

# Shell Control Box 3.0

## Product Description



**BalaBit**  
Shell Control Box



## Introduction

Shell Control Box (SCB) is an activity monitoring appliance that controls access to remote servers, virtual desktops, or networking devices, and records the activities of the users accessing these systems. For example, it records as the system administrators configure your database servers through SSH, or your employees make transactions using thin-client applications in VMware View. The recorded audit trails can be replayed like a movie to review the events exactly as they occurred. The content of the audit trails is indexed to make searching for events and automatic reporting possible. SCB is especially suited to supervise privileged-user access as mandated by many compliance requirements, like PCI-DSS. It is an external, fully transparent device, completely independent from the clients and the servers. The server- and client applications do not have to be modified in order to use SCB; it integrates smoothly into the existing infrastructure.

SCB logs all administrative traffic (including configuration changes, executed commands, etc.) into audit trails. All data is stored in encrypted, timestamped and signed files, preventing any modification or manipulation. In case of any problems (server misconfiguration, database manipulation, unexpected shutdown) the circumstances of the event are readily available in the audit trails, thus the cause of the incident can be easily identified. The recorded audit trails can be displayed like a movie – recreating all actions of the administrator. All audit trails are indexed on a separate indexing-server, enabling fast forwarding during replay, searching for events (for example, mouse clicks, pressing the Enter key) and texts seen by the administrator. Reports and automatic searches can be configured as well. To protect the sensitive information included in the communication, the two directions of the traffic (client-server and server-client) can be separated and encrypted with different keys, thus sensitive information like passwords are displayed only when necessary.

SCB can also remove the encryption from the traffic and forward the unencrypted traffic to an Intrusion Detection System (IDS), making it possible to analyze the contents of the encrypted traffic. That way traffic that was so far inaccessible for IDS analyzes can be inspected real-time. Other protocols tunneled in SSH can be inspected as well. Similarly, the list of files transferred and accessed in the encrypted protocols can be sent to a Data Leakage Prevention (DLP) system.



## Application areas and typical end-users

### Policy compliance

Compliance is becoming more and more important in several fields – laws, regulations and industrial standards mandate increasing security awareness and the protection of customer data. As a result, companies have to increase the control over and the auditability of their business processes, including server administration and remote system access. Regulations like the Sarbanes-Oxley Act (SOX), the Payment Card Industry Data Security Standard (PCI-DSS), the Health Insurance Portability and Accountability Act (HIPAA), or the Basel II Accord all mandate the strict protection of sensitive information – be it personal data, credit card information, or other. Such data is usually stored in a database on a central server, and is accessible only via dedicated applications, such as the accounting software. These applications always create the logs and reports necessary for policy compliance. However, these applications are aware only of legitimate accesses to the database. The server storing the database has to be accessible also by server administrators for maintenance reasons. Having superuser privileges on the server, these administrators have the possibility to directly access and manipulate the database, and possibly even to erase the traces of such actions from the server logs. However, SCB can audit the actions of the administrators, and as SCB is independent from both the administrators and the administered servers, offers a unique way to complement the logs and reports of other applications.

### Organizations having outsourced IT

Many organizations hire external companies to configure, maintain, and oversee their servers and IT services. This essentially means that the organization is willing to trust the administrators of this external company with all their data (for example, private and business e-mails, customer information, and so on), or even with the operation of business-critical services, like the online shop of the company. Obviously, in such situations it is reassuring to have an independent device that can reliably log all administrative activities. SCB does exactly this – it provides detailed information about any problems with the server, making it easy to find those responsible. Using the 4-eyes authorization method, SCB provides real-time control over the remote server access and the administrative actions.

### Organizations offering remote management

Organizations on the other end of the outsourcing line – like server- and webhosting companies – can equally benefit from SCB. It gives them the possibility to oversee and audit the administrators, and is also a great tool to evaluate their effectiveness. The recorded audit trails can also be used as evidence to settle any issues about the remotely administered servers. SCB also improves the control over Service Level Agreements (SLA), as the fulfillment of the services can be verified using the recorded audit trails and access reports.

## Organizations using thin-client infrastructures

SCB can audit the protocols used in popular thin-client solutions (for example, RDP, VMware view), providing an application-independent way to record and monitor the activities of every client.

## Real-time file transfer and file access monitoring

SCB can send the content of certain channels to an external Data Leakage Prevention (DLP) system that can recognize, track and alert on the access (data at rest) and transfer (data in motion) of sensitive data. That way the DLP policy of the organization can be extended to the – so far uncontrolled – encrypted protocols like SSH and SFTP.

