What are IKE and IKEv2 VPN protocols?

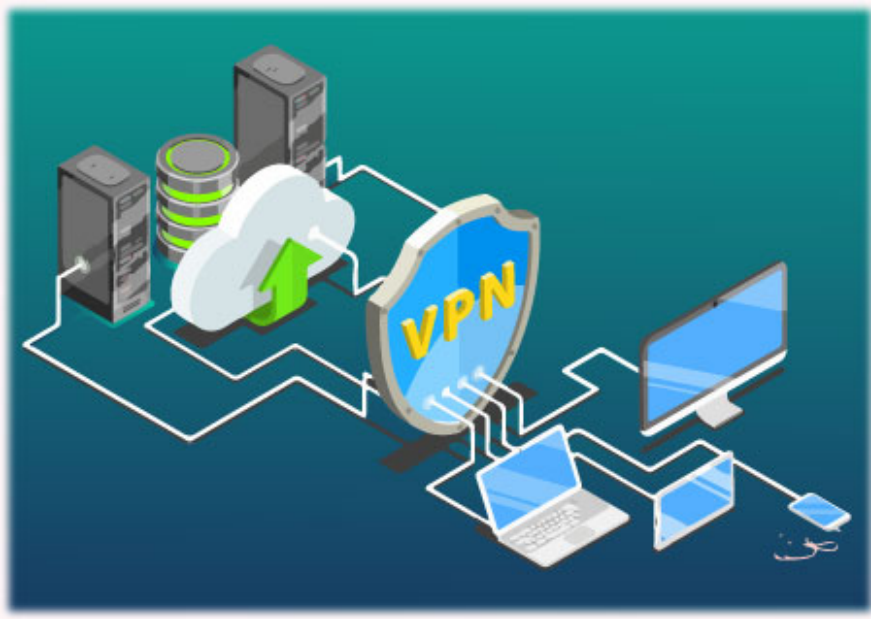
Internet Key Exchange, or IKE, is an IPSec-based tunneling protocol that provides a secure VPN communication channel and identifies means of automatic connection and authentication for secure IPSec links the way they are protected.

The first version of the protocol (IKEv1) was introduced in 1998 and the second version (IKEv2) was released seven years later. There are several differences between IKEv1 and IKEv2, of which IKEv2 reduces bandwidth requirements.

A detailed introduction to IKEv2

Why use IKEv2?

1. 256-bit data encryption
2. Implement IPSec for security
3. The connection is stable and consistent
4. MOBIKE support ensures better speeds



Security

IKEv2 uses server certificate authentication, which means it will not take any action until the identity of the requester is determined. This fails in most man-in-the-middle and DoS attack attempts.

Reliability

In the first version of the protocol, if you try to switch to a different Internet connection, for example from WiFi to mobile Internet, when the VPN is turned on, it will interrupt the VPN connection and will request to reconnect.

This has certain undesirable consequences like performance degradation and altered previous IP addresses. Thanks to the reliability related measures adopted in IKEv2, this problem has been overcome.

In addition, IKEv2 implements MOBIKE technology, allowing it to be used by mobile users and many others. IKEv2 is also one of the few protocols that support Blackberry devices.

Speed

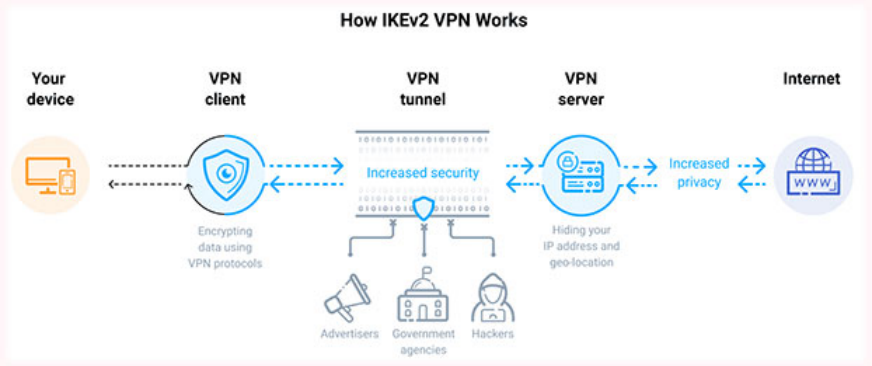
IKEv2's good architecture and efficient communication system deliver better performance. Also, its connection speed is significantly higher, especially due to the built-in NAT transport feature which makes it much faster to bypass the firewall and establish a connection.

Features and technical details

IKE's goal is to create the same symmetric key for all parties to communicate independently. This key is used to encrypt and decrypt common IP packets, used to transfer data between VPN peers.

IKE builds a VPN tunnel by authenticating both parties and reaching agreement on encryption methodology and integrity.

IKE relies on basic security protocols, such as the Internet Security Association and Key Management Protocol (ISAKMP), A Versatile Secure Key Exchange Mechanism for internet (SKEME), and the Oakley Key Determination Protocol.



ISAKMP specifies a framework for authentication and key exchange, but does not define them. SKEME describes a flexible key exchange technique that provides fast key refresh.

Oakley allows authenticated parties to exchange key documents over an insecure connection, using the Diffie – Hellman key exchange algorithm. This method provides a perfect secret forward method for keys, identity protection, and authentication.

The IKE protocol uses the UDP 500 port perfect for network applications where perceived latency is critical, such as games, voice and video communications. Furthermore, the protocol is linked with Point-to-Point (PPP) protocols.

This makes IKE faster than PPTP and L2TP. With the support of AES and Camellia ciphers with a key length of 256 bits, IKE is considered a very secure protocol.

Advantages and disadvantages of the IKEv2 protocol

Advantages

1. Faster than PPTP and L2TP
2. Supports advanced encryption methods
3. Stable when changing the network and re-establishing the VPN connection, when the connection is temporarily lost
4. Provides enhanced mobile support
5. Easy to set up

Defect

1. Using a UDP port 500 may be blocked by some firewalls
2. Not easy to apply on the server side