Learn about SSH

SSH protocol (also known as Secure Shell) is a method for secure remote login, from one computer to another computer.

SSH protocol (also known as Secure Shell) is a method for secure remote login, from one computer to another computer. It offers several alternative options for strong authentication, communication security protection and integrity with strong encryption features. It is a safe alternative to unprotected login protocols (such as telnet, rlogin) and unsafe file transfer methods (such as FTP).

Main content about SSH

1. What is SSH?
2. Typical uses of the SSH protocol
3. How does SSH protocol work?
4. Powerful authentication with SSH keys
5. SSH provides strong encryption and integrity protection features

What is SSH?

SSH, also known as Secure Socket Shell, is a network protocol that provides administrators with a secure way to access remote computers. SSH also refers to the suite of protocols that implement the protocol. Secure Shell provides strong authentication and communication security between two computers connected over unsecured networks such as the Internet. SSH is widely used by network administrators, to manage systems and remote applications, allow them to log on to another computer over the network, execute commands and move files from one computer to another. Other computer.

SSH can refer to both the encrypted network protocol and the utility suite that implements that protocol. SSH uses the client-server model, connects a secure client shell application, the end point at which the session is displayed, with an SSH server, the end point at which the session is active.

In addition to Microsoft Windows, SSH software is available by default on most operating systems. SSH also supports tunneling techniques, forwarding arbitrary TCP ports and connecting X11, while file transfers can be done using secure file transfer protocols or secure copy (SCP) protocols. link. By default, the SSH server listens on standard TCP port 22.

The SSH set includes three utilities: Slogin, ssh and scp. Those are safe versions of previous unsafe UNIX utilities like rlogin, rsh and rcp. SSH uses public key encryption to authenticate remote computers and allows remote computers to authenticate users, if needed.

The first SSH version appeared in 1995 and was designed by Tatu Ylönen, a researcher at Helsinki Technology University, who founded SSH Communications Security. Over time, various errors have appeared in SSH-1 and it has become obsolete. The Secure Shell protocol suite is now SSH-2 and is considered standard in 2006. It is incompatible with SSH-1 and uses Diffie-Hellman key exchange and stronger integrity checks (using verification code). real via message) to improve security. Client and SSH servers can use some encryption methods, mainly AES and Blowfish.

However, no exploit flaw was found in SSH2, although according to sources of information leaked by Edward Snowden in 2013, the National Security Agency could decrypt some SSH traffic.

Shellshock, a security hole in the Bash command processor, can be executed on SSH. In fact, the biggest threat to SSH is poor key management. If you don't selectively select, rotate, and remove SSH keys appropriately, organizations can lose control of who has access to which resources and when they can access them, especially when SSH is used in application-to-application processes (from applications to applications) automatically.

Typical uses of the SSH protocol

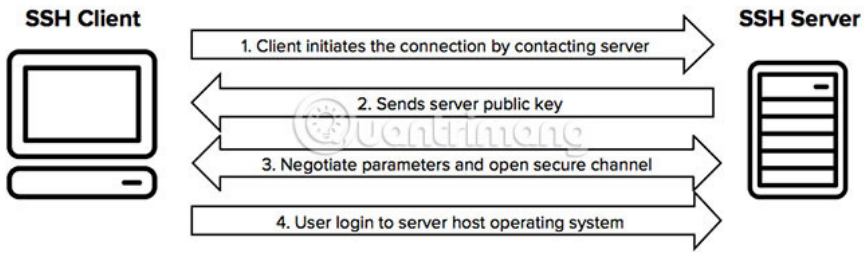
The protocol is used in corporate networks to:

1. Provides secure access to users and automated processes
2. Transfer interactive and automated files
3. Play remote commands
4. Network infrastructure management and system components keep other important tasks.

How does SSH protocol work?

The protocol works in the client-server model, which means that the connection is established by the SSH client connecting to the SSH server. SSH client controls the connection setup process and uses public key encryption to verify the identity of the SSH server. After the setup phase, the SSH protocol uses strong symmetric encryption algorithms and hash algorithms to ensure the privacy and integrity of the data exchanged between the client and the server.

The figure below shows a simple set of safe shell connections.



Powerful authentication with SSH keys

There are several options that can be used to authenticate users. The most popular options are passwords and public key authentication.

The public key authentication method is used primarily for automation and sometimes by system administrators to log in once. It has been used much more widely than the public has ever predicted. The idea is to have an encryption key pair - a public key and a private key - and configure the public key on the server to allow access and authorization to anyone who has a private key copy that can be accessed. server update. The keys used for authentication are called SSH keys. Public key authentication is also used with smart cards, such as CAC and PIV cards used by the US government.

The main use of authentication keys is to enable secure automation. Secure shell file transfer is used to seamlessly integrate applications and is also used for automated systems and configuration management.

As you can see, large organizations have more SSH keys than they imagine and managing SSH keys becomes very important. SSH keys grant access the same as granting access via user name and password. They require a similar start and end process.

In some cases, we will find several million SSH keys that allow access to production servers in the client environment, with 90% of the keys actually not being used and representing access rights already licensed but never terminated. Ensuring proper policies, processes and audits to use SSH are very important for proper identity and access management. Traditional identity management projects have skipped up to 90% of all login information, by skipping SSH keys. Services and tools for implementing SSH key management are also provided.

SSH provides strong encryption and integrity protection features

When the connection is established between the client and the SSH server, the transmitted data will be encrypted according to the parameters negotiated during the setup process. During the negotiation process, the client and server agree on the symmetric encryption algorithm to be used and create the encryption key to be used. Traffic between communication parties is protected by strong encryption algorithms according to industry standards, such as AES (Advanced Encryption Standard), and the SSH protocol also includes a mechanism to ensure integrity. integrity of the data is transmitted using standard hash algorithms, such as SHA -2 (Standard Hashing Algorithm).

See more:

1. Introducing OpenSSH
2. VPN and SSH: Which method is more secure?
3. Install SSH on the Router for secure web access anywhere