Customer Success Story

European Telco Defends Its Network and Customers

Executive Summary

Customer Name

COLT Telecom

Industry

Telecommunications

Business Challenge

Protect the COLT IP/MPLS network and customers' traffic from distributed denial of service (DDoS) attacks

Network Solution

Cisco DDoS Protection solution

Business Value

- Provides scalable, carrier-class attack protection
- Promotes high customer satisfaction with COLT managed services

COLT defends its customers' traffic and networks against DDoS attacks using the Cisco DDoS Protection solution.

Business Challenge

Headquartered in London, COLT is a leading European provider of business communications, delivering data, voice, and managed network services to major and midsize businesses as well as to wholesale customers. The company serves more than 50,000 customers in 13 countries. Although its customers span all industry segments, financial services organizations constitute its largest single market segment. COLT's communications services underpin the mission-critical activities of more than 1000 financial firms. As one of only four network providers approved by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), COLT connects more than 650 European SWIFT members to SWIFT's highly secure IP network. SWIFT's worldwide community includes banks, securities brokers and dealers, investment managers, as well as members' payment, securities, treasury, and trading market infrastructures. COLT's customers also include Europe's top seven stock exchanges, the world's top 25 financial institutions, and the top three global information providers.

COLT delivers its services over a 20,000-kilometer network that includes metropolitan-area networks (MANs) in 32 European cities with direct fiber links connecting 10,000 customer buildings with 12 data centers. The company also has more than 1000 peerings in Europe and the United States that provide Internet connectivity to hundreds of ISPs around the world. Over this network, COLT delivers managed data services that range from storage-area network (SAN) and switched Ethernet services to IP VPN, Gigabit IP over Ethernet, and high-performance Internet access services. Security offerings include router-based firewall, dedicated firewall, intrusion detection, antivirus and spam protection, DDoS protection, and business continuity services.

Protecting its network – and, therefore, its customers' critical business traffic – against DDoS attacks is a priority for COLT. Thousands of DDoS attacks occur around the world weekly – and each one can seriously affect the targeted company's revenue.

In 2002, COLT began looking for a solution to complement its existing infrastructure security program with the goal of protecting the IP network and important systems, such as Domain Name Servers, from DDoS attacks launched using large botnets. Access control lists (ACLs), quality-of-service (QoS) policies, and data plane and control plane policing techniques were already deployed, protecting the IP Multiprotocol Label Switching (MPLS) network core, but these techniques had little power over DDoS attacks.

"It is critical for a Service Provider to assure high network availability even when a flood of bad packets arrives at the network," says Nicolas Fischbach, senior manager of Network Engineering Security for COLT. "If those packets reach critical systems, the access network, or customer premises, it's too late to prevent harm." In 2002, the only option was to "blackhole" the destination IP address of an attack. This meant making the customer's server unreachable – effectively dropping all traffic sent to it. Unfortunately, blackholes also affected business-critical traffic, which didn't help customers' businesses either. In either case, an attacker achieved its intended goal.

Finding an appropriate DDoS detection and mitigation solution was challenging. The new solution needed to secure a large, open IP backbone without becoming an obstacle to desirable traffic. It could not introduce additional complexity or restrictions into the network, nor could it create an operations or management burden. It would have to operate transparently to customers. Most importantly, the new solution would have to integrate easily with COLT's existing infrastructure, routing protocols, and MPLS core network – all while delivering high scalability. These requirements significantly reduced the pool of potential solutions.

The COLT Security and Backbone Engineering teams evaluated several alternatives, but only the Cisco® DDoS Protection solution met the requirements for a carrier-class solution.

