Cyberoam

Unified Threat Management

Case Study

Organization
ESBC LTD

Country
Nairobi, Kenya
Africa

Industry/ Vertical
ITeS

ESBC Servers contained applications and data which were under constant threat from spyware attacks. So they needed a strong Firewall and IPS solution.

-Mr. Frank Wamakonjio
ICT Manager
ESBC

http://www.cyberoam.com

Eden Square Business Center (ESBC) Confides Cyberoam for its Network Security

About ESBC LTD

ESBC opened it first serviced offices in Nairobi at the beginning of April 2006 to cater to the growing number of local and international businesses trying to break into or expand their businesses across the East African region. It is the first company in the region to provide such an extensive range of serviced and virtual office solutions.

ESBC aims to be the leading provider of serviced and virtual office solutions in Africa. These solutions will be a catalyst to the growth of enterprise and thereby make a significant contribution to the development of the continent.

The ESBC LTD Challenge

The ICT Manager, Frank Wamakonjio at ESBC outlined the basic requirements saying, “Internet is one of the most business critical resources for our organization.”

Mr. Wamakonjio was looking for a single box solution that would offer:

Securing the Perimeter

ESBC wanted to protect their servers by a strong firewall solution and access control management over all the WAN network resources.

Warding off Intrusion Attacks

ESBC was looking for an IPS tool to minimize the chances of cyber-criminals gaining visibility of internal network resources through hacking, remote exploits, Denial-of-service (DoS) attacks and other unpredictable attacks. The management was concerned that even a single successful intrusion could lead to unbearable consequences for their business. Moreover, any black-out of the network due to a DoS attack could cause the company to suffer significant revenue losses.

Malware and Spam Control

The organization was facing frequent breakdown issues due to annoying virus, root-kit, worm, Trojan and spyware infections. These malware attacks which often took a blended form through email attachments, PDF, Word documents etc. had the potential to corrupt useful files and destroy important data.

ESBC also wanted to secure its entire email network from newly emerging malware threats and reduce overall spam incidence. This was required to keep mails secure and in-boxes clean. The spam filtering was required to be totally automated and perform irrespective of the language and content of the mail with an absolute minimum amount of false positives - as no organisation can afford to lose a single business opportunity should a legitimate email be wrongly classified as spam.

Watching Website Access

The organization sought to keep an eye on and limit its users from accessing unproductive sites such as music, video, social networking, etc to help them in their work. Opening up access to these sites for all users resulted in bandwidth getting “choked”. They wanted a suitable content filtering solution with reporting feature for showing graphs and traffic results on specific sites accessed by its employees.

VPN Connectivity

ESBC has evolved into an organization with independent networks at remote sites supporting many users. The primary challenges for ESBC were to provide access to sensitive data across a more secure and stable VPN. Internet is relied on profoundly to allow remote sites VPN access back to the main office.

Cyberoam ICSA and Checkmark certified firewall - provides granular access controls over Internet traffic and the network resources.

Business Continuity Concerns

One major issue was the connectivity problem. "If Internet was down our business activities would come to a halt," Mr. Wamakonjio said. To avoid a single point of failure, multiple locations had multiple ISP links. So, multiple ISP links load balancing, and failover is also a critical need.

The Cyberoam Solution

In order to address their challenges, ESBC looked into a number of security products including Cisco ASA 5520 SSM AIP. However, after seeing a trial demo of Cyberoam, they took the decision of deploying the Cyberoam appliance – one (1) CR200i at the head office and two (2) CR50ia at the branch office in gateway mode.

The business benefits were as follows:

Firewall Protection

ICSA and Checkmark - dual certified Cyberoam’s stateful inspection firewall now cordons off the organization’s network against any unauthorized access. ESBC users are given controlled access to network and internet resources, ensuring that no security loopholes are left open.

Cyberoam’s Gateway Anti-Virus solution, with the industry’s best malware detection rates, scans mail and web traffic over the entire organization network

Barricading Intrusions

Mr. Wamakonjio used default IPS policies from the firewall rule to protect ESBC’s corporate network from DoS and spoofing attacks and other exploits. He also used IPS to protect their network, LAN and mail server from these intrusion attempts.

With a comprehensive database of 3000+ IPS signatures, Mr. Wamakonjio now feels that the company’s data is well protected from several variants of spyware attacks, spoofing and DoS attacks in addition to keyloggers, Trojans and more.

Solving the Spam and Malware Concern

Cyberoam’s Check Mark Certified anti-virus solution scans the Web surfing (HTTP, HTTPS, FTP) and mail traffic (SMTP, IMAP, POP3) to ensure that no malware sneaked in. All FTP transactions are also scanned for total security.

Check Mark certified anti-spam solution ensures that not a single mail made it to the internal inboxes. The spam is neutralized at the gateway. Continuous spam protection was installed and had instantaneous effect.

The Virus Outbreak Detection feature protected the organization for Zero Day Attacks and Vulnerability Exploits.

Following the Cyberoam appliance dictum of Quick-Configure-and-Fire, the intelligent anti-spam solution required almost no human intervention to put it on war footing. Signature-less Virus Outbreak Detection technology protects the organization against any mail-based Zero-Day attack, hours before traditional signature-dependent solutions.

Web Content Filtering

Cyberoam's 82+ category strong Web Content filtering technology kept the organization's internet resources productively focused. Mr. Frank said, "Being able to choose what sites to allow access to and what sites to block was an essential feature for ESBC when deciding on a Web filtering product." The IPS and Content filtering features ensure that all P2P is blocked and that there is no breach of data.

Cyberoam's Web filtering solution, with more than eighty two (82) categories ensures that the users of the Internet do not access pornography, violence and other harmful content on the Web

VPN Connectivity

The CR200i appliance deployed at the Head Office was used to ensure IPSec VPN connectivity along with the Two (2) CR50ia appliances at remote offices. This allowed remote office users to flawlessly access their work without any uncertainties of collapses in Internet traffic.

Threat-free Tunnelling (TFT)-driven VPN ensures that all such traffic is securely encrypted and no malware sneaks through it.

Continuous Data Availability

Driven by academic need of company's connectivity over Internet, the organization has (4) ISP links. Cyberoam's Multi-Link Manager intelligently load balances the traffic and manages link failover between the four (4) broadband links. These links terminate on Cyberoam. The Multi-Link Manager constantly monitors the performance of the links. In case of a link failure, the load is automatically transferred to the working link, seamlessly, which leads to 100% Internet uptime, and round the clock availability of requisite bandwidth. In case of a link failure, Cyberoam automatically switches the traffic to the working link. So the organization gets a transparent multilink management with no human interference.

Threat-free Tunneling (TFT)-driven VPN ensures that all traffic is securely encrypted and no malware sneaks through it.

To Round it Off

Cyberoam gave ESBC the choice to implement a one-window security-connectivity set-up across their whole enterprise infrastructure.