Cyberoam

Unified Threat Management

Case Study

Organization
Imperial Bank, Nairobi, Africa

Industry
Banking

Looking after your interest!

Martin Osonga
Sr. I.T. Security Officer
Imperial Bank

www.cyberoam.com

Cyberoam UTM Protects Mission-Critical Banking Systems in Imperial Bank, Kenya

Background:
Imperial Bank, Nairobi, Kenya established in March 1993, has been ranked amongst the top 10 Banks in Kenya by Market Intelligence. The bank has won the Financial Reporting Award four times, which is presented annually by the Institute of Certified Public Accountants of Kenya, Capital Markets Authority and the Nairobi Stock Exchange.

Imperial Bank places a high degree of importance on safe banking environment and applying the highest standards of business integrity, security and professionalism in all areas of the bank's activities.

Challenge:
Following the precedent of high standards set in their banking practices, the bank wanted to regulate the Internet access and secure the internal network in addition to securing branch connectivity.

Explaining the security and access control needs, Martin Osonga, Senior I.T. Security Officer at the Imperial Bank said, “We needed a Deep Inspection Firewall to control the Internet access. We also wanted to regulate the exposure of the servers placed in the DMZ the external world in addition to auditing them. This is a very important security aspect as we also provide Internet banking.”

“We were looking for content security,” added Mr. Osonga, “Which included intrusion prevention system, gateway anti-virus and anti-spam, and web content filtering solution. We wanted a secure way to connect our back office operations at the Head Office, to the branches spread over Kenya. So a VPN solution which supports high levels of encryptions and security was also the need of the hour.”

In spite of the multiple security needs, Mr. Osonga wanted a single, integrated solution, catering to all their requirements. He was particularly concerned about the web server deployed in the DMZ. The server catering to the Internet banking facility is a very sensitive resource which he wanted to be secured against any Denial of Service or an intrusion attempt.

“We must secure our core banking business data and resources against blended threats. You can say that this is our one and only requirement.” Mr. Osonga gave an example of what he meant by a blended threat, “Suppose, a user in my network receives a mail which contains a Trojan, intended to launch a DoS attack on my server; or a user, during unproductive surfing, accidentally downloads a key-logger intended to record the user names and passwords to our servers and sends the information back to its originator, it can be a disaster for the bank. In such a scenario, a single security feature individually cannot be effective. Multiple security features are required to mitigate such blended threats.”

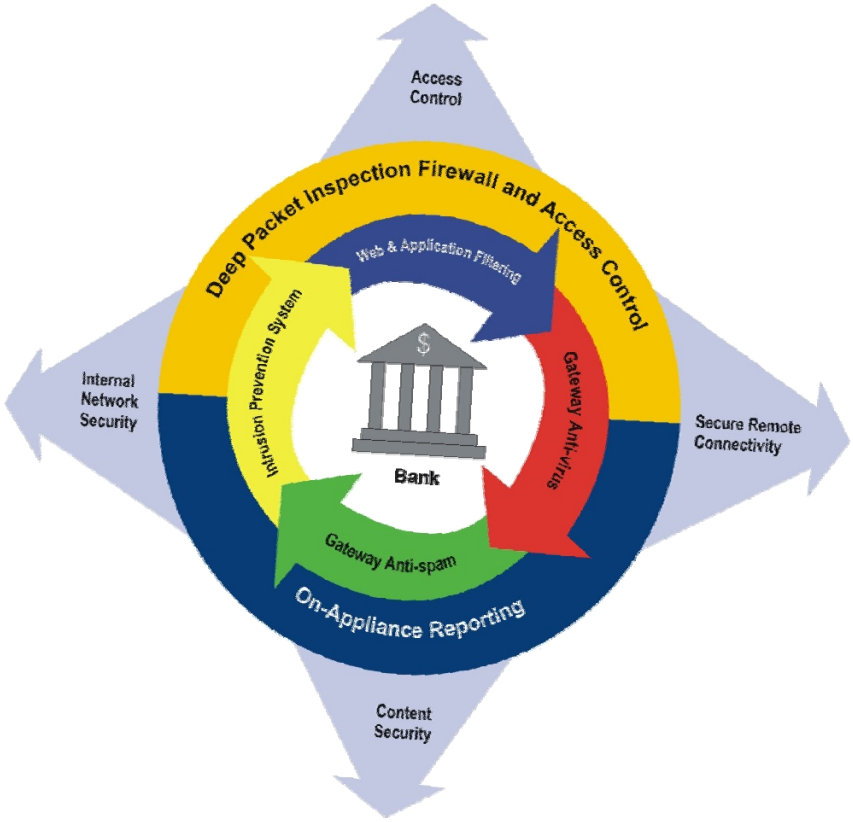
Solution:

