MONITOR PRIVILEGED ACCESS TO LEGACY NETWORK DEVICES

Shell Control Box Use Case

The Challenge – Audit Telnet Connections

Many large enterprises operate obsolete network infrastructure with countless outdated devices. If you are a manager of a mature telecommunication firm, you can be particularly affected, since you may also operate thousands of legacy devices, such as old routers, gateways, switches, and so on. Typically, these network devices are remotely managed via Telnet protocol by accessing the hardcoded shared account (for example, "administrator") of the device. However, these accounts hold superuser privileges and are often shared among your network operators. Thus, operating such devices causes the following risks:

Sharing passwords

If multiple operators can access the same privileged account, you can never know who did what on a device. For example, an accidental misconfiguration of a mission-critical router can cause serious service outage - without knowing the responsible party and the root-cause of the incident. The turnover of network administrators can cause a further headache for you, as leaving employees take all administrator passwords with them, unless you change these passwords after every time an operator leaves your company, or changes role.

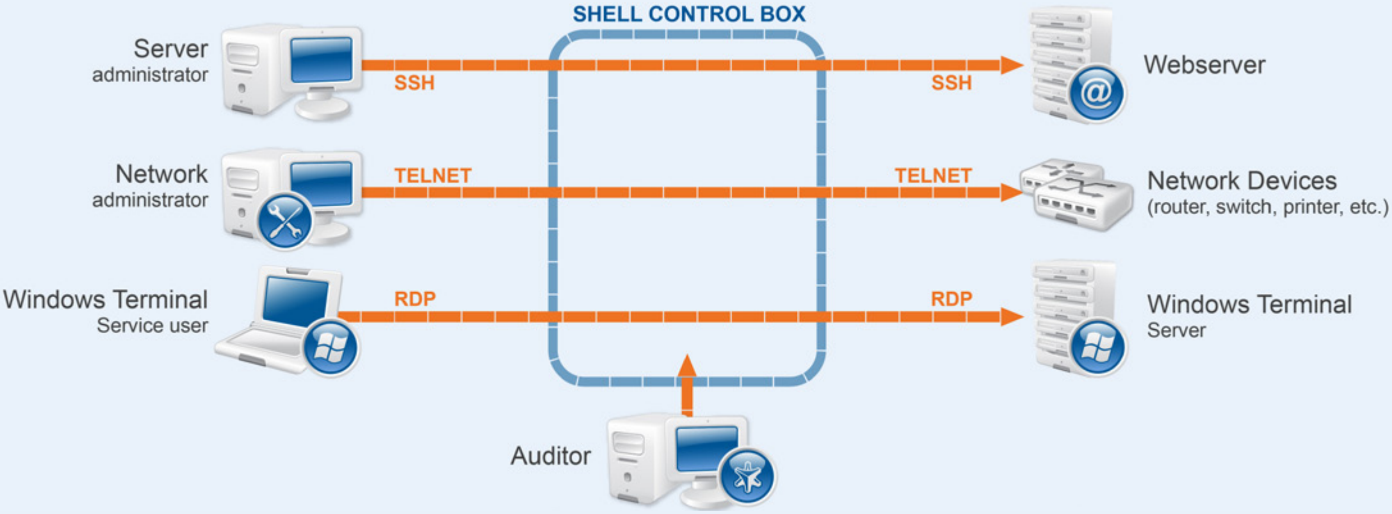
Insufficient logging

Many legacy network devices do not generate event logs. Even if the device supports logging, these logs are typically not detailed enough for fast troubleshooting. Furthermore, your operators - accessing the administrator account on the device - have the capability to erase any trace of their actions from these logs.

All in all, your legacy telecommunication devices can be operated by many "unknown" (internal or external) administrators, whose activities are not monitored. Without a proper audit solution in place, you are not able to answer the question of "who managed what and why?" in your old telecom network.

