

OpenVPN, IKEv2, SSTP

Index

- [LLTP vs PPTP vs SSTP](#)
- [SSTP vs OpenVpn](#)
 - [Advantages of OpenVPN over SSTP](#)
 - [Advantages of SSTP over OpenVPN](#)
 - [Conclusion of SSTP vs. OpenVPN: Which One Should You Use?](#)
- [IKEv2](#)
 - [Conclusion of IKEv2 vs. OpenVPN](#)
- [Migrating from SSTP to IKEv2 or OpenVPN](#)
 - [Option - 1](#)
 - [Option - 2](#)

4:05:12

- **OpenVPN® Protocol**, an SSL/TLS based VPN protocol. An SSL VPN solution can penetrate firewalls, since most firewalls open TCP port 443 outbound, which SSL uses. OpenVPN can be used to connect from Android, iOS (versions 11.0 and above), Windows, Linux and Mac devices (macOS versions 10.13 and above).
- **Secure Socket Tunneling Protocol (SSTP)**, a proprietary SSL-based VPN protocol. An SSL VPN solution can penetrate firewalls, since most firewalls open TCP port 443 outbound, which SSL uses. SSTP is only supported on Windows devices. Azure supports all versions of Windows that have SSTP (Windows 7 and later). **SSTP supports up to 128 concurrent connections only regardless of the gateway SKU.**
- **IKEv2 VPN**, a standards-based IPsec VPN solution. IKEv2 VPN can be used to connect from Mac devices (macOS versions 10.11 and above).



IKEv2 and OpenVPN for P2S are available for the [Resource Manager deployment model](#) only. They are not available for the classic deployment model. The Basic gateway SKU does not support IKEv2 or OpenVPN protocols. If you are using the Basic SKU, you will have to delete and recreate a production SKU virtual network gateway.

LLTP vs PPTP vs SSTP




#LLTP

#PPTP

#SSTP

05-01-2024

3:13:16

| | PPTP | L2TP | SSTP |
|----------|--|--|---|
| PLATFORM |  iOS |  iOS |  |
| SECURITY | Basic encryption | IPSec Encryption | SSL 3.0 Encryption |
| FIREWALL | TCP port 1723 easy to block | UDP Port 500 easy to block | Use 443 port hard to block |
| RESULT | Old and outdated Don't use | Better than PPTP | Good but mostly Windows |

[source]([SSTP - What is SSTP VPN? \(youtube.com\)](#))

SSTP provides better security comparative to PPTP L2TP.

#SSTP vs #OpenVpn

The main difference between SSTP and OpenVPN is that

- **#SSTP** is less secure than **#OpenVPN**. This is because SSTP uses the deprecated SSL 3.0 protocol which is vulnerable to the POODLE bug.
- On the other hand, OpenVPN uses the TLS protocol which is generally more secure and is not affected by POODLE.
- Another difference between SSTP and OpenVPN is that SSTP primarily works on Windows and might be hard to configure on other operating systems,
- Whereas OpenVPN works on every platform. Read on to learn more about the differences between SSTP vs. OpenVPN.

02-01-2024 12:38:41

| #SSTP | #OpenVPN |
|--|---|
| Short for Secure Socket Tunneling Protocol. | Sometimes shortened to OVPN; VPN stands for Virtual Private Network. |
| Microsoft's proprietary encryption standard | Open source |
| SSTP does not require you to install third-party software. | OpenVPN depends on third-party software. |
| SSTP uses TCP. | OpenVPN can use UDP or TCP. |
| Limited configuration capabilities. | Highly configurable and customizable. |
| SSTP uses AES-256 encryption. | OpenVPN can use strong SSL encryption such as Blowfish-128 AES-256 encryption. |
| Uses deprecated SSL 3.0, which is a big security concern (vulnerable to POODLE attacks). | Uses TLS which is not impacted by most variants of POODLE cyberattacks. |
| SSTP fully integrates with Windows. While SSTP also supports Linux and macOS, it may be very hard to configure SSTP on a non-Windows device. | OpenVPN is available on Windows XP and later as well as Solaris, macOS, Linux, iOS, Android, and many other desktop and mobile operating systems. |
| Easy to set up. | Might be difficult to configure. |

[source](#)

Advantages of OpenVPN over SSTP

- OpenVPN uses TLS instead of SSL, which makes it not susceptible to POODLE attacks.
- OpenVPN can run over UDP, which makes it faster.

- OpenVPN is highly customizable, which allows more flexibility and the use of very secure encryption algorithms such as AES-256.
- OpenVPN is open source, which means it is regularly inspected, maintained, and updated by its community of supporters.
- OpenVPN works on every platform, whereas SSTP may have compatibility issues with non-Windows devices.

Advantages of SSTP over OpenVPN

- SSTP is more stable and easier to set up on Windows devices, as it is a proprietary protocol developed by Microsoft.
- SSTP uses TCP port 443 by default, which is the same port used by HTTPS traffic. This makes it harder to detect and block by firewalls and censorship tools.

Conclusion of SSTP vs. OpenVPN: Which One Should You Use?

SSTP is a fast and stable VPN protocol that works well on Windows devices, but it has some security drawbacks due to its use of SSL 3.0. In contrast, OpenVPN is a more secure and versatile VPN protocol that works on every platform and offers more configuration options. Use OpenVPN if you can.

#IKEv2

[source]([IKEv2 vs. OpenVPN: What's the Difference? - Rublon](#))

Conclusion of IKEv2 vs OpenVPN

IKEv2 and OpenVPN are two secure protocols used to establish and authenticate communication between a VPN client and a VPN server. Generally, IKEv2 is faster than OpenVPN. Further, IKEv2 has the ability to re-establish a connection after a loss of signal and handle changes in the network very well thanks to the MOBIKE protocol. On the other hand, OpenVPN can use both UDP and TCP as transport layer protocols. It is open-source, secure, reliable, and cost-efficient.

Summing up, if you need a secure and versatile protocol, OpenVPN is a good choice. However, if you care about speed or want to use a mobile VPN client, go for IKEv2.

Migrating from SSTP to IKEv2 or OpenVPN

- cases when you want to support more than 128 concurrent P2S connection to a VPN gateway but are using SSTP.

Option - 1

- Add IKEv2 in addition to SSTP on the gateway
- both can co-exist on the same gateway and give you a higher number of concurrent connections.
- simply enable IKEv2 on the existing gateway and redownload the client.
- Adding IKEv2 to an existing SSTP VPN gateway won't affect existing clients. [source](#)
- ! If a Windows client is configured for both SSTP and IKEv2, it tries to connect using IKEV2 first and if that fails, it falls back to SSTP.

3:43:34

Option - 2

- Remove SSTP and enable OpenVPN on the Gateway
- Since SSTP and OpenVPN are both TLS-based protocol, they can't coexist on the same gateway.
- You'll have to disable SSTP and enable OpenVPN on the gateway.
- This operation causes the existing clients to lose connectivity to the VPN gateway until the new profile has been configured on the client.
- Once the gateway has been configured, existing clients won't be able to connect until you [deploy and configure the OpenVPN clients](#).

Tuesday, 16-01-2024, 12:55 pm

breakdown of supported protocols for each VPN type in Azure:

Point-to-Site (P2S):

- OpenVPN (SSL)

- IKEv2
- Secure Socket Tunneling Protocol (SSTP)

Site-to-Site (S2S):

- IPsec IKEv2
 - IPsec IKEv1
-