Shell Control Box (SCB)

BalaBit

DEVELOPER'S STATEMENT

The Shell Control Box by BalaBit is an activity monitoring solution for privileged access that controls access to remote servers, virtual desktops, or networking devices, and records the activities of the users accessing these systems.

One of the two BalaBit products to be reviewed under West Coast Lab's (WCL) new Performance Validated program is Shell Control Box (SCB). As with syslog-ng Store Box, the SCB test allowed WCL to provide an independent review of the solution.

To test SCB, WCL was provided with a x2200 Sun Microsystems server running SCB. WCL also tested a virtual version of SCB.

Testing of the SCB solution was conducted on a custom-built network at WCL's UK facility. The network itself consisted of a variety of client and server machines running a range of both Windows and Linux-based operating systems.

WCL downloaded SCB from the BalaBit website as a virtual machine, then SCB was imported onto a server running VMPlayer. Before full deployment, SCB requires basic network configuration (Host IP address, gateway address, and so on) and the license is imported to SCB at the end of the initial configuration.

SCB is an independent appliance designed to integrate with ease, offering high availability and is configured via a clean, intuitive web interface. The roles of each SCB administrator are clearly defined using a set of privileges. SCB receives connection attempts for a specific target host then forwards the connection. The solution enables the creation of rules allowing the administrator to permit or deny connections based on set criteria, and provides for the auditing of network connections. SCB also works in conjunction with BalaBit's Audit Player to allow logged network traffic to be replayed in real time and supports the following protocols: Secure Shell (SSH), Remote Desktop (RDP), Telnet and terminal emulators using the standard TN3270, VNC and VMware View. WCL only examined the following during the test period: VNC, RDP, SSH, and Telnet.

Product
Shell Control Box (SCB)
Manufacturer
BalaBit
Contact Details
www.balabit.com
Certification
www.westcoastlabs.com

The recorded audit trails can be replayed like a movie using the aforementioned Audit Player enabling a review of events exactly as they occurred. The audit trail is indexed to make searching for events and automatic reporting possible, enabling identification of misconfigurations and other human errors during forensics analysis. SCB works in conjunction with network firewalls and can supplement further security devices benefiting network and IT security administrators by controlling all remote connections on a given network.

SCB acts as a proxy gateway, and any transferred connections and traffic are inspected on the application level (Layer 7 in the OSI model) giving control over protocol features such as the authentication and encryption methods or permitted channels.

In order to test SCB it was necessary to establish inbound connections over a network to a specific machine. VNC, SSH, RDP and Telnet connections were established; each of the connection types and combinations were tested using access control lists.

These included machines with various access permissions and, once connections had been established, WCL also tested the solution's ability to terminate the connections successfully. WCL then replayed the network traffic logs through the Audit Player for verification.

westcoast labs
PERFORMANCE VALIDATED

WEST COAST LABS VERDICT

Testing of the SCB virtual machine showed that all connections were received and handled correctly, the administrator was able to terminate established connections and the logged files were 100% accurate. Tests also showed the capability of Audit Player to recreate the data from the session in an accurate movie-like format.