## Organizations in need to control SSH

Many organizations have to permit outgoing SSH connections, but do not wish to do so without control, as virtually any other protocol can be tunneled into SSH. SCB can control what type of traffic is permitted in an SSH connection, and can separately enable the different traffic types like terminal connections, SFTP file transfers, port- and X11 forwarding, or agent-forwarding. It is also possible to extract the transferred files from SFTP and SCP connections for further analysis.

## Organizations using jump hosts

Many organizations use jump hosts to access remote servers or services. SCB can be used to authenticate and audit every access to the jump hosts. Since SCB can support strong authentication methods (for example, X.509 certification based authentication) and authentication to user directories (for example, Microsoft Active Directory and other LDAP databases), it can greatly simplify the key and password management of the hosts. This is especially useful if an organization has to access very many remote hosts, or has lots of jump hosts.

## Public references

The list of companies and organizations using the BalaBit Shell Control Box includes:

- Dubai Islamic Bank PJS (<http://www.dib.ae/>) – United Arab Emirates
- FIDUCIA IT AG (<http://www.fiducia.de/>) – Germany
- Hungarian Post Co. Ltd. (<http://www.posta.hu>) - Hungary
- Svenska Handelsbanken AB (<http://www.handelsbanken.com/>) – Sweden
- Wilo SE (<http://www.wilo.de>) - Germany



# Product features and benefits

- Oversee and audit the work of system administrators
- Control SSH (including X11 forwarded), RDP5, RDP6, RDP7, VMWare View, VNC, Telnet, and TN3270 connections
- Audit SCP and SFTP connections, list file operations, and extract transferred files
- Collect reliable information for forensics situations
- Fine-tuned access control to your servers and audit trails
- SCB is independent from the servers and clients, and difficult to compromise
- Easy integration into your existing infrastructure
- 4-eyes authorization for remote system- and data access
- Supports High Availability
- Manage easily from a web browser
- Automatic data archiving and backup

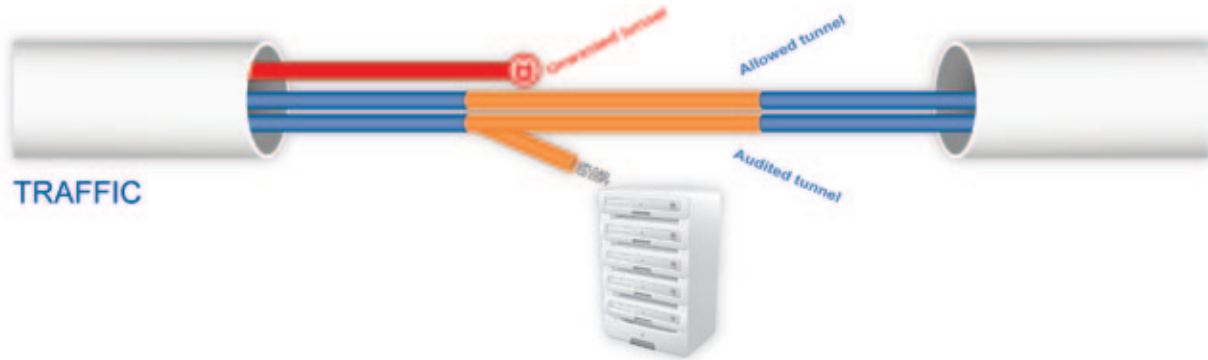


## Business benefits:

- Comply with regulations and policy mandates
- Accountability of remote access and data transfers
- Better and easier control of SLAs
- Proactive, technical and psychological control to prevent unwanted and malicious access
- Detailed access reports
- Savings on troubleshooting and IT forensics situations

## Protocol inspection

SCB acts as an application level proxy gateway: the transferred connections and traffic are inspected on the application level (Layer 7 in the OSI model), rejecting all traffic violating the protocol – an effective shield against attacks. This high-level understanding of the traffic gives control over the various features of the protocols, like the authentication and encryption methods used in SSH connections, or the channels permitted in RDP traffic.



## Supported protocols

SCB supports the following protocols:

- The Secure Shell (SSH) protocol (version 2) used to access Unix-based servers and network devices
- The Remote Desktop Protocol (RDP) versions 5, 6, and 7 used to access Microsoft Windows platforms, including 2008 Server and Windows 7,
- The X11 protocol forwarded in SSH, used to remotely access the graphical interface of Unix-like systems
- The Telnet protocol used to access networking devices (switches, routers) and the TN3270 protocol used with legacy Unix devices and mainframes
- The Virtual Network Computing (VNC) graphical desktop sharing system commonly used for remote graphical access in multi-platform environments.
- The VMware View application used to access remote virtual desktops (currently only direct connections using the RDP display protocol are supported).

