SatCom For Net-Centric Warfare November 2008

MilsatMagazine

Mission Critical — Secure Satellite Networking

IN THIS ISSUE

Locking the Back Door...

...To Distributed Satellite Networks

by Bert Wilhelm, UPLOGIX

Satellite communications represent a cost-effective and reliable means of transporting voice, video, and data to and from remote locations. However, as the adoption of satellite based networks continues to grow, so do the security challenges for operational and IT staff. Maintaining network connectivity and availability, preventing outside intrusions especially from foreign grounds, and closing the loop on vulnerabilities due to natural disasters and power outages, have all become mission critical components to managing the remote infrastructure at the edge. Even more critical is having secure, always-available access to the remote infrastructure, especially when the network is compromised.

Should you lose your network connection, one of the most commonly used forms of access control is through ***out-of-band*** (**OOB**) connections, which have been largely unaddressed from a security standpoint. When a problem arises with an enterprise network connection via satellite, the OOB connection acts as the 'back door' to provide a secondary means of accessing devices and systems if the primary connection has been lost.

Unfortunately, OOB connectivity for remote console management has not seen the same degree of security improvements that have been made to production networks. For example, access to an OOB connection may require only a static username and password and the connection may not be encrypted. This is a risky practice because remote administration requires access to the device console. If the unsecure OOB connection is hacked, then the thief has console access to the network equipment and/or servers. This means 'carte blanche' to execute operations and changes to the devices and could gain access to other parts of the network. If configuration changes or updates don't work, it's critical to be able to retrace the steps that were taken. If contractors or other third parties do work, logging provides a record of their activities.

ECLIPSE
SATELLITE ROUTERS
EFFICIENT BROADBAND SOLUTIONS
secure reliable satellite platform for mission critical applications.
AAE
www.aaesys.com
info@aaesys.com
408.732.1710

Entering the picture is a new technology called ***secure remote management*** (**SRM**). SRM brings new functionality and intelligence that takes an integrated approach to solving the OOB security predicament. SRM does this by locking the ‘back door’ to ensure internal security and management policies are always enforced, even during a network outage.

Secure Remote Management: Locking the Back Door

Compared with traditional network and systems management tools that rely on the network and remains labor-intensive, secure remote management combines the localized control and connectivity of a console server with the intelligence of an enterprise software solution. The platform ‘front-ends’ a remote office’s equipment by safeguarding against the vulnerability of the OOB dial connection, allowing only outbound dialing or answering calls when the primary connection has been lost. Secure remote management controls access to routers, switches, and servers by enforcing AAA policies and integrating with IAM systems.

Schlumberger, one of the world’s leading oil services company, was faced with the challenge of maintaining constant connectivity with isolated locations. Communications between customers’ remote sites, such as offshore oil rigs, and Schlumberger’s land-based teleports is conducted via VSAT satellite communications, which are often interrupted due to rain-fade and other types of unavoidable interference. An out-of-band solution was required that could maintain constant communications and manageability even when the main communications link was down or disrupted.

Implementing secure remote management has allowed IT staff to automate network fault diagnosis and recovery, as well as perform routine network maintenance (such as the configuration and provisioning of devices). SRM ensures network availability, even when the primary connection is down. Furthermore, if the main broadband satellite link goes down or is disrupted, the secure remote management appliance deployed at the disconnected remote location automatically dials out to a low earth orbit (LEO) satellite via an integrated external modem to re-establish an alternate, out-of-band network connection.

Losing access to your distributed network or being blind-sided by internal security threats has been greatly overlooked. By locking the back door with new secure remote management practices, military and energy organizations now have access and control regardless if the network is up or down — putting IT staff at ease knowing they aren’t the easiest target on the block.

About the author

Bert Wilhelm is the Director of Product and Technical Marketing at Uplogix and can be reached at bwilhelm@uplogix.com.

Uplogix puts the power of your most trusted IT admin everywhere, all the time.

Omaha

No support staff required at "lights out" data center

Proactive maintenance capabilities give offsite administrators control of routine system maintenance, keeping the lights out and the data flowing.

How Secure Remote Management Works

As secure remote management (SRM) appliances are deployed at remote locations, they can locally manage a wide variety of networking gear, including switches and routers, intelligent racks, and power and environmental control systems.

To ensure the SRM appliances can communicate during a network outage, a secure and reliable alternative communication path is designed into the architecture. Through this direct connection to the console (serial) ports of the remote devices, the appliance can query the connected devices every few seconds, storing the data locally.

As the data is stored locally and doesn't need to be transmitted on a regular basis, there isn't a cost penalty for sampling frequently. Detailed event logs are available on an as-needed basis to help with problem resolution. Once a sufficient repository of data has been gathered, it can then be analyzed. For an SRM appliance polling console ports at a remote location, the amount of data to indicate a problem can usually be gathered in 30 seconds or less.

Once the data has been gathered, a policy engine inside the appliance determines if a parameter is in or out of specification, and either resolves the incident based on pre-approved guidelines, or communicates the problem back to the network management center.

Once a problem signature is recognized, the SRM appliance can take steps to automatically resolve the incident and restore the service.

In addition to restoring network connectivity, the logged and stored management data enable IT and service providers to establish root cause that required the reboot so it can be avoided in the future, or established as a routine device issue that the SRM appliance is authorized to address automatically.

Unexpected downtime is always a possibility during software upgrades of network hardware. In some cases, the devices fail to boot after a new software load, thereby requiring a reliable and secure way to backtrack. In these cases, the SRM appliance needs to be able to restore the last-known-good-configuration automatically. The local control logs can then be examined once the network has been restored to understand what caused the network aberration.

Management actions and associated logging data exchanged between the NOC and the remote sites should be safeguarded. Designing a remote management platform with a robust AAA (authentication, authorization, and audit) security model, combined with the physical properties of a specific purpose appliance, ensures the protection of the systems and network devices and the network itself. This way, all actions are logged and stored locally, giving visibility to all management actions to these devices.