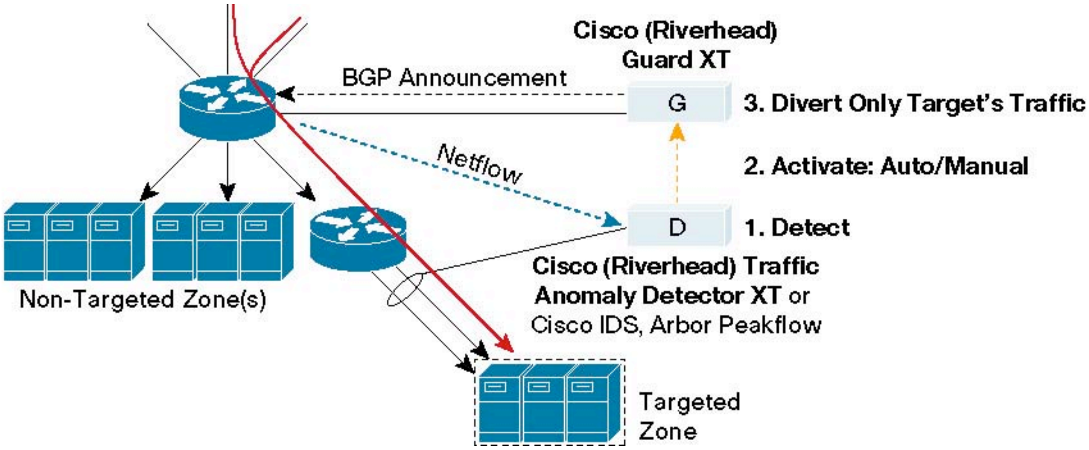
Network Solution

COLT took the approach of deploying the Cisco DDoS protection solution in its regional cleaning centers, which are located at the edge of its network to be as close as possible to the source of an attack. This enables COLT to filter traffic at the network edge, where attacks are most easily detected and stopped.

The COLT network is MPLS enabled. COLT's network edge, which faces other ISPs, is distributed across Europe and includes locations in New York. Peering and transit routers are Cisco 12000 or 7200 series routers. All COLT edge routers run the latest version of Cisco IOS® Software and take full advantage of native features such as Transit, Infrastructure, and Receive ACLs and Control Plane Policing (CoPP). COLT also uses CiscoWorks LAN Management Solution (LMS) to manage configuration, software versions, and reporting on its IP network backbone.

Customers connect to the COLT network or to a COLT data center using DSL, E1 to STM-4, or Fast/Gigabit Ethernet links. These connections are usually terminated on Cisco 7200, 7500, 7600, and 12000 series routers for WAN links or Cisco Catalyst® 6509 switches for Internet Solution Center links. The switches connect COLT's systems, server farms, managed hosts, and customers that are co-located in a COLT data center. The switches are deployed with Cisco Catalyst 6500 Series Supervisor Engine 720 modules, which provide subsecond failover to help ensure high availability. They also incorporate Cisco Catalyst 6500 Series Firewall Services modules, a high-speed integrated firewall with advanced security features.

