4 best tips for server protection

Today cybercriminals are more aggressive than ever. Let's set up server protection with the following basic steps to prevent attackers!

Server protection is one of the biggest concerns for security groups today. Weak protection could open the door for attackers to gain unauthorized access to the server through some kind of malware. Today cybercriminals are more aggressive than ever. Let's set up server protection with the following basic steps to prevent attackers!

SSH key: The must-have element for server protection

Also known as Secure Shell, the SSH keys are an encrypted network protocol. SSH keys provide a higher level of security than regular passwords.

This is because SSH keys are much better against a Brute Force attack. Why? Because it's almost impossible to decode. In contrast, a regular password can be cracked at any time.

When SSH keys are generated, there are two types of keys: the private key and the public key. The private key is saved by the administrator, while the public key can be shared with other users.

Unlike traditional passwords on servers, SSH keys have a long string of bits or characters. To crack them, the attacker will spend some time trying to decrypt the access by trying different combinations. This happens because the keys (public and private) must match to unlock the system.

Set up a firewall

Having a firewall is one of the basic measures to ensure server protection. A firewall is essential because it controls incoming and outgoing traffic based on a variety of security parameters.

These security parameters apply depending on the type of firewall you use. There are three types of firewalls based on their technology: Packet filtering firewall, proxy filter firewall, and state firewall. Each of these services provides a different way to access the server.

For example, a filtering firewall is one of the simplest mechanisms for securing a server. Basically, it checks IP address, port source, destination IP address, destination port, and protocol type: IP, TCP, UDP, ICMP. Then, compare this information with the specified access parameters, and if they match, access to the server is allowed.

A proxy filter is used as an intermediary between two parties to communicate. For example, a client computer requests access to a website. This client must create a session with the proxy server to authenticate and test the user's access to the Internet before creating a second session to access the website.

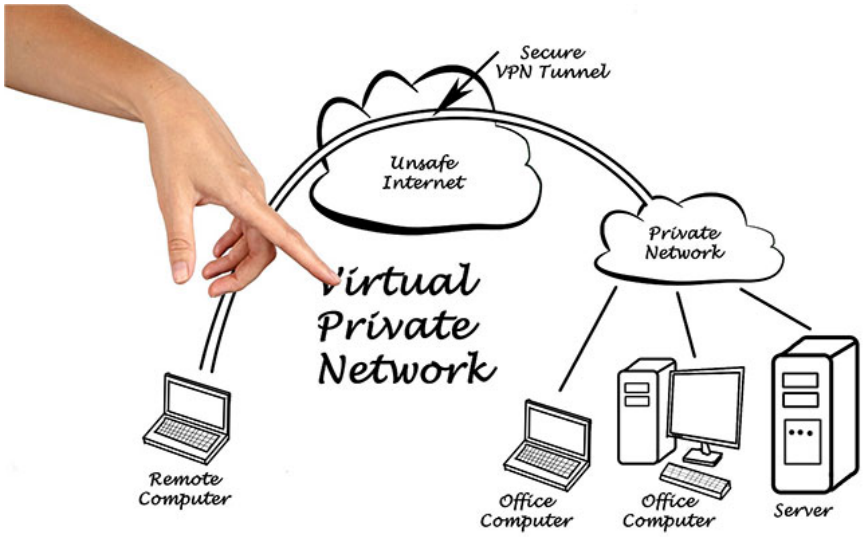
In terms of state firewalls, it combines the technology of proxy and packet filtering. In fact, it is the most used firewall for server protection, as it allows the application of security rules using UFC firewalls, nftables, and CSF firewalls.

In a nutshell, using a firewall as a server protection tool will help you protect content, validate access, and control traffic coming and going through pre-set security parameters.

VPN setup

Setting up a VPN (virtual private network) is essential to accessing the remote servers' information according to the security parameters of the private network. Basically, a VPN acts like a virtual cable between the computer and the server.

This virtual cable creates a tunnel for encrypted information to pass. In this way, the information exchanged between the server and the authorized computer is protected from any intrusion.



Server protection is underpinned by VPN, as it controls access to specific ports through the private network. This means that public access to the server is still blocked, and only users with access to the private network can exchange information with the server.

In short, VPNs provide security protocols to protect information passing through servers and create a secure connection through data encryption.

Encrypted using SSL and TLS

SSL and TSL encryption is an alternative if you don't want to use VPN tunnels. SSL (Secure Sockets Layer) is a digital certificate that protects the transmission of information.

On the other hand, TSL (Transport Layer Security) is the second generation after SSL. TLS establishes a secure environment between users and servers to exchange information. It does this using the protocols HTTP, POP3, IMAP, SMTP, NNTP, and SSH.

Using SSL and TSL through KPI (Public Key Infrastructure), you can create, manage, and validate certificates. You can also identify systems with specific users to encrypt communication.

In other words, when you set up an authorization certificate, you can track the identities of each user connected to your private network and encrypt their traffic to prevent communication from being compromised. Attack and strengthen your server protection.