Resilience Gateway from Opengear

PRODUCT REVIEW PRODUCT REVIEW PRODUCT R

Support professionals working in large distributed networks depend heavily on remote access to critical infrastructure devices, but this can present problems. While it frees them from lengthy on-site visits, access will be interrupted in the event of network failure and security can also become a concern.

The Opengear Resilience Gateway overcomes these issues as it provides secure remote access to all critical network devices, from any location, even when the main network is down. If the WAN link at a remote site fails for any reason, it can switch over to a high-speed 4G LTE cellular network for out-of-band (OOB) management access.

The Resilience Gateway provides dual LAN ports, four RJ-45 serial ports for device connectivity and four USB ports for monitoring UPS devices. The front slot accepts a cellular SIM card which Opengear claim is a substantial differentiator; it's 4GB of internal Flash memory stores all the user and device access logs.

Initial setup in the lab was simple and we used the well-designed web interface to secure administrative access and configure the cellular network. For the latter, you can set it to automatically activate when the primary network link goes down or leave it on permanently.

IP pass-through is a handy feature because if the remote site's WAN connection fails, this device acts as a redundant gateway. In this mode, all site traffic is transparently routed through the appliance, allowing the site to gain Internet access via the cellular network.

Access security is tight because the Resilience Gateway essentially provides a single sign-on service for managed devices. With support staff providing one set of credentials, the appliance provides access only to those devices that they have permission for.

For serial port management, we connected HP ProCurve switches and a Dell SonicWALL firewall directly to the appliance using DB9 to RJ-45 converters. For each port, we defined basic details such as the baud rate and flow control, chose a logging level and decided what types of access would be permitted.

The Resilience Gateway supports an excellent range of options and we could choose from Telnet, SSH, raw TCP, RFC 2217, web terminal and more. They then appeared in the serial port list in the web interface along with their associated access options and the status of any active users.

We also tested using an APC Smart-UPS 1000 UPS connected directly to one of the appliance's USB ports. This took seconds to configure after which the web console offered full details on areas such as battery charge time, input and output voltages and load.

User and group access controls are impressive, offering a huge range of authentication methods including TACACS, RADIUS, LDAP and Kerberos. Strong security is central with PCI-DSS, FIPS140-2, SSL and SSH, stateful firewall, OpenVPN and IPsec. We easily determined which ports each user could manage and their permitted access methods.

The Auto-Response feature associates conditions with trigger and resolve actions. Conditions range from environmental issues, UPS status, or a disconnected serial cable, and these in turn can trigger email, SMS or SNMP alerts and then run a custom script.

Accessing our network devices from the appliance's web console was simple and we could even define server IPMI management ports as RPC devices and remotely control their power supplies. Using PuTTY we could also SSH to the appliance and select serial ports from its menu to activate a secure serial session to our HP switch CLIs.

The Resilience Gateway is an ideal solution for time-poor support staff managing geographically distributed networks. It's easy to use, it offers extremely tight remote access security and its cellular backup link avoids ever losing contact with critical network devices again. NC

Product: Resilience Gateway
Supplier: Opengear
Web site: www.opengear.com
Telephone: +44 (0)208 133 4255
Email: sales@opengear.com
Price: £678 excluding VAT