## Traffic inspection and auditing with SCB

SCB records all sessions into searchable audit trails, making it easy to find relevant information in forensics or other situations. Audit trails can be browsed online, or followed real-time to monitor the activities of the administrators. All audit trails stored on SCB and the archiving server are accessible from SCB's web interface. The Audit Player application replays the recorded sessions just like a movie – all actions of the administrators can be seen exactly as they appeared on their monitor. Audit trails are indexed by a separate indexing-server. This makes the results searchable

on the SCB web GUI. Audit player enables fast forwarding during replays, searching for events (for example, mouse clicks, pressing Enter) and texts seen by the administrator. It is also possible to execute searches on a large number of audit trails to find sessions that contain a specific information or event. SCB can also execute searches and generate reports automatically for new audit trails.

In addition to recording audit trails of the inspected protocols, embedded protocols (for example, other protocols tunneled in SSH, port-forwarding) and transferred files can be recorded as well. Recorded files from SCP and SFTP connections can be extracted for further analysis. It is even possible to convert the audited traffic into packet capture (pcap) format to analyze it with external tools.

To prevent manipulation and provide reliable information for the auditor, SCB timestamps, encrypts and signs all audit trails. The audit trails are compressed; idle connections do not consume disk space.

## Achieve reliable auditing

Auditing is usually based on the logs generated on the audited server. This model is inherently flawed, as logs of interactive events are usually not too detailed, and there is no way to ensure that the logs stored on or sent by the server are not manipulated by an administrator or attacker. But SCB is an independent device that operates transparently, and extracts the audit information directly from the communication of the client and the server. This prevents anyone from modifying the audited information – not even the administrator of SCB can tamper the encrypted audit trails. SCB also generates detailed changelogs of any modification of its configuration.

## Detailed access control – who, when, how, from where can access which server

SCB allows you to define connections: access to a server is possible only from the listed client IP addresses. This can be narrowed by limiting various parameters of the connection, for example, the time when the server can be accessed, the usernames and the authentication method used in SSH, or the type of channels permitted in SSH or RDP connections. Controlling the authentication means that SCB can enforce the use of strong authentication methods (public key), and also verify the public key of the users. Also, SCB can authenticate the users to an external user directory. This authentication is completely independent from the authentication that the user performs on the remote server.

The following parameters can be controlled:

- The IP address of the client machines allowed to access the server.
- The group of administrators permitted to access the server (based on username black- and whitelists or LDAP groups) when using SSH or RDP6 with Network Layer Authentication.
- In addition to the authentication performed on the remote server, it is also possible to require an additional, outband authentication on the SCB web interface. Authorization can be based on this outband authentication as well.
- The authentication method (for example, password, public-key, certificate) required to access the server using SSH.
- The time period when the server can be accessed (for example, only during working hours).
- The type of the SSH or RDP channel permitted to the server (for example, SSH terminal or port forward, RDP file sharing, and so on).

The above rules can be applied both on the connection level and the channel level. That way access to special channels can be restricted to a smaller group of administrators – only those will have access who really need it.

## 4-eyes authorization

To avoid accidental misconfiguration and other human errors, SCB supports the 4-eyes authorization principle. This is achieved by requiring an authorizer to allow the administrators to access the server. The authorizer also has the possibility to monitor the work of the administrator real-time, just like they were watching the same screen.

The 4-eyes principle can be used for the auditors as well: SCB can use multiple keys to encrypt the audit trails. In this case, multiple decryption keys are needed to replay the audit trails, so a single auditor on his own cannot access every information about your systems.

## Verify the identity of the servers

SCB has the built-in capability to verify the SSH host keys and certificates identifying the servers, preventing man-in-the-middle attacks and other manipulation.

## Retain all data for over a year

SSH and Telnet terminal sessions that take up the bulk of system-administration work are the most interesting type of traffic for auditing purposes. But such traffic typically does not take up much space on the hard disk (only about 1 MB per hour, depending on the exact circumstances), so SCB can store close to 500.000 hours of the system administrators activities. That means a company who constantly has 50 administrators working online (7x24) can store all SSH and Telnet sessions on SCB for over 1 year – in searchable, replayable, readily accessible format. And these figures do not include the data archived on the remote backup server, which are equally accessible from SCB. RDP sessions take up considerably more space (but usually under 1 MB per minute), meaning that SCB can store the data of several weeks of work.