Mr. Osonga scoured the market for a solution to fit their security needs. He initially used the spam and virus detection rates as bench marks. While Cyberoam had the best figures in the industry, during the evaluation, he found that the prompt response and strong technical assistance from Cyberoam was also an added advantage. He soon realized that Cyberoam's technical assistance will play a decisive role in his purchase decision due to its long term benefits.

Cyberoam helped us secure our core banking infrastructure against Internet-based blended threats.
- Mr. Osonga

Imperial Bank purchased a Cyberoam 250i UTM appliance, which is deployed in the Head office in the gateway mode. Mr. Osonga was impressed with Cyberoam's reports. Prior to Cyberoam, the bank had a firewall. "In an Internet security solution, you need good reporting feature to allow you to monitor the users' behavior and usage trends. With our previous firewall, I had to depend on third party solutions, which often were plagued by compatibility problems. Finding the right information became a long and tedious process. With Cyberoam I checked the reports first. For the first time I did not have to rely on external solutions and in no time, I had all the relevant reports. This saved a lot of my time, energy and efforts."

Cyberoam UTM Shield



On-Appliance Reporting feature of Cyberoam is one of its most impressive features. It helps us to gain perfect visibility of Internet usage trends and user behavior patterns.

Mr. Osonga found that the On-Appliance reporting feature of Cyberoam was richly loaded with various templates to provide complete visibility. The data in the reports helped him formulate firewall rules and security policies. He found Cyberoam GUI very user friendly as most of the options were placed within easy reach of the administrator.

The combination of firewall and Intrusion Prevention features of Cyberoam protected the Web server from external and internal intrusion attempts. This ensured that the bank's internet banking services ran flawlessly as the servers were secured against any internal or external attack. The same combination helped mitigate any DoS attacks. All IM and P2P traffic is blocked to ensure that no sensitive information is leaked and no malware enters the banking network.

Upon deployment of Cyberoam's gateway Anti-Spam, Mr. Osonga found that at least 30% of the total mail traffic was spam. The UTM effectively blocked the spam mails and the Imperial Bank employees were pleased to see clean inboxes.

Cyberoam's gateway Anti-Virus scanned the web and mail traffic for hidden malware. This protected the Internet users while surfing and no malware entered the core banking network from the Internet.

The web content filtering feature curbed harmful surfing and ensured that Internet usage was productive. Cyberoam is kept up to date automatically through continuous updates to help protect against the latest viruses, worms, Trojans and other blended threats.

Mr. Osonga is now in the next phase of deployment and plans to connect all the branches to the head office using Cyberoam's secure encryption VPN feature.

Firewall and IPS combination helps me secure my mission critical servers against internal and external intrusion attempts.

"Cyberoam deployment protects our mission-critical, banking system. Cyberoam UTM solution offers a large range of features, high performance and scalability. At the same time, it is easy to administer, helping us meet the growing needs of Imperial Bank effectively," concluded Mr. Osonga.

Cyberoam

USA - Sales Toll Free: +1- 866-663-2927 | Support Toll Free: +1-877-380-8531
India - Sales: +91-79-66065606 | Support Toll Free: 1-800-301-00013
EMEA/APAC - Sales: +91-79-66065787 | Support: +91-79-66065777