

# SECURE OUT-OF-BAND MANAGEMENT OF CRITICAL INFRASTRUCTURE AT THE ENTERPRISE BRANCH OFFICE

ROBERT WALDIE, OPENGEAR UK

As the enterprise pushes into the cloud, it is important to remain mindful of the distributed IT and communications assets that are fundamental to day-to-day operations. The widespread adoption of IaaS solutions to virtualize back office infrastructure has alleviated some of the management and maintenance headaches associated with physical IT infrastructure, however it is by no means a silver bullet.



## The out-of-band imperative

From telephony, conferencing and underlying networking hardware, to back up power systems and desktop PCs, the enterprise is reliant on a disparate array of systems from a multitude of vendors. These systems form the backbone of day-to-day operations across various locations, and faults and failures can leave an enterprise hamstrung.

It is therefore critical to develop a strategy that addresses the secure monitoring and control of these systems, that enables fault notification, instant remediation and secure out-of-band access when problems do occur, in order to safeguard business continuity.

A complete out-of-band management solution must have integrated physical connectivity to disparate systems, provide a uni-

fied management interface for these systems, offer enterprise-grade security features with the ability to integrate seamlessly with existing authentication and data encryption systems, and be cost-effective to deploy with minimal on-going costs.

## Distributed site challenges

Distributed sites typically have few or no on-site staff available to resolve problems with critical infrastructure in a timely manner, further compounding the problem of costly downtime. Distributed sites are increasingly reliant on IT managed solutions providers to look after their infrastructure – in the case of enterprise branch offices, the solutions provider may be the internal IT services department.

This represents an acute vulnerability to business continuity, making the development and implementation of an out-of-band management strategy all the more important.

For branch office or satellite sites, the requirement for out-of-band management is two-fold – access to the site through a dedicated out-of-band connection at the network edge, and out-of-band access to the IT and communications infrastructure at the site.

### Out-of-band at the edge

The first of these requirements is often addressed by means of a backup DSL circuit or redundant fibre channel, that provides failover network connectivity to the entire site in the event of loss of connectivity via the primary link. However, the example of a routing change at the ISP or core router necessitating an emergency configuration change at the distributed site, illustrates that this is not good enough.

What is required is an inbound access path wholly separate from the principal means of site connectivity. A dedicated management device with integrated out-of-band connectivity, such as cellular wireless or PSTN modem, at each branch office site, is a cost effective and reliable way to meet this requirement.

It is imperative to secure out-of-band management traffic with enterprise-grade security, such as IPsec VPN with x.509 certificate authentication and strong cryptography – even more so if the out-of-band link is routed over the WAN or other public network.

### Infrastructure & device management

IT and communications equipment vendors have gone some way to facilitate the out-of-band management of their systems, by equipping them with dedicated management interfaces.

Networking and communications equipment, such as routers and IP PBX systems, typically provide an RS232 serial console port for direct access to the configuration and management CLI. Many also provide a dedicated management NIC for IP access to a GUI or CLI – in particular managed switches, firewalls and load balancers.

The traditional out-of-band management path for server infrastructure is also by way of an RS232 serial console with BIOS redirection, or legacy bolt-on KVM over IP device. Modern servers are equipped with a specialized lights-out management NIC, such as iLO from HP, IMM and RSA from IBM, and ALOM from Sun, providing virtual KVM, power control and systems monitoring capabilities over IP.

The third class of critical infrastructure found at branch office sites are the smart power devices – UPS back-up power systems, and intelligent PDU strips. Again, connectivity to these devices varies across vendors and models, with a combination of RS232 serial, Ethernet network and USB.

Power monitoring and control is a cornerstone of remote infrastructure management, for notifications when systems have switched over to back up power, notifications when batteries require replacing – and, crucially, enabling remote systems to be powered off and on. The protocols and MIBs to interrogate and control power devices vary dramatically across the different makes and models of power equipment typically found scattered across distributed locations.

To connect to and communicate with this multitude of management interfaces, an out-of-band infrastructure management solution must be geared towards interconnection and interoperability.

### Enforcing enterprise security policy

When deployed, a unified infrastructure management solution is not just a single interface for operational monitoring and control, it is also a single point where security policy may be applied.

Security audits reveal that these management back doors are often configured with default or weak credentials – an alarming vulnerability at nerve centre of the enterprise. As well as this, the complexity of enforcing a unified security policy across a disparate array of management interfaces results in these invaluable tools for out-of-band management and rapid problem remediation remaining disconnected or disabled.

Of particular concern is that embedded systems such as those found in networking, communications and power equipment are now seen as soft targets by malicious parties. The complexity of keeping firmware up to date with the latest security patches means such systems are increasingly falling victim to targeted exploits. Many are powered by low power microcontrollers that are simply not up to the task of providing enterprise grade encryption, and are easy prey for network DOS attacks.

Such concerns have led to the development and growing adoption of ISO 27001 standards for Information Security Management, which mandates the total separation of corporate and management networks.

To address these security concerns and ensure ISO 27001 compliance, an infrastructure management gateway is required to terminate all management interface connections – be they network, serial, or USB – and securely broker all communications between the management interfaces and the management client. This single point of access can then authorize all access against a core authentication server using protocols like TACACS+ and LDAPS, and enforce enterprise policy such as two-factor authentication.

To ensure security and accountability best practice, a management solution must also store audit trail logs of access attempts, transcripts of management sessions, and alert central operators when malicious patterns are detected.

### Conclusion

Opengear's unique range of Advanced Console Manager and Infrastructure Manager appliances are purpose built to deliver secure out-of-band management of critical infrastructure across all enterprise locations, and address the vulnerabilities woven in the fabric of the distributed enterprise.

Opengear integrates with enterprise data encryption and authentication systems to extend enterprise security policy for secure management of distributed assets, while built-in out-of-band and redundant connectivity options ensure high availability to safeguard business continuity.



#### **ROBERT WALDIE, VP BUSINESS DEVELOPMENT (UK & EUROPE)**

*Robert Waldie manages the Opengear UK operation and is responsible for technology partnering, channel development, marketing strategy, channel sales training and technical support there and in Europe. Prior to setting up the UK operation Robert led the Opengear software development team. Before Opengear working as a software engineer with*

*Secure Computing /Cyberguard / Snapgear and BRDC developing embedded Linux security and network applications. Robert holds a BSc in Computer Science and a BA in Linguistics from the University of Queensland.*