# Integrating SCB into your network

To make integration into your network infrastructure smooth, SCB supports different operation modes: bridge, router, and bastion mode. To simplify integration with firewalled environments, SCB supports both source and destination address translation (SNAT and DNAT).

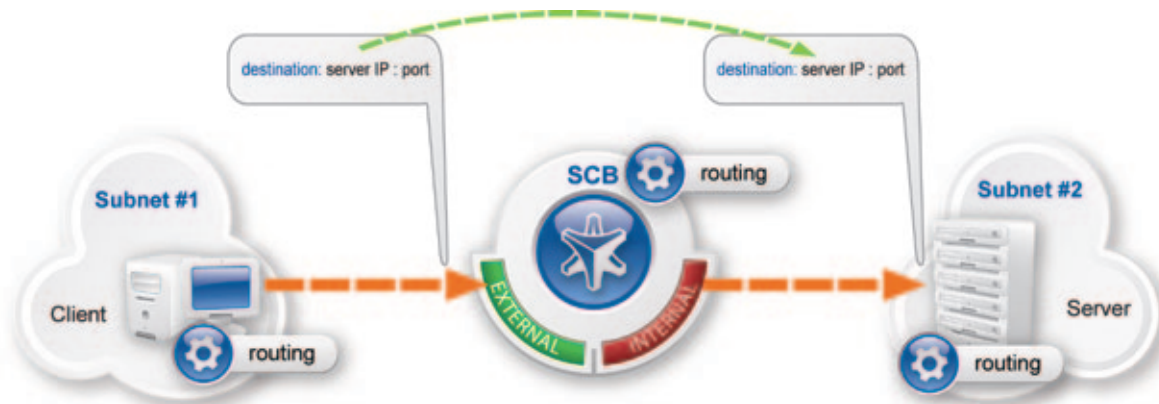
## Bridge mode

In Bridge mode, SCB acts as a network switch, and connects the network segment of the administrators to the segment of the protected servers at the data link layer (Layer 2 in the OSI model).



## Router mode

In Router mode, SCB acts as a transparent router connecting the network segment of the administrators to the segment of the protected servers at the network layer (Layer 3 in the OSI model).



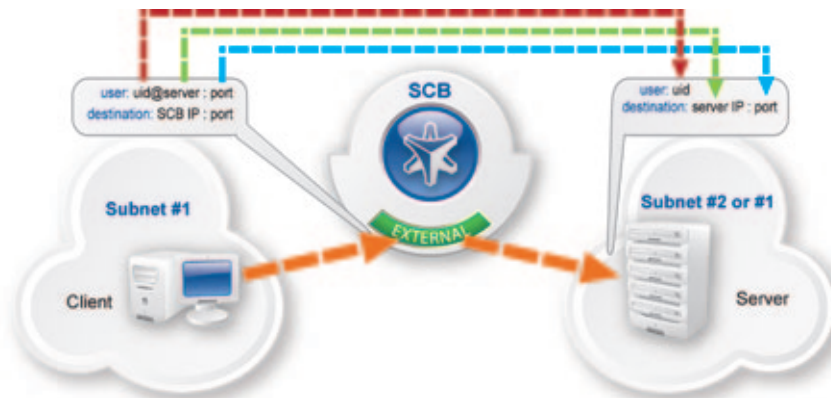
## Bastion mode

Administrators can address only SCB, the administered servers cannot be targeted directly. The firewall of the network has to be configured to ensure that only connections originating from SCB can access the servers. SCB determines which server to connect based on the parameters of the incoming connection (the IP address of the administrator and the target IP and port).



## Nontransparent operation

SCB can operate in nontransparent mode as well, extracting the address of the target server from the inspected protocol itself. Nontransparent operation is mainly used in Bastion mode, and simplifies the integration of SCB into the network infrastructure.



## Integration to user directories

SCB can connect to a remote LDAP database (for example, a Microsoft Active Directory server) to resolve the group memberships of the users who access the protected servers. Rules and policies can be defined based on group memberships. When using public-key authentication in SSH, SCB can authenticate the user against the key or X.509 certificate stored in the LDAP database.

Administrators and auditors accessing the web interface of SCB can also be authenticated to an LDAP database. RADIUS authentication (for example, using SecurID) is also supported both for accessing the web interface, and also to authenticate the audited SSH sessions.

