Our IT team needs constant, high-speed Internet connectivity to maintain our high-traffic website, which acts as our face to the world

- Mr. Duncan Kikata
IT Manager
Capital FM, Kenya

http://www.cyberoam.com

Cyberoam Ensures Constant, High-Speed Internet Connectivity for Capital FM

About Capital FM Kenya

Capital FM was the first independent, privately owned radio station in Kenya. Capital FM which initially covered Nairobi and its environs now has a nationwide coverage and broadcasts live 24 hours a day. While several other FM stations catering to all tastes have continued to appear, 98.4 Capital FM has maintained its popularity – especially among the middle-class and upper-class markets.

Capital FM has spread its digital media footprint, which is why it says "from Kogelo to Kansas, you can listen live to Capital FM". For over 10 years now, Capital FM has also been offering live streaming of its radio broadcasts to Kenyans and to the world, making it a truly global station.

Seeing the power of the Internet as a communication medium, Capital FM launched its Digital Media division. Today its website www.capitalfm.co.ke– receives over 1 million visitors with over 15 million page views a month. Visitors from across 100 different countries – with the majority from Kenya (67%), USA, UK, South Africa, Germany, Canada, Uganda, and even as far as Brazil and Australia – enjoy the Capital FM offering.

The Capital FM Challenge

"Our IT team needs constant, high-speed Internet connectivity to maintain our high-traffic website, which acts as our face to the world," said Mr. Duncan Kikata, IT Manager at Capital FM. Any downtime would spell catastrophe for them. Additionally, most of their core business processes are dependent on the Internet. Prior to Cyberoam installation, they had the following network security concerns.

Vulnerable Network Perimeter

The Capital FM network was vulnerable to network-based attacks through Phishing, Pharming, hacking, remote exploits, Denial-of-service (DoS) attacks and other unpredictable attacks. Hence, Mr. Kikata desired a robust security solution that would minimize chances of the Capital FM network being exposed to unauthorized, external sources that would exploit, harm or even destroy their network's internal resources.

Network Compromised from Within

Another major concern for Mr. Kikata was nuisance from within the network itself. In the absence of a firm hand upon Internet access, employees' internet activities could not be controlled. Unprotected and unruly web surfing and uploading/downloading by employees invited a deluge of malware which created havoc throughout the network. Also, uncontrolled Internet access took a toll on their productivity as it became more of a distraction than a useful tool.

Previously, we had been using Cisco products. So, we wanted a product that could match Cisco in security platform and Cyberoam did that

Cyber Threats

The threat of malware attacks from viruses, worms, Trojans, etc. kept the Capital FM IT team on their toes. These attacks could culminate into corrupt files, defaced web pages, PDFs and design documents, loss of critical data and system crashes resulting in huge downtime. Any such kind of an attack would cost Capital FM money, effort, man-hours and, in some cases, even their reputation.

The Cyberoam Solution

Mr. Kikata was on the lookout for a network security solution that would protect the Capital FM network from the 'inside' as well as the 'outside'. After looking into a number of security solutions, they found what they were looking for in Cyberoam. "Previously, we had been using Cisco products. So, we wanted a product that could match Cisco in security platform and Cyberoam did that," said Mr. Kikata. They deployed One (1) CR 100ia in Gateway Mode at their office in Nairobi's Central Business District.

After deployment of Cyberoam, the following business benefits were noticed.

Network Perimeter Barricaded

Identity forms the basis upon which security policies in Cyberoam are defined

Cyberoam's ICSA and Checkmark certified firewall provides granular access controls over Internet traffic and network resources. Users are given controlled access to network and internet resources, ensuring that no security loopholes are left open.

With a comprehensive database of 3000+ signatures, Cyberoam's Intrusion Prevention System protects Capital FM's data from several variants of spyware attacks, spoofing and DoS attacks in addition to keyloggers, Trojans and more.

Identity Based Security

Identity forms the basis upon which security policies in Cyberoam are defined. This identity-based security protects against insider threats by giving full visibility of user activities in the network. It is like monitoring exactly "Who is Doing What". Mr. Kikata integrated Cyberoam with an external Active Directory (AD) Server to take full advantage of Cyberoam's identity-based security. Now, he is able to keep a close watch on each user's activities in the network which enables him to make informed decisions about what security policies to implement.

Cyber Threats Kept at Bay

Cyberoam's identity-based filtering allows Mr. Kikata to set individual user Internet access policy, surfing quota, time limits and bandwidth restrictions.

Cyberoam's Gateway Anti-Virus & Anti-Spyware solution secures the Capital FM network by providing real-time protection against viruses, worms, Trojans, keyloggers, spyware and more on all web (HTTP, FTP) and mail (SMTP, POP, IMAP) traffic.

Controlled Internet Surfing

Cyberoam's 82+ categories tough Web Content filtering technology made it easy for Mr. Kikata to tackle the issue of unbridled surfing and downloading over the Internet by the employees.

Cyberoam's identity-based filtering allows Mr. Kikata to set individual user Internet access policy, surfing quota, time limits and bandwidth restrictions.

Cyberoam gave us more reason to smile since it acts as a long term solution for our security needs.

Cyberoam blocks inappropriate and unsafe Web content, including phishing and other malware-laden sites. This is done through a constantly updated database of millions of websites. Moreover, Cyberoam's identity-based filtering allows Mr. Kikata to set individual user Internet access policy, surfing quota, time limits and bandwidth restrictions.

Business Continuity Upheld

Cyberoam's Automatic Link Failover feature helps in upholding business continuity in Capital FM even in the face of an Internet-link outage. Capital FM uses 2 Internet links out of which one acts as the primary link while the other acts as a backup. In case of failure of the primary link, Cyberoam automatically redirects Internet traffic through the backup link without manual intervention. "Cyberoam's Automatic Link Failover helps in business continuity and considerably reduces the work load of the IT team", said Mr. Kikata.

To Conclude

"Cyberoam gave us more reason to smile since it acts as a long term solution for our security needs. We got more than what we were looking for," said Mr. Kikata.

Elitecore Product

Cyberoam
Unified Threat Management

www.cyberoam.com | sales@cyberoam.co