

Organization

Al Shafar General Contracting LLC

Industry

Construction



Mr. Surendran Pariyanghat
(IT Manager, ASGC)

ASGC needed comprehensive Internet Security and robust VPN solutions for their Head Office and remote Construction sites.

www.cyberoam.com

Cyberoam VPN Provides Un-Interrupted Business Security and Connectivity in a Fully Dynamic Environment

Case Study of Al Shafar General Contracting LLC (Dubai)

Background

Al Shafar General Contracting (ASGC), a flagship company of the Al Shafar group, is Dubai's leading building contractor company. Their construction gamut covers high-rise towers, residential complexes, factories, shopping malls, palaces, universities, hotels, retail developments and ancillary services.

With Head Offices in Dubai and Abu Dhabi, ASGC has constructions interests spread over far flung places in United Arab Emirates.

The Challenge

Seamless and cost effective business connectivity with the remote construction sites spread across UAE through the Internet was the primary need of ASGC. This business requirement can be drilled down to two basic technical requirements:

- The Head Office and the Remote Construction sites and Branch Offices ought to be connected over the Internet through a Virtual Private Network (VPN). VPN Connectivity to the remote construction sites is of vital business importance. The regular day-to-day functioning on the sites, instant on-site updates and implementations are solely dependent on the VPN connectivity between the Head Office and Branch Offices.
- ASGC needed an Internet Security Solution to provide security over the Internet at the Head Office and at the remote sites.

While the office interconnectivity through Internet was a recent requirement, the Internet security was taken care of by a pure firewall solution. Mr. Surendran Pariyanghat, the IT Manager at Al Shafar found that the blended threat scenario required a gateway level comprehensive Internet security solution which included a Firewall, Gateway Anti Virus, Anti Spam, Intrusion Detection and Prevention and Web Content Filtering.

Talking about VPN, Surendran said, "The main challenge for any VPN solution lay in the DDNS-based networking environment which demanded a robust architecture and proactive support. We were looking for a solution that would work under the most trying technical and environmental circumstances. Our business connectivity depended on it."

The main challenge for any VPN solution lay in the Dynamic DNS-based networking environment which demanded a robust architecture and proactive support.

Short DDNS update interval and Enhanced Dead Peer Detection features of Cyberoam VPN ensured correct update of DDNS IP addresses in spite of Internet connectivity fluctuation, frequent power outages.

The Head Office and the Branch Offices/ Construction Sites are connected through the same ISP, with a limited pool of IP addresses. Al Shafar's Head Office and remote offices use ADSL links and Dynamic DNS to connect to the Internet. The DDNS IP addresses are leased to a site during the Internet link's up-time.

The challenges faced in site-to-site VPN connectivity are:

- **Erroneous update of DDNS IP addresses** - The DDNS needed constant update through HTTP (Internet). The multiple HTTP proxies deployed with the ISP, sometimes stripped vital information from the network packet. This results in an erroneous update of DDNS IP addresses. Without valid IP addresses on both sites, a site-to-site VPN tunnel cannot be established.
- **Connectivity fluctuation** - High fluctuation of ISP Link connectivity causes the DDNS IP address to be reassigned to another site. In case of a connectivity outage, ADSL redials the PPPOA and on getting the connectivity, it is assigned a new DDNS IP address. If the link connectivity fluctuates, the IP address update does not remain in sync.
- **Power outages** - Repeated power outages at remote construction sites lead to improper shutdowns. Once the power is restored, the VPN device would be up and functioning, while the ADSL router might still not be ready. Such sequence of booting causes VPN tunnel failure.

The complexity is compounded as there are no trained IT professionals on the remote sites to locally trouble-shoot. This demanded that the solution be inherently robust and be backed up by a strong and proactive post-sales support.

Cyberoam Solution

ASGC turned to Bulwark Technologies for a solution. As per their advice they have deployed three (3) Cyberoam CR 50i appliances in the Head Office and ten (10) CR 25i appliances at remote construction sites. As new construction sites keep coming, the tally of Cyberoam appliances keep going up.

One appliance at the Head Office was dedicated to gateway security, while the other two appliances were used to connect to the remote construction sites over site-to-site, IPsec VPN tunnels. Around fifteen (15) Cyberoam's CR 25i appliances are deployed at remote sites spread across UAE. These appliances are used to connect to the Head Office through VPN.

Robust VPN Architecture

Cyberoam's short DDNS update interval ensures that, in spite of frequent link connectivity fluctuations, the IP address is always in sync for both the peers in a site-to-site VPN tunnel.

The robust architecture of Cyberoam's VPN has Enhanced Dead Peer Detection feature which checks the peer constantly. If the remote office is unreachable after a stipulated number of tries to re-establish the tunnel, the Head Office switches to listening mode and the peer at the remote office tries unlimited times to reach the Head Office. Once the link comes up, the tunnel is instantly established.

Both these architectural facets of Cyberoam UTM take care of recurrent power outages, link connectivity fluctuation and multiple IP address reassignments.

Cyberoam UTM's Content Filtering solution has curbed all the malicious and unproductive surfing within the organization. Anti Spam solution has given great relief - clean inboxes.

Technical Support

The dearth of on-site technical staff did not hinder Cyberoam's proactive support. Using road warrior connection, they gained access to remotely deployed Cyberoam appliances to troubleshoot them. Cyberoam support found that a few ADSL routers were port forwarding incorrectly. The determined Cyberoam support team restarted the routers remotely to maintain uninterrupted business connectivity for ASGC.

“Cyberoam UTM's VPN solution and support are excellent. In the initial stages of the deployment support identified and isolated all the technical bottlenecks and resolved them. They ensured that all our VPN tunnels were up round-the-clock. The product stability and robustness gives us good Return Over Investment. We are so satisfied with Cyberoam UTM, that in the current phase, we have made it mandatory to deploy a new Cyberoam UTM at each new remote construction sites.” said Surendran.

Comprehensive Internet Security

Cyberoam UTM appliances deployed at the Head Office had identity-based Firewall, Gateway Anti Virus, Gateway Anti-Spam, Intrusion Detection and Prevention and Web Content Filtering security features which provided comprehensive Internet security cover.

“The Content Filtering solution has curbed all the malicious and unproductive surfing within our organization. Anti Spam solution has given us a great relief clean inboxes,” Surendran concluded, checking his mail.