What is secure shell?

Secure Shell (SSH) is a robust protocol for connecting to servers remotely. In the realm of remote server access, security is going to be more and more important to keep your information safe. Secure Shell is primarily used for logging in to Linux servers, Unix servers, and certain networking equipment such as routers.

Alternatives to SSH

SSH provides a shield against prying eyes, but how does it compare to its alternatives?

Telnet is one popular alternative. Telnet exposes your typed commands, including passwords, to anyone on the network equipped with the right tools.

Although Transport Layer Security (TLS) encrypts data within web browsers, SSH secures data in interactive terminal sessions or file transfers. This encryption ensures that sensitive information remains confidential during communication.

Another alternative is virtual private networks (VPNs). VPNs also offer encryption but grant access to entire networks after connection. SSH adheres to the principle of least privilege, restricting users to specific hosts, enhancing security.

Another option might be remote-control software like VNC or GoToMyPC. They focus on graphical user interfaces and desktop experiences, which may not align with most Linux servers that operate sans desktop environments.

Operation

SSH operates through two key components: the SSH server and the SSH client. The SSH server, residing on the target server, establishes secure network connections, undergoes mutual authentication, and initiates encrypted login sessions or file transfers.

Conversely, the SSH client establishes a connection to the SSH server, ensuring a secure interaction. The client makes requests, such as “log me in” or “copy this file.”

SSH keys

In the SSH protocol, an access credential is known as an SSH key. It serves a similar purpose as usernames and passwords, although system administrators and power users typically use the keys to automate procedures and achieve single sign-on.

Displaying the fingerprint of an SSH key is a useful way to verify that you're using the correct key and that the remote server's key hasn't been tampered with. To display the fingerprint of an SSH key, you can use the **`ssh-keygen`** command-line tool.

Key takeaways

SSH prioritizes security in remote server access: Secure Shell (SSH) is a robust and trusted protocol for securely connecting to servers remotely. It finds widespread use in accessing Linux servers, Unix servers, and specific networking equipment, serving as a shield against unauthorized access and data breaches.

Comparing SSH with alternatives: When you compare SSH to alternatives like Telnet, its security superiority becomes clear. Telnet exposes commands, including passwords, to potential threats, whereas SSH's encryption guarantees confidentiality during interactive terminal sessions and file transfers. Unlike virtual private networks (VPNs) that offer network-wide access, SSH adheres to the principle of least privilege, ensuring users are restricted for enhanced security.

SSH's operational mechanics and key role: SSH functions through two core components: the SSH server and the SSH client. The SSH server establishes secure connections, authenticates parties involved, and initiates encrypted sessions. Conversely, the SSH client establishes secure interactions with the server and enables actions like secure login or file copying.

Just like a password, the security of your SSH key is critical. Never share your SSH private key with anyone or put SSH keys into your application code. With someone having access to your information, they can gain unauthorized access by logging in and pretending to be you.

Mark as completed

Like Dislike Report an issue