



## Organization

International Energy Services Limited (IESL)

## Country

Nigeria  
Africa

## Industry

Energy Services



The company contains sensitive information that can be possibly targeted by attacks from external entities and outside access attempts. Thus they needed a strong Firewall and IPS solution.

- Mr. Williams Oluwagbenro O  
IT Manager  
IESL

## Cyberoam UTM Solution Leaves Nothing to Chance for IESL

### About International Energy Services Limited (IESL)

Established in 1990, International Energy Services Limited (IESL) is an indigenous Energy Services Company set up with the aim of providing integrated and customer oriented services in the oil and gas industry with specialized expertise for both onshore and offshore developments.

IESL is involved in Engineering Designs, Pipelines, and PRMS, Oil & Gas Platforms and Facilities, Project Management & Inspection Services, Engineering Technical Services, Maintenance, Procurement, Construction and Contracting Services, Environmental/Analytical Laboratory, QHSE Consultancy Services, Solar & Power Engineering Services. It has assembled a highly qualified team of professionals with worldwide experience that can provide practical solutions to complex problems during all phases of engineering projects: - designs, structural and facilities upgrade/revamping, pipelines, gas plants, refineries, etc.

Internet is used as a lifeline as it is the principle business enabler and there can be no compromise when it comes to Internet connectivity and security, as it is the most productive resource. Thus, business cannot be run without Internet connections.

### The IESL Challenge

#### Uninterrupted Internet Connectivity

The varied business requirements of Internet are as follows:

- HR/Admin: The HR team/management uses Internet for administrative work.
- Design section: A team of designers require uninterrupted Internet connectivity to enable web transfer of huge CAD files containing parts and assemblies.

According to Mr. Williams Oluwagbenro O, the IT Manager at IESL, "Continuous Internet connectivity with no breakdown or downtime was the most important requirement for us. Apart from that, we also had to address these additional business challenges."

#### Securing the Periphery & Warding off Intrusion Attacks

Mr. Williams wanted a solution that would control the entire Internet traffic and establish clear-cut boundaries between the internal networks and the outside world. Servers in the internal networks hosted sensitive information related to their engineering projects and employee private details, which had to be protected.

They were also 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. Therefore, they needed a strong Firewall & IPS solution which would be capable in retorting these threats.

#### Scheming Surfing Practices

Unmanaged Internet access presents many challenges and introduces unnecessary risk. When workers inadvertently or deliberately access sites containing inappropriate, illegal, or dangerous content, use instant messaging (IM) and peer-to-peer (P2P) applications, they expose themselves to legal liability, and experience degraded network performance.

Continuous Internet connectivity with no breakdown or downtime was the most important requirement for IESL

ICSA and Checkmark - dual certified Cyberoam's stateful inspection firewall solution cordons off IESL's network and guards its servers against any unauthorized access.

Cyberoam's 82+ category strong Web Content filtering technology kept the organization's internet resources productively focused.

The organization needed to know who was accessing what sites and as such needed an identity based filter and reporting system that would include the users' online behavioral audit. Fixing a content filtering solution can do away with these problems.

### **Spam Control**

IESL 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 organization can afford to lose a single business opportunity should a legitimate email being wrongly classified as spam.

### **Load balancing & Failover**

Continuous Internet connectivity with no breakdown or downtime was the most important requirement for IESL. "IESL requires load balancing and reliable performance while providing sufficient bandwidth for employees to access web-based resources safely and securely," says Mr. Williams.

### **The Cyberoam Solution**

In order to address their challenges, IESL looked into a number of security products including GateProtect. However, after seeing a trial demo of Cyberoam, they took the decision of deploying the Cyberoam appliance – one (1) CR500ia at the head office in Lagos in gateway mode.

### **Identity based Security**

Cyberoam UTM comes with a unique identity-based security solution which protects against insider threats by giving complete visibility into "Who is doing What" in the network and allows creation of user identity-based policies. Mr. Williams used Cyberoam's Active Directory (AD) facility to achieve the task of integrating IESL's users in the network through a wizard to import users.

Moreover, the automated single-sign-on (SSO) feature of Cyberoam allows transparent authentication of the end users as soon as they boot their machines

### **Firewall & Stopping Intrusions**

IESL operates Cyberoam's ICSA and Checkmark Certified Perimeter Firewall between the Internet and the organization's network to establish a secure environment for the organization's computer and network resources. Coupled with Intrusion Prevention module, Cyberoam UTM can counter any Denial of Service attack. Mr. Williams now felt the network is secure.

### **Filtering Solution**

IESL installed Cyberoam not only to manage employee Internet access, but to minimize the risk of other web security threats. In addition, they chose Cyberoam to help improve employee productivity and save network bandwidth. IESL uses Cyberoam to block access to specific category of websites. They utilize the Cyberoam's reporting functionality to help identify organizational risk levels for productivity, security and network bandwidth loss trends.

Cyberoam's content filtering database has more than 44 million sites neatly categorized into more than 82+ categories. This large number of categories permits a high degree of specificity in designing an organization's Internet use policy.

Cyberoam reporting gives absolute visibility into “Who is doing What” in the network.

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

### Spam Free Internet

Cyberoam’s Check Mark Level 5 certified Anti-Spam solution offers 98% protection against zero-hour attacks with .0001% false positive rate, minimizing the threat of business mail loss.

Recurrent Pattern Detection (RPD) powered signature-less anti-spam technology works instantly on deployment, with the least human intervention and is language independent. Also, Reputation-based filtering makes decisions based on comprehensive information about the source of the message. Reputation filters rely on objective data to assess the probability that a message from any given IP address is spam. This saves a lot of bandwidth & protects users from spam, viruses, phishing, and spyware threats.

Moreover, it also blocks spam in any language regardless of the content, e.g. image, audio, video or zip-based spam. The anti-spam feature is also equipped with Virus Outbreak Detection. This protects the organization against any zero day attack.

### Round the Clock Connectivity

Cyberoam’s Multilink manager increases the overall network performance by load balancing the network traffic between their two (2) ISP links terminating on them, delivering continuity in security. In case of failure, the load is automatically transferred to the other ISP link, which leads to 100% Internet uptime, and round the clock connectivity to their employees.

### To wind up

“Of all the solutions we looked at, Cyberoam is definitely the best fit with our technology and our needs. We highly recommend them to any corporate that wants to get a lever on its security problems and prevent unauthorized intrusions, whether from outside or inside the network.” said Mr. Williams.



### Toll Free Numbers

**USA :** +1-877-777-0368 | **India :** 1-800-301-00013

**APAC/MEA :** +1-877-777-0368 | **Europe :** +44-808-120-3958

Copyright © 1999-2010 Elitecore Technologies Ltd. All Rights Reserved. Cyberoam and Cyberoam logo are registered trademark of Elitecore Technologies Ltd. Although Elitecore has attempted to provide accurate information, Elitecore assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Elitecore has the right to change, modify, transfer or otherwise revise the publication without notice.

