ARE YOU PROVIDING VPN access for your consultant?

Do you really know what they are doing and what has happened?

A virtual private network (VPN) is a network that uses primarily public telecommunication infrastructure, such as the Internet, to provide remote offices or travelling users access to a central organizational network.

VPNs typically require remote users of the network to be authenticated, and often secure data with encryption technologies to prevent disclosure of private information to unauthorized parties.

Nowadays VPN is widely used in many sectors for different reasons. Some use it to secure their end-user access to the corporate access others use it to give secure access to their outsource partners. Examples are widely available and create a growing demand for VPN-like services.

Control and monitor VPN access

While secure VPN solutions are a very good method to address different issues, it is very hard to control and monitor what is really happening inside the connection. When you provide VPN access to someone, you usually trust them. However, blind trust conceals the truth. When the VPN user can access critical systems or sensitive data, you definitely want to monitor and control their activities.

1

Example 1

A company uses secure VPN connection to grant access to their internal IT environment to an outsource IT partner. The outsource IT partner has access to all critical environments and the company can only hope that they will not do anything harmful.

2

Example 2

A company uses secure VPN connection to grant access to their internal application to some users. The users can access the application remotely anytime without further control. If the application cannot monitor user activity, no one would know what happens exactly during a connection.

3

Example 3

A company uses secure VPN connection to grant access to their IT environment to the internal IT team. System administrators can manage the whole IT environment without strict control and the company can only hope that they can trust their employees. In a forensics situation it is difficult to detect who did what and when on a server.

Shell Control Box can help your business

Shell Control Box (SCB) is an appliance that controls privileged access to remote systems and records the activities into searchable and replayable movie-like audit trails.

Benefits for you

Strengthen controls in IT outsourcing

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. Obviously, in such situations it is reassuring to have an independent device that can reliably log all administrative activities. SCB provides detailed information for troubleshooting and forensics situations to uncover the root of the problem.

Monitor your key users

SCB operates transparently and extracts information into audit trails directly from the communication of the client and the server, providing reliable, easy-to-access data and content. Now you have a tool to monitor who did what and when on a remote device.

Protect your corporate properties and secrets

Be sure of who accesses your network, when the event occurs and what actions the user performs. 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.

Managed file transfer

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, SCP, and SFTP.

Forensics

In case of any problems (server misconfiguration, database manipulation, and unexpected shutdown) the circumstances of the event are readily available in the audit trails, so the cause of the incident can be easily and quickly identified. The recorded audit trails can be played back 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 Enter) and texts displayed on the screen.