AUDIT

PRIVILEGED WEB ACTIVITIES

Shell Control Box Use Case

> "WITHOUT AUDITING ADMINISTRATIVE WEB-TRAFFIC, YOU CAN LOSE SLEEP IF YOU RELY SOLELY ON THE RELIABILITY OF YOUR NETWORK ADMINISTRATORS."
> – ZOLTÁN GYÖRKŐ, CEO, BALABIT IT SECURITY

Who manipulated my firewall?

Network and system administrators are a potential security risk in many situations. They have high or even unrestricted access to your networking devices, operating systems or virtualization infrastructure. Typically, the web interfaces of these systems can be accessed and remotely managed via HTTP/HTTPS protocol. In these cases, network administrators can, for example:

- remotely configure your firewall, router or other network devices,
- set privileges on your Windows server, or
- manage your virtual machines in a VMware vSphere or Citrix XenServer environment.

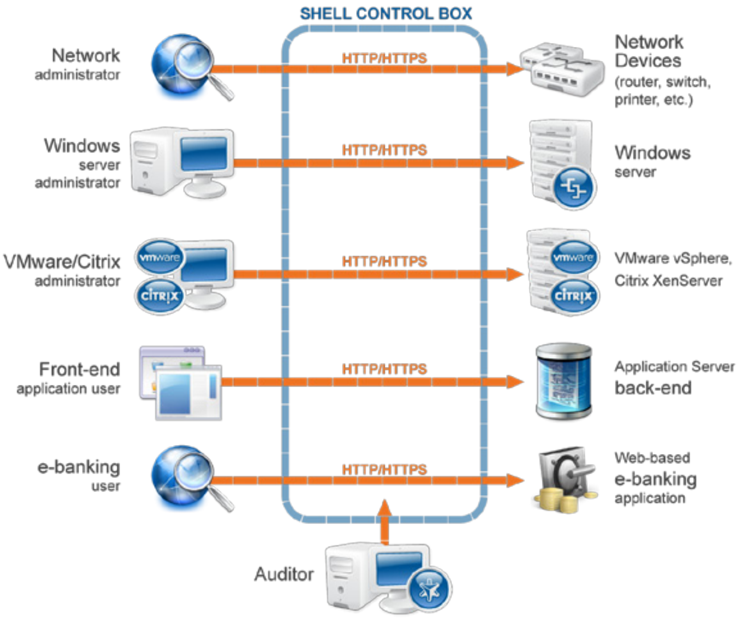
Without a proper audit solution in place, these actions remain uncontrolled. Furthermore, several administrators typically access the same administrative account, sharing the account password, which could not be treated as secure anymore. Consequently, it is very hard to answer questions such as "who manipulated my firewall configuration and why" or "who stopped my VMware machine".

Who did what in the e-banking system?

Beyond administrators, there are several users in your network, who have privileged access to your sensitive business applications, such as the e-banking system or the customer service front-end. In many cases, these applications are web-based and accessible via HTTP(S) connection. The problem is similar: if the user accidentally – or intentionally – modifies sensitive data (for example, customer records) in these applications, he/she can cause great damage to your business. In addition, these custom applications typically do not create sufficient logs, making forensics investigations costly and circumstantial. As a result, answering questions such as "who did what in the e-banking system?" is more than challenging again.

The Solution – HTTP Audit Device

In such situations it is reassuring to have an independent device that can reliably audit HTTP-sessions. The BalaBit Shell Control Box (SCB) is an activity monitoring appliance that controls privileged access to remote servers and networking devices and records activities in searchable and re-playable audit trails. SCB is a single tool to transparently control and monitor user actions performed via widely used administrative protocols, such as SSH, RDP, Telnet, VNC or Citrix. SCB 3 F4 extends the control and auditing functionality to the HTTP and HTTPS protocols, as well, to record administrative access to the web interfaces of various devices and applications, such as routers, firewalls or web-services. As illustrated on Figure 1, SCB can record as your network administrator configures your router or your Windows admin performs administrative tasks on a remote Windows system.* You can also audit as your VMware administrator manages the vSphere infrastructure or your customer service employee makes transactions in the front-end application.

