



## Organization

Al Wathba National Insurance Company

## Country

United Arab Emirates,  
Middle East

## Industry/ Vertical

BFSI



Internet is one of our most critical resources.

- Mr. Azhar M. Mousa  
IT Manager  
AWNIC

## Cyberoam Ensures Secure Internet Connectivity at AWNIC

### About AWNIC

Al Wathba National Insurance Company (AWNIC) is a United Arab Emirates-based company established in year 1997, and listed in Abu Dhabi Stock Exchange in 2000. AWNIC's Board is headed by H.E.SK. Saif Bin Mohammed Bin Butti as Chairman and Mr. Rashid Bin Darwish Al Ketbi as Dy.Chairman and Managing Director.

The company underwrites all types of General Insurance Products and is well supported by a panel of highly rated international Reinsurers. Its products and services include such insurances as: fire and general accident, property, motor, medical, and marine and aviation.

### The AWNIC Challenge

“Internet is one of our most critical resources”, said Mr. Azhar M. Mousa, IT Manager at AWNIC. They use Internet for maintaining their interactive website, business activities and general surfing. Also, they host their Online Insurance application on an internal Web Server which is accessed over Internet by clients, brokers and staff all over UAE. Hence, Mr. Mousa expressed, “Constant, uninterrupted and safe Internet connectivity is a must for AWNIC”. He had the following concerns regarding network security and Internet.

### Remote Connectivity Concerns

AWNIC has several branches spread all across UAE. Users at Branch Offices need to constantly remain in synchronization with the Head Office and with each other for efficient business continuity. Hence, safe and secure inter-office connections, in other words, VPN connections were of highest priority to Mr. Mousa.

### Onslaught of Malware and Spam

Business activities involved users surfing the Web, transferring files and exchanging emails. Hence, they were constantly exposed to the danger of malware infestation. These malware attacks, which often took a blended form through email attachments, PDF, design documents etc, had the potential to alter constructive files and destroy significant data. Simple day-to-day activities were often hampered when such malware infiltrated the system. As a result, productivity suffered as the IT department had to interfere to rectify the situation.

Like all financial institutions, AWNIC was a target for hordes of unsolicited Spam. Almost 40% of their incoming email traffic was Spam. It not only was a cause of constant harassment to employees, but also had a detrimental effect on AWNIC's network resources.

### Unbridled Web Surfing

“There are millions of potentially harmful websites harbouring illegal or inappropriate content, and so we needed to ensure that employees connecting to our network would be protected with the most advanced Web filtering technology.” said Mr. Mousa. They needed strong web filtering solutions which could control all Internet access and give informative reports on Internet usage.

After searching the market for competent security solutions, they decided to go with Cyberoam

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

Cyberoam's Gateway Antivirus and Antispyware features screen all web and mail traffic

## The Cyberoam Solution

AWNIC did have certain network security solutions in place, namely, WatchGuard solutions to protect their network gateway and MailMarshal to screen incoming and outgoing emails. But they were not satisfied with their performance and so, were looking for solutions that would stand up to their expectations. After searching the market for competent security solutions, they decided to go with Cyberoam.

They deployed Six (6) Cyberoam Appliances in their network, all in Gateway Mode. The appliances and their locations are given below. They purchased these appliances from Cosmos Computer Co LLC, partner to Cyberoam.

Appliance Model	Location
CR 200i	Abu Dhabi (Head Office)
CR 25ia	Abu Dhabi – Murror Traffic
CR 25ia	Abu Dhabi – Mussafah
CR 25ia	Al Ain
CR 25ia	Dubai
CR 25ia	Sharjah

After deployment of Cyberoam, Mr. Mousa noticed the following business benefits.

### Network Perimeter Firewalled

The Cyberoam firewall acts as a filter between the company's gateway and the Internet in order to block malicious attempts to access the network, and allow only legitimate traffic. ICSA and Checkmark - dual certified Cyberoam's stateful inspection firewall solution now cordons off Awnic's network and guards its servers against any unauthorized access. The organization's users are given controlled access to network and internet resources, ensuring that no security loopholes are left open.

### Remote Connectivity Secured

"Thanks to Cyberoam, I am able to extend business operations at Branch Offices while simultaneously protecting our internal systems", said Mr. Mousa. The Cyberoam appliance deployed at the Head Office is used to facilitate IPsec VPN connectivity along with the Cyberoam appliances at Branch Offices. This allows remote office users to seamlessly access Head Office resources without security worries. Cyberoam's Threat-free Tunneling (TFT)-driven VPN ensures that all such traffic is securely encrypted and no malware sneaks through it.

### Web Surfing Reined In

Cyberoam UTM's web content filtering feature controls Internet access in the entire organization by blocking inappropriate and unsafe Web content, including phishing and other malware-laden sites. This is done through a constantly updated database of millions of sites divided into 82+ categories including pornography, P2P, entertainment and job search. "Cyberoam's Content Filtering feature has helped in increasing the overall employee productivity of our organization", said Mr. Mousa.

### Mitigating Malware and Spam Onslaught

Cyberoam's Gateway Antivirus and Antispyware features screen all web and mail traffic, and make sure that no malware or spyware creeps through the edge. Additionally, the Antivirus blocks attachments for specified file types such as executables, media files, PDF, zipped files etc. before these blended threats can harm the network.

Cyberoam managed to meet all our network security requirements. It came as a pleasant treat after disappointment from other security solutions

Recurrent Pattern Detection (RPD) powered signature-less Antispam technology works instantly on deployment, with the least human intervention and is language independent. It blocks spam in any language regardless of the content, e.g. image, audio, video or zip-based spam. The Antispam feature is also equipped with Virus Outbreak Detection. This protects the organization against any zero day attack.

### To Draw a Close

“Cyberoam managed to meet all our network security requirements. It came as a pleasant treat after disappointment from other security solutions”, said Mr. Mousa.



### 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.