Figure 1
Cisco Guard Systems are Located at the Network Edge



How the Cisco DDoS Solution Works

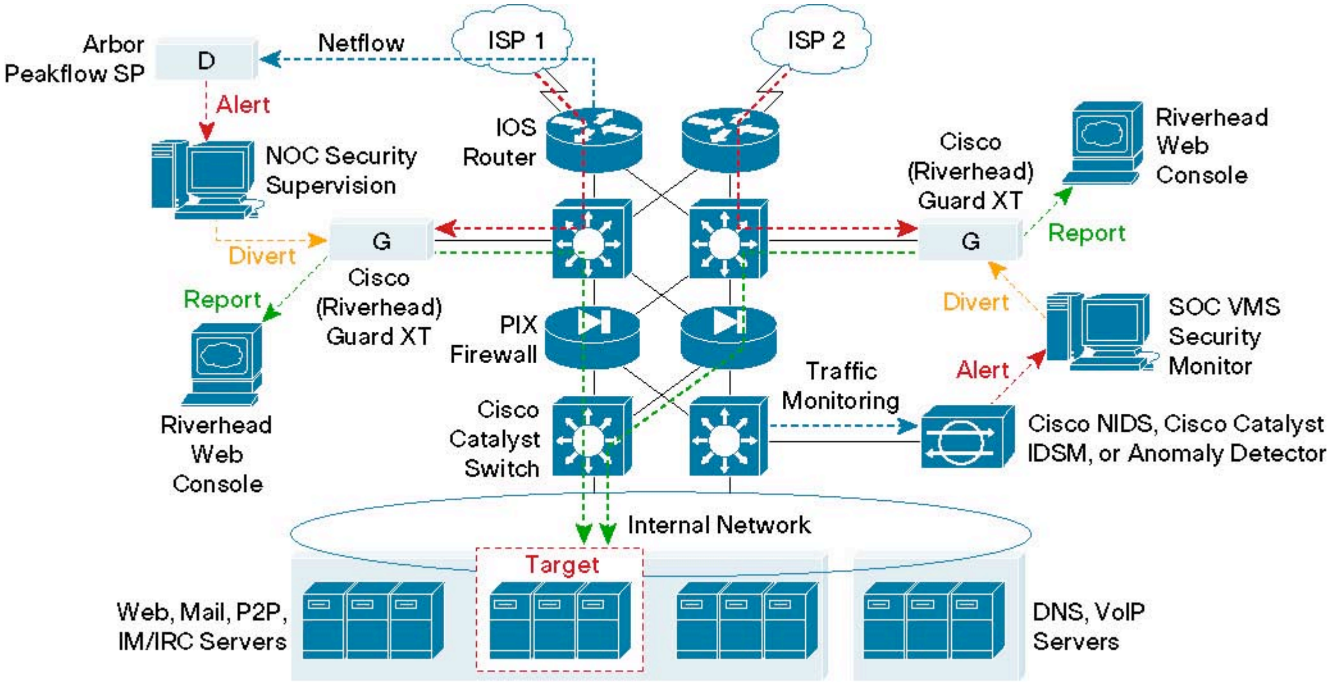
A primary component of the COLT IP Guardian solution is the Cisco Guard XT 5650 DDoS mitigation appliance, which performs traffic cleaning. As it would be impractical to place a Cisco Guard system at every exchange point in the network, COLT deploys them in four regional cleaning centers – in the "United States" region, and in Europe a North region, a Central region, and a South region. By default, traffic entering the COLT network in that region stays in that region unless the cleaning center is down, in which case the traffic is automatically redirected to another region using Border Gateway Protocol (BGP). In each regional center, the Cisco Guard appliance is directly connected to a powerful and high bandwidth core router. Each has a BGP session with every peering and transit edge routers.

Each Cisco router that connects to an ISP generates NetFlow network telemetry data, which is sent to an Arbor Peakflow Monitor. The monitors send aggregated NetFlow data to a controller that displays network events to COLT operations and engineering staff. When incoming traffic exceeds the parameters that define "normal" traffic, this anomaly is detected and an event is displayed in COLT's London Network Operations Center. COLT personnel then make the decision to activate the Cisco Guard protection for that customer.

When this decision is made, traffic triggering the event is diverted to the nearest Cisco Guard unit for cleaning by announcing the IP address or network being attacked. Using MPLS Long Diversion features that COLT pioneered in conjunction with the Cisco DDoS Protection solution, COLT network engineers create protection zones on the Cisco Guard, which trigger a BGP update to the network. The update tells all edge devices that the most specific route to reach the customer under attack now goes through the Cisco Guard, creating an MPLS Label Switch Path (LSP) from each edge router to the closest Cisco Guard. The attack traffic is transported to the Cisco Guard, cleaned, and sent back into the network. The cleaned traffic follows the normal routed path to the customer. The COLT IP Guardian service requires no customer premises equipment.

Figure 2

Using MPLS and BGP techniques, traffic is dynamically diverted to the Cisco Guard where DDoS, botnet, harmful traffic, and other malicious threats are detected



With Cisco Guard systems deployed in regional cleaning centers, COLT can offer its IP Guardian service to selected customers while protecting its own infrastructure – even when large DDoS attacks enter the network.

The Cisco Guard XT 5650

The Cisco Guard XT 5650 delivers multigigabit performance to protect even the largest networks from DDoS attacks. It performs per-flow-level attack analysis, identification, and mitigation to block specific attack traffic. Alerted by the Cisco Traffic Anomaly Detector XT or Arbor Peakflow SP, the Cisco Guard XT 5650 diverts the traffic for the attacked destination and subjects it to the Multiverification Process (MVP) algorithm for cleaning. On COLT's infrastructure, the MVP architecture imposes multiple layers of defense designed to identify and block the packets and flows responsible for the attack while allowing legitimate transactions to pass, ensuring business continuity even while under attack.

"It's an illusion to think that any DDoS filtering solution can filter out 100 percent of bad packets," says John Baldwin, senior manager of Managed Data Products for COLT. "Even if you filter 98 percent of the attack traffic, if the attack is 1 Gbps in size, there will still be 20 Mbps of unwanted traffic that can hit the end-customer's network. So it's important that the customer has appropriate network connectivity with links whose bandwidth can be turned up if needed and distributed DNS servers to enable flexible disaster recovery."

"Before we deployed the Arbor Peakflow SP and Cisco DDoS Protection solution, we were blind to the actual scope of impact that DDoS attacks were having. Now we can observe exactly what is happening and we can quantify how many attacks we see, what type of attacks they are, and which customers are most often targeted."
– Nicolas Fischbach, Senior Manager, Network Engineering Security, COLT Telecom

Product List

Cisco Guard XT 5650

Cisco Network Foundation Protection

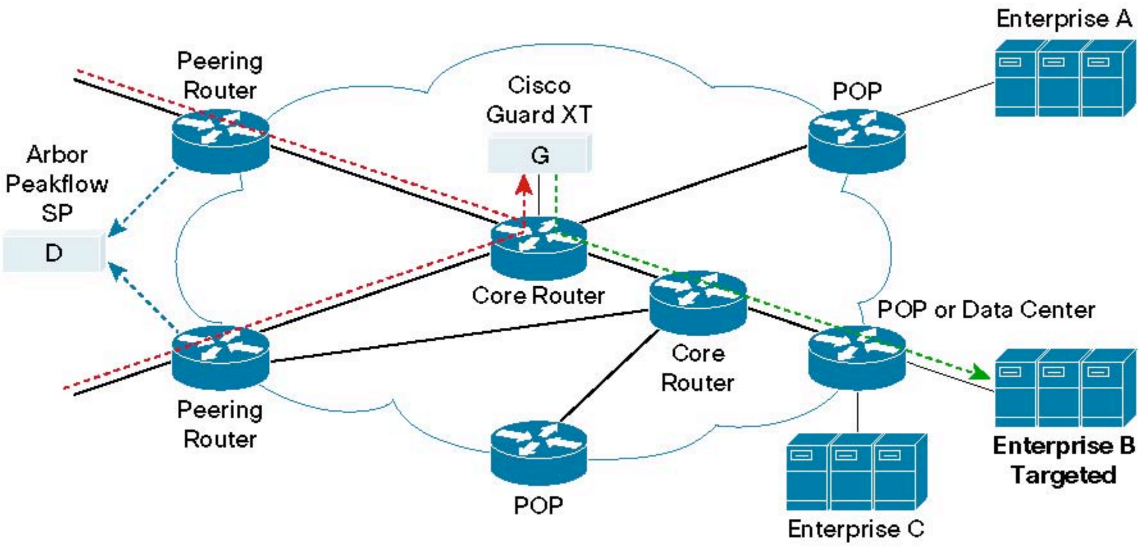
Cisco IOS NetFlow v5

Arbor Peakflow SP

Business Value

Currently, COLT offers its IP Guardian service to customers whose network infrastructures can cope with any bad packets that evade the detection engine of the Cisco Guard. For example, the customer still requires sufficient spare bandwidth, CPU cycles, and server memory, as well as distributed DNS servers, to adequately defend against a large attack. Customers can use the COLT IP Guardian service as a dedicated service that provides continuous levels of protection or as an on-demand service, where preventative steps are taken only once an attack has been detected. While the solution is able to protect any COLT customer, the initial target market is customers that use at least 4-Mbps bandwidth services.

