SpeedFusion Bandwidth Bonding and Security