## Managing SCB

SCB is configured from a clean, intuitive web interface. The roles of each SCB administrator can be clearly defined using a set of privileges:

- manage SCB as a host;
- manage the connections to the servers;
- view the audit trails and reports, and so on

Access to the SCB web interface can be restricted to a physically separate network dedicated to the management traffic. This management interface is also used for backups, logging to remote servers, and other administrative traffic. Users accessing the web interface can be authenticated to an LDAP or a RADIUS database. All configuration changes are automatically logged; SCB can also require the administrators to add comments when they modify the configuration of SCB. SCB creates reports from the configuration changes, and the details and descriptions of the modifications are searchable and can be browsed from the web interface, simplifying the auditing of SCB.

## High Availability support

SCB is also available with high availability (HA) support. In this case, two SCB units (a master and a slave) having identical configuration operate simultaneously. The two units have a common file subsystem; the master shares all data with the slave node as soon as the data is received: every configuration change or recorded traffic is immediately synchronized to the slave node. If the master unit stops functioning, the other one becomes immediately active, so the protected servers are continuously accessible. SCB1000d and larger versions are also equipped with dual power units.

## Automatic data and configuration backups

The recorded audit trails, the configuration of SCB, and every other data can be periodically transferred to a remote server using the following protocols:

- Network File System protocol (NFS);
- Rsync over SSH;
- Server Message Block protocol (SMB/CIFS).

The latest backup – including the data backup – is easily restored via SCB's web interface.

## Automatic data archiving

The recorded audit trails are automatically archived to a remote server. The data on the remote server remains accessible and searchable; several terabytes of audit trails can be accessed from the SCB web interface. SCB uses the remote server as a network drive via the Network File System (NFS) or the Server Message Block (SMB/CIFS) protocol.

## Software upgrades

Software upgrades are provided as firmware images – upgrading SCB using the SCB web interface is as simple as upgrading a network router. SCB stores up to five previous firmware versions, allowing easy rollback in case of any problems.

## Support and warranty

Support and software subscriptions for SCB can be purchased on an annual basis in various packages, including 7x24 support and on-site hardware replacement. Contact BalaBit or your local distributor for details.

## Hardware specifications

SCB appliances are built on high performance, energy efficient, and reliable servers that are easily mounted into standard rack mounts.

### **BalaBit Shell Control Box N1000**

- 1xQuad Core CPU, 4 GB RAM, 1 TB HDD – RAID1.
- Software license to audit 10 servers, upgradeable to unlimited servers.

### **BalaBit Shell Control Box N1000d**

- 2xQuad Core CPU, 24 GB RAM, redundant power supply, 1 TB HDD – RAID1.
- Software license to audit 10 servers, upgradeable to unlimited servers.

### **BalaBit Shell Control Box N10000**

- 2xQuad Core CPU, 24 GB RAM, redundant power supply, 10 TB HDD in internal storage, RAID 50.
- Software license to audit 50 servers, upgradeable to unlimited servers.

### **BalaBit Shell Control Box VA**

- Virtual appliance to be run under Vmware ESXi
- Software license to audit 5 servers, upgradeable to unlimited servers.



## Free evaluation

A fully-functional evaluation version of SCB is available as a VMware image upon request. An online demo is also available after registering on our website.

**TO TEST THE BALABIT SHELL CONTROL BOX, REQUEST AN EVALUATION VERSION AT [HTTP://WWW.BALABIT.COM/MYBALABIT/](http://www.balabit.com/mybalabit/)**

To learn more about commercial and open source BalaBit products, request an evaluation version, or find a reseller, visit the following links:

- The syslog-ng homepage: <http://www.balabit.com/network-security/syslog-ng/>
- The Shell Control Box homepage: <http://www.balabit.com/network-security/scb/>
- The syslog-ng Store Box (SSB) homepage: <http://www.balabit.com/network-security/syslog-ng/log-server-appliance/>
- Product manuals, guides, and other documentation: <http://www.balabit.com/support/documentation/>
- Request an evaluation version: <https://www.balabit.com/mybalabit/>
- Find a reseller: <http://www.balabit.com/partnership/commercial/>

## New since version 3.0

Version 3.0 of the Shell Control Box was released in September, 2010. To learn about new features since this release, visit <http://www.balabit.com/network-security/scb/whatsnew/>

### ***New in SCB 3.1***

- SCB 3.1 supports the Terminal Services Gateway Server Protocol, so SCB can act as a Terminal Services Gateway (also called Remote Desktop Gateway), receiving connections using the Terminal Services Gateway Server Protocol and transferring them to the target servers using the RDP protocol.
- SCB 3.1 supports the Citrix ICA protocols. Reliable connections also known as Common Gateway Protocol (CGP) are also supported. SCB can also act as a SOCKS proxy to permit inband destination selection and the use of connection brokers.