The Solution – Telnet Audit Device

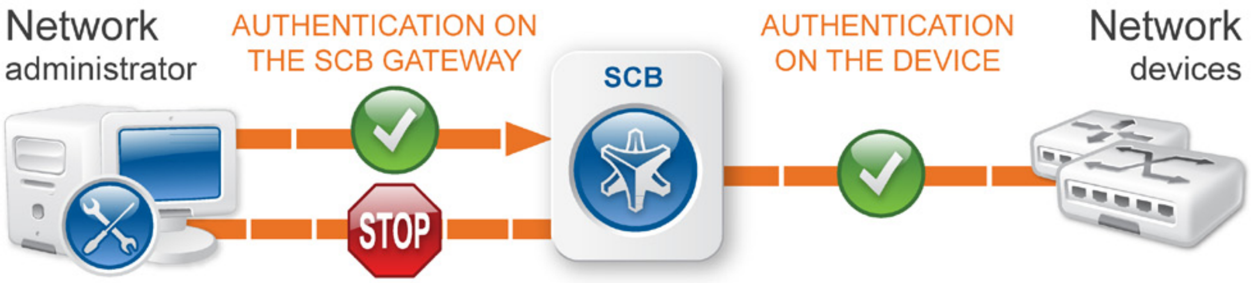
In such situations, it is reassuring to have an independent device that can reliably audit Telnet-sessions. The BalaBit Shell Control Box (SCB) is an activity monitoring appliance that controls privileged access to your remote networking devices, and records activities in searchable and re-playable audit trails. SCB is a single tool that transparently controls and monitors operator actions performed via widely used administrative protocols, such as Telnet, TN3270, SSH, RDP, VNC or Citrix. You do not need to change your existing network environment, and your operators can do their day-to-day jobs without changing their working habits.



Gateway authentication and usermapping

SCB can require performing gateway authentication, meaning that your network operators must authenticate on SCB as well. In addition, SCB can enforce the use of strong authentication methods (for example public keys), which are typically not supported by legacy devices. Telnet connections can be authenticated to a central authentication database such as LDAP or RADIUS as well. In addition, connections using general usernames (for example “Admin”) can be connected to real user accounts.

User-mapping policies can be also defined. This describes who can use a specific username to access the remote device: only members of a specified user group (for example “operators”) can use the specified username (for example “admin”).


Network administrator
AUTHENTICATION ON THE SCB GATEWAY
STOP
SCB
AUTHENTICATION ON THE DEVICE
Network devices

Destination Selection

SCB supports in-band destination selection in Telnet connections - the operator can type the address of the target device and the username during the gateway authentication process. You do not need to maintain a target host database in SCB, as is in the case with jump host solutions.

Credential Store

A credential store offers a way to store user credentials (for example, admin passwords) and use them to login to the target device, without the user having access to the credentials. In this way your operators only have to authenticate on SCB with their usual password. If the operator is allowed to access the target device, SCB automatically logs in to the target device using the password from the credential store.

Encryption

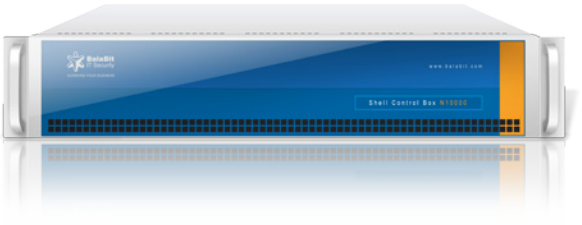
SCB allows you to control and audit Telnet sessions that are encrypted using TLS or SSL. Additionally, it can even encrypt the unencrypted communication between the client and SCB, if needed for data-security reasons. This is important, as many Telnet devices can be accessed only via unencrypted connection.

Fast audits and forensics

SCB makes all operator activities traceable by recording them in high quality and confidential audit trails. SCB replays the Telnet sessions just like a movie – all actions of the operators can be seen exactly as they appeared on their monitor. The Audit Player enables searching for events (for example, typed commands or pressing Enter) and texts seen by the user. In the case of any problems (firewall manipulation, unexpected shutdown, etc.) the circumstances of the event are readily available in the trails, thus the cause of the incident can be easily identified. By generating custom activity reports, audit process is supported further and corrective actions can be made.

Real-time alerting and blocking

SCB can also monitor the Telnet traffic in real-time, and execute various actions if a certain pattern (for example, a suspicious command or text) appears in the command line or on the screen. This functionality helps you prevent malicious operator activities as they happen instead of just recording or reporting them. For example, you can configure the appliance to block the “enable” command, thus preventing the operator to enter privileged mode on Cisco devices.



To summarize, SCB reliably controls and monitors your network operators managing Telnet devices, which increases security and facilitates compliance in your legacy network.

Telecommunication customers using BalaBit products:

orange telenor interoute fon MTS DATA BASE FACTORY T-Systems

About BalaBit

BalaBit IT Security is an innovative information security company, a global leader in the development of privileged activity monitoring, trusted logging and proxy-based gateway technologies. We help protect customers against internal and external threats and meet security and compliance regulations.

BalaBit is also known as “the logging company”, based on the company’s flagship product, the open source log server application, which is used by more than 850 000 companies worldwide and became the globally acknowledged de-facto industry standard.

BalaBit, the fastest-growing IT Security company in the Central European region according to Deloitte Technology Fast 50 (2012) list, has local offices in France, Germany, Russia, and in the USA, and cooperates with partners worldwide. Our R&D and global support centers are located in Hungary, Europe.

Learn More

Shell Control Box homepage   SCB Case Study - Telenor   Request an online demo   Request a callback