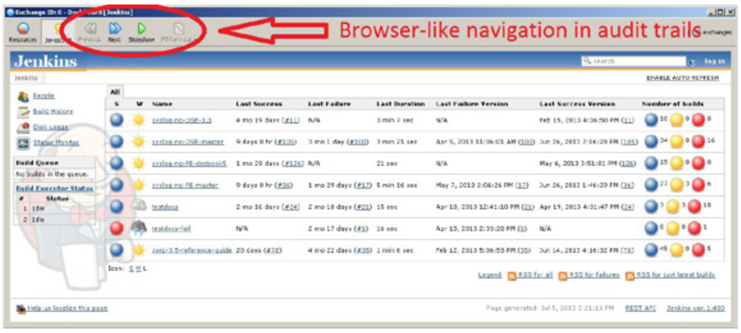


SHELL CONTROL BOX
Network administrator
HTTP/HTTPS
Network Devices (router, switch, printer, etc.)
Windows server administrator
HTTP/HTTPS
Windows server
VMware/Citrix administrator
vmware
CITRIX
HTTP/HTTPS
vmware
CITRIX
VMware vSphere, Citrix XenServer
Front-end application user
HTTP/HTTPS
Application Server back-end
e-banking user
HTTP/HTTPS
Web-based e-banking application
Auditor

Figure 1. Audit of HTTP/HTTPS traffic by Shell Control Box

Technical implementation

SCB records the complete HTTP traffic between the client and the device and renders the visited webpages. Then, you can access a human readable audit trail, in which you can track the actions of the monitored user, as if you were using a web-browser (Figure 2). The audit trails are indexed, making it possible to search the content of the communication, for example, to find specific POST requests or transferred files.



#	Status
1	Idle
2	Idle

S	W	Name	Last Success	Last Failure	Last Duration	Last Failure Version	Last Success Version	Number of builds
●	☀	syslog-ng-OSE-3.3	4 mo 19 days (#11)	N/A	3 min 7 sec	N/A	Feb 15, 2013 4:36:50 PM (11)	● 10 ● 0 ● 0
●	☀	syslog-ng-OSE-master	9 days 0 hr (#105)	3 mo 1 day (#100)	3 min 21 sec	Apr 5, 2013 11:06:01 AM (100)	Jun 26, 2013 2:06:28 PM (105)	● 34 ● 0 ● 16
●	☀	syslog-ng-PE-docbook5	1 mo 29 days (#126)	N/A	21 sec	N/A	May 6, 2013 3:51:01 PM (126)	● 15 ● 0 ● 0
●	☀	syslog-ng-PE-master	9 days 0 hr (#36)	1 mo 29 days (#17)	5 min 16 sec	May 7, 2013 2:06:26 PM (17)	Jun 26, 2013 1:46:29 PM (36)	● 27 ● 3 ● 6
●	☁	testdocs	2 mo 16 days (#24)	2 mo 18 days (#21)	15 sec	Apr 10, 2013 12:41:10 PM (21)	Apr 19, 2013 4:01:47 PM (24)	● 3 ● 3 ● 18
●	☂	testdocs-fail	N/A	2 mo 17 days (#1)	16 sec	Apr 10, 2013 2:33:20 PM (1)	N/A	● 0 ● 0 ● 1
●	☀	zorp-3.5-reference-guide	20 days (#78)	4 mo 22 days (#35)	1 min 6 sec	Feb 12, 2013 5:06:53 PM (35)	Jun 14, 2013 4:16:32 PM (78)	● 45 ● 0 ● 5

Icon: S M L

Legend RSS for all RSS for failures RSS for just latest builds

Help us localize this page

Page generated: Jul 5, 2013 2:21:15 PM REST API Jenkins ver. 1.480

Figure 2. HTTP-session audit

Auditing HTTP and HTTPS connections is possible in both transparent and non-transparent modes. In non-transparent mode SCB can be used as a HTTP proxy to simplify client configuration and integration into your network environment.

* *SCB supports remote Windows management performed by Windows PowerShell task automation framework (via HTTPS).*

Benefits for Your Company

- Ability to audit HTTP(S)-based administrative access to network devices, Windows and virtualization platforms
- Ability to control user sessions in custom web-applications
- Detect data leakage in e-banking or other front-end applications
- Faster troubleshooting and forensics in case of web-traffic-related incidents
- Independent, transparent, tamper-proof audit tool

About BalaBit

BalaBit IT Security is an innovative information security company, one of the global leaders in developing privileged activity monitoring, trusted logging and proxy-based gateway technologies to help customers be protected against insider and outsider threats and meet security and compliance regulations. BalaBit, the second fastest-growing IT Security company in the Central European region concerning Deloitte Technology Fast 50 list, has local offices in France, Germany, Italy, Russia, and in the USA, and cooperates with partners worldwide. Its R&D and global support centers are located in Hungary, Europe.

More information: www.balabit.com

Learn More

- Shell Control Box overview
- Request an online demo
- Request a callback