of tracking infected hosts.

Phase Two: Protection:

- After suspicious traffic patterns are identified, the fast reporting of Cisco Service Control allows system administrators to intervene, quickly redirecting or quarantining infected machines. The solution can be configured to protect network resources by automatically identifying and blocking malicious traffic, a process that normally requires manual configuration of network devices. This capability helps block further propagation of malicious software across the network.
- In the spam example, quarantining the zombie machines limits the amount of spam that gets through the network.

Phase Three: Notification:

- Because infected users are unaware of the infection, in addition to stopping the attack originating from their machines, Cisco Service Control notifies subscribers of the infection and redirects them to support centers where they can take corrective action.

The Cisco Service Control Application for Broadband takes advantage of the application- and subscriber-aware architecture of the platform to monitor and analyze application-level traffic, allowing the service provider to quickly identify DoS, virus, or spam zombie activity from a particular subscriber, block the transmission, and redirect the infected subscribers to sites where infected systems can be purged of system corruption.

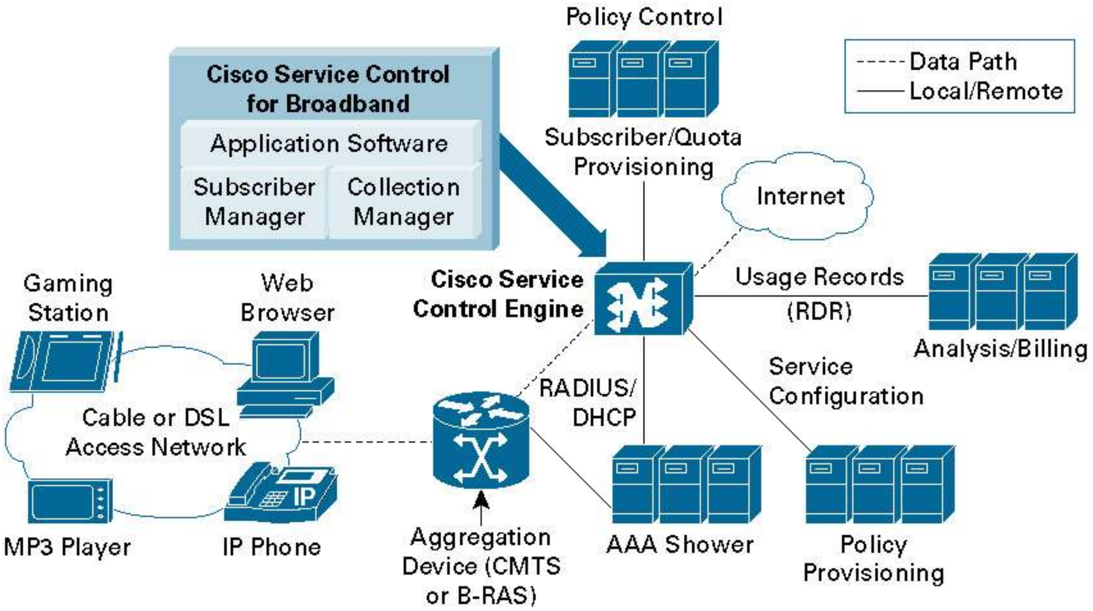
BUSINESS BENEFITS

Cisco Service Control enhances a provider’s ability to detect, manage, and ameliorate the impact of DoS, virus, and spam zombie attacks on their network, helping operators to:

- Identify broadband subscribers infected by worms and other malicious programs and analyze their impact on overall service quality
- Reduce overall response time, operational costs, and technical support calls associated with the diagnosis and response to large-scale worm infections in a broadband network
- Enhance overall customer satisfaction by providing proactive identification, notification, and redirection to technical support if DoS attacks, viruses, or spam zombie infections occur
- Avoid network outages and congestion as a result of early detection and mitigation
- Proactively manage spam zombie traffic disseminating from broadband subscribers; avoid potential service provider blacklisting resulting from spam zombie sourcing

ARCHITECTURE

Figure 1
Cisco Service Control in the Network



PRODUCTS, PARTNERS, OR SERVICE OFFERINGS

- Cisco SCE 1000 Series Service Control Engine
- Cisco SCE 2000 Series Service Control Engine
- Cisco Service Control Application for Broadband
- Cisco Service Control Collection Manager
- Cisco Service Control Subscriber Manager
- Cisco Service Control Quota Manager

WHY CISCO?

Cisco offers the industry’s leading service control solutions, offering multigigabit performance and stateful deep packet inspection as well as worldwide technical assistance and support. Cisco is speeding the evolution of networks from generic transport to platforms offering higher-value, higher-margin services. Programmable, scalable, and purpose-built for the communications sector, Cisco Service Control technology accelerates network delivery of advanced IP services. The Cisco Service Control platform adds intelligence, stateful deep packet inspection, and multigigabit analysis to existing network infrastructure and helps carriers identify and charge for dissimilar content applications while simultaneously managing performance requirements of different applications. The Cisco Service Control solution is deployed in more than 50 companies worldwide.

FOR MORE INFORMATION

For more information about the Cisco Service Control solution, visit http://www.cisco.com/go/servicecontrol or contact your local Cisco account representative.

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

De/LW7907 02/05

Printed in USA