SearchSecurity.com

Internet Key Exchange (IKE)

By Andrew Zola

What is Internet Key Exchange (IKE)?

Internet Key Exchange (IKE) is a standard protocol used to set up a secure and authenticated communication channel between two parties via a virtual private network (VPN). The protocol ensures security for VPN negotiation, remote host and network access.

A critical role of IKE is negotiating security associations (SAs) for IP Security (IPsec). SAs are security policies defined for communication between two or more entities. A set of algorithms and mutually agreed-upon keys are used and represented by both parties when attempting to establish a VPN tunnel or connection.

There are two versions of IKE standards:

1. IKE protocol defined in RFC 2409
2. IKE version 2 (IKEv2) defined in RFC 7296

Most often, IKE uses X.509 public key infrastructure (PKI) certificates for authentication and a Diffie-Hellman key exchange protocol to establish a shared secret session.

A hybrid protocol, IKE, also implements two earlier security protocols, Oakley and SKEME, within an Internet Security Association and Key Management Protocol (ISAKMP) TCP/IP-based framework.

The SKEME protocol is an alternate version for the exchange key. ISAKMP RFC 2408 is used for negotiations, establishing security associations and securing connections between IPsec peers, specifying the framework for key exchange and authentication. Oakley RFC 2412 is used for key agreements or exchanges and defines the mechanism used over the IKE session for key exchange. Diffie-Hellman is the default algorithm used for exchange.

How does IKE work in IPsec?

IKE is a part of IPsec, a suite of protocols and algorithms used to secure sensitive data transmitted across a network. The Internet Engineering Task Force (IETF) developed IPsec to provide security through authentication and encryption of IP network packets and secure VPNs.

In IPsec, IKE defines an automatic means of negotiation and authentication for IPsec SAs. This is required for the encryption and decryption process because it negotiates security. IKE offers several benefits for IPsec configuration, including automatic negotiation and authentication, anti-replay services, certification authority support and the ability to change encryption keys during an IPsec session.

The IKE protocol uses User Datagram Protocol (UDP) packets to create an SA, generally needing four to six packets with two to three messages. An IPsec stack intercepts relevant IP packets, encrypting and decrypting them as needed.

Understanding phase 1 and phase 2 of IKE

The original version of IKE sets up secure communications channels in two phases: phase 1 and phase 2.

In phase 1, an authenticated connection between the host and user is established using a preshared key or a digital certificate. The goal is to secure the communications that occur in phase 2. The Diffie-Hellman key exchange algorithm creates a secure authentication communication channel. This digital encryption method uses numbers raised to specific powers to produce decryption keys. The negotiation should result in session keys and one bidirectional SA.

Phase 1 operates under one of two modes: main mode or aggressive mode. The main mode consists of both parties sending three two-way exchanges equaling six messages in total. The first two messages confirm encryption and authentication algorithms. The second set of two messages starts a Diffie-Hellman key exchange, where both parties provide a random number. The third set of messages verifies the identities of each party.

Aggressive mode accomplishes the same task as the main mode but does so in just two exchanges of three messages. Whereas the main mode protects both parties' identities by encrypting them, the aggressive mode does not.

Phase 2 of IKE negotiates an SA to secure the data that travels through IPsec, using the secure channel created in phase 1. The result is a minimum of two SAs that are unidirectional. Both parties also exchange proposals to determine which security parameter to use in the SA.

Phase 2 operates in only one mode: quick mode. Quick mode provides three resources: proxy IDs, perfect forward secrecy (PFS) and replay protection. The proxy IDs of each participant are shared with each other. PFS delivers keys independent from preceding keys. Replay protection is a security method to protect against replay attacks.

The main and aggressive modes found in phase 1 only apply to IKE version 1 and not to IKE version 2.

What is IKE version 2, and what are its improvements?

IKEv1 came out in 1998 and was followed by the released IKEv2 in 2005. IKEv2, updated in 2014, negotiates and authenticates IPsec SAs and provides secure VPN communication channels between devices. This version does not include phases 1 or 2 like its predecessor, but message exchanges still negotiate an IPsec tunnel. The first of the four messages is a negotiation to decide a security attribute. The second is where each party authenticates its identity. The third includes the creation of additional SAs. The fourth message removes SA relationships, detects IPsec tunnel liveliness and reports errors.

Improvements in IKEv2 over IKEv1 are as follows:

- requires less bandwidth;
- demands fewer cryptographic mechanisms to protect packets;
- requires only one four-message initial exchange mechanism;
- supports mobile platforms, including smartphones;
- supports the securing of Stream Control Transmission Protocol (SCTP) traffic;
- provides more resistance to denial-of-service (DoS) attacks;
- comes equipped with the built-in Network Address Translation (NAT) traversal needed to support routers that perform translations;
- detects automatically if an IPsec tunnel is still live so that IKE can automatically reestablish a connection if needed;

- enables message fragmentation and allows IKEv2 to operate in areas where IP fragments might be blocked and an SA may fail to establish; and
- enables rekeying to build new keys for SA.

What are the advantages of using IKE?

IKE includes the following benefits:

- automatic negotiation and authentication;
- anti-replay services;
- ability to change encryption keys during an IPsec session;
- calculating shared keys;
- fast connection speeds using NAT and NAT traversal;
- attempts to restore a connection whenever the connection drops;
- supports a variety of devices, including desktops and smartphones; and
- prevents DoS and replay attacks.

What are the potential challenges of using IKE?

IKE may pose the following challenges:

- IKEv1 is vulnerable to Bleichenbacher attacks, which obtain information about a device based on the device's response to receiving a modified ciphertext. IOS and Cisco Systems still support IKEv1.
- Using IKEv2 in some operating systems (OS) may require users to make additional manual configurations. For example, if IKE in Junos OS is not explicitly configured, Junos OS defaults to version 1 of IKE.

There is also a chance that a firewall or a network administrator could block IKEv2's UDP port, causing a VPN to stop working.

What is an L2TP IP VPN Internet Key Exchange?

Internet Service Providers (ISPs) use Layer Two Tunneling Protocol (L2TP) to enable VPN operations. By using IKE, this networking protocol negotiates and authenticates secure VPN connections.

Learn the difference between site-to-site and remote access VPNs and the benefits and use cases for each.

25 Feb 2022