Figure 3
Three Types of Service Environments for Deploying the Cisco Guard Solution



Managed Service Based on COLT Pioneered MPLS-Based Long Diversion
- Detection at SP Edge, Flexible Diversion to Regional Cleaning Center, No CPE Required
- Incremental Deployment for Specific Large Customers and Regions

Now when any customer comes under attack, COLT engineers invoke the IP Guardian capabilities. In addition to protecting customer traffic, the Cisco DDoS Protection solution protects the COLT network as well. If a significant attack occurs, it not only affects the target customer, it can also affect other customers by overloading parts of the network. The Cisco DDoS Protection solution gives COLT new visibility into DDoS attacks and their potential impact on its network.

“Before we deployed the Arbor Peakflow SP and Cisco DDoS Protection solution, we were blind to the actual scope of impact that DDoS attacks were having,” says Fischbach. “Now we can understand exactly what is happening and we can quantify how many attacks we see, what type of attacks they are, and which customers are most often targeted. We still must work with the customer to determine if an attack is actually affecting their service in order to offer the best possible protection.”

Baldwin adds, “Unlike other security offerings that rely on traditional firewalls or other customer premises equipment, the COLT IP Guardian service detects and protects while the traffic is still on the COLT network. In this way, the attack is prevented and reduced long before reaching the customer’s site. We know that when we detect an attack and confirm with the customer that it needs protection, we can help and the outcome is usually extremely positive.”

The solution is cost-effective for COLT because the company does not have to add excessive bandwidth simply to handle unwanted traffic, which also helps minimize the cost of expensive international bandwidth. As a network-based solution – able to filter traffic before it reaches the customer access – the Cisco DDoS Solution also contributes significantly to improved network uptime and fewer incidents that require escalation and consume IT resources. Flexible, dynamic operation enables COLT to quickly and easily deploy new policies or changes to accommodate rapidly changing threat environments.

The IP Guardian service delivers a unique advantage to COLT customers as well. Customers can protect their Websites and e-commerce operations from DDoS attacks while allowing genuine traffic to continue flowing, thus avoiding costly downtime and revenue loss.

> **“Unlike other offerings that rely on traditional firewalls or customer premises equipment, the COLT IP Guardian service detects and protects while the traffic is still on the COLT network. In this way, the attack is prevented and reduced long before reaching the customer’s site. We know that when we detect an attack and confirm with the customer that it needs protection, we can help and the outcome is usually extremely positive.”**
> – John Baldwin, Senior Manager, Managed Data Products, COLT Telecom

Next Steps

COLT continues to fine-tune the service and the capabilities of the Cisco DDoS Protection solution, as well as evaluate new IP Guardian service features. For example, COLT is exploring an on-demand service, in which IP Guardian steps can be initiated once an attack has been detected and import traffic profile data from Arbor Peakflow SP. Filtering complex traffic like Voice over IP (VoIP) or Peer-to-Peer (P2P) is another feature under consideration. Customers are beginning to request real-time reporting and notification of attack protection – all of which capabilities can be used to enhance the original IP Guardian service.

“The Cisco DDoS Protection solution is a worthwhile investment for COLT,” says Fischbach. “The ability to secure our backbone and our customers’ traffic has enabled COLT to gain a competitive advantage and a customer satisfaction advantage. Every time we have invoked protection, customers have been extremely satisfied with the results.”

For More Information

To learn more about Cisco DDoS Protection solution, visit: www.cisco.com/go/cleanpipes.

To learn more about Cisco security solutions, visit: www.cisco.com/go/security.

To learn more about Cisco switching solutions, visit: www.cisco.com/go/switching.

To learn more about Cisco routing solutions, visit: www.cisco.com/go/routing.

To learn more about COLT Telecom, visit: www.colt.net.

This customer story is based on information provided by COLT Telecom and describes how that particular organization benefits from the deployment of Cisco 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.

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

DR/LW9743 11/05

Printed in the USA