BROCADE

Massively Scalable Routers Protect Global Network Traffic Against DDoS Attacks

EXECUTIVE SUMMARY

Challenge
Deliver highly available services to global clients in spite of nonstop DDoS attacks

Solution
- Brocade MLXe Routers for core routing
- Brocade NetIron CER 2000 Series Routers deployed as backup
- Brocade ICX 7750 Switches for high-density 10 Gigabit Ethernet connectivity
- Brocade ICX 7450 Switches for high-density 10 Gigabit Ethernet connectivity

Results
- Deployed 700 gigabytes of capacity across a global network infrastructure
- Delivers clean traffic with minimal latency or rerouting across the network
- Successfully mitigates hundreds of DDoS attacks daily

Micron21

The Micron21 Data center hosts hundreds of thousands of Internet Web sites and cloud services for local, national, and international businesses and government agencies. It securely transmits data to more than 1600 peered networks around the world every day. Core business services range from basic Web hosting to cloud services, disaster recovery solutions, security surveillance, and many others. But one of its best-known capabilities is its Distributed Denial of Service (DDOS) protection, which helps keep clients' Web sites running smoothly.

Solving a Massive Challenge

When Micron21 first began offering services, it used a Cisco platform. As the company grew, the more attractive it became as a target for cyber terrorists. Suddenly, DDoS attacks were bringing the network to its knees, and the Micron21 team had no idea where the traffic was coming from. After enabling NetFlow, the team could see source and destination data. However, when an attack occurred, network routers could not provide source and destination data while also passing traffic.

"We wanted massive routers with massive capacity and the ability to show us source and destination so that we could control network flows," said James Braunegg, Managing Director of Micron21. "We chose Brocade® MLXe Routers so that we can route large amounts of unwanted traffic and survive the very worst possible day."

Growing Globally

In 2010, Micron21 deployed its first Brocade MLXe Routers in its Melbourne data centers, connected over point-to-point dark fiber. Now it could roll out high-availability, geographically redundant IP services for mission-critical hosting. The team could simultaneously monitor and pass traffic during a DDoS attack and then normalize the unwanted traffic to avoid affecting other clients. Rapid growth continued, and Micron21 continued to deploy Brocade MLXe Routers. In 2014, the company expanded internationally, purchased more Brocade MLXe Routers, and also invested in anti-DDoS hardware, which was deployed in the United States and Australia.

micron21

"For the most effective DDoS protection, we want to be as close to the attack source as possible," said Braunegg. "We also want to connect to as many networks as possible so we can control the flow of inbound traffic when our customers are under attack."

Now Micron21 had the capacity to absorb an attack and the technology to clean Australian traffic within Australia and clean international traffic in the United States. This approach worked better, but during a DDoS attack, traffic comes from all over the world to a single location. Micron21 expanded its network again to deploy scrubbing centers in Amsterdam, Singapore, Los Angeles, Sydney, and Melbourne.

Micron21 locations are connected over a global Multiprotocol Label Switching (MPLS) network for optimal routing of clean traffic across regions. Brocade MLXe Routers reside at the network edge, in front of DDoS mitigation systems, load balancers, and firewalls in each location. Brocade CER 2000 Series Routers provide backup designated router (BDR) functionality if required. Micron21 also uses Brocade ICX® 7450 Switches and Brocade ICX 7750 Switches at its points of presence to provide high-density, 10 Gigabit Ethernet (GbE) connectivity in a compact form factor.

Clean and Connected

Micron21 is one of the most connected networks in Australia. The latest implementation of Brocade solutions increased network capacity to 700 gigabytes and extended the company's reach to global customers. This infrastructure enables Micron21 to deliver tiered service offerings, such as remote protection for Web sites and online resources or network-based protection with Soak & Scrub services. Domestic traffic within each scrubbing region is cleaned within the region—as close to the source as possible. This ensures that only clean traffic travels across the network while minimizing latency and avoiding the need to reroute international traffic.

Massive Mitigation

With a highly fault-tolerant site infrastructure, Micron21 now addresses large DDoS attacks. Braunegg says that attackers are always devising new ways to increase their impact. A recent attack directed traffic at 90 Gbps against a client. Another attack launched 3 Gbps against another client, but originated entirely within Australia on a Tier 1 provider's network.

"Whether a DDoS attack is 90 Gbps or 3 Gbps, our network absolutely handles it," said Braunegg. "We successfully mitigate hundreds of attacks daily."

Heading for Tier IV

To date, Micron21 has experienced 30 percent growth per year, and it expects that rate of growth to continue. With a blue-chip client list, Micron21 is now building Australia's first Tier IV-certified data center and aims to complete construction and certification in 2017. Thanks to Brocade, its traffic will be protected.

"When it's finished, we will have the best datacenter in Australia from a power, cooling, and network point of view," said Braunegg. "Our clients—whether small businesses or large hosting companies and global enterprises—will not only continue to receive highly available services, they'll also have some of the most advanced DDoS protection available."

For more information,
visit www.brocade.com.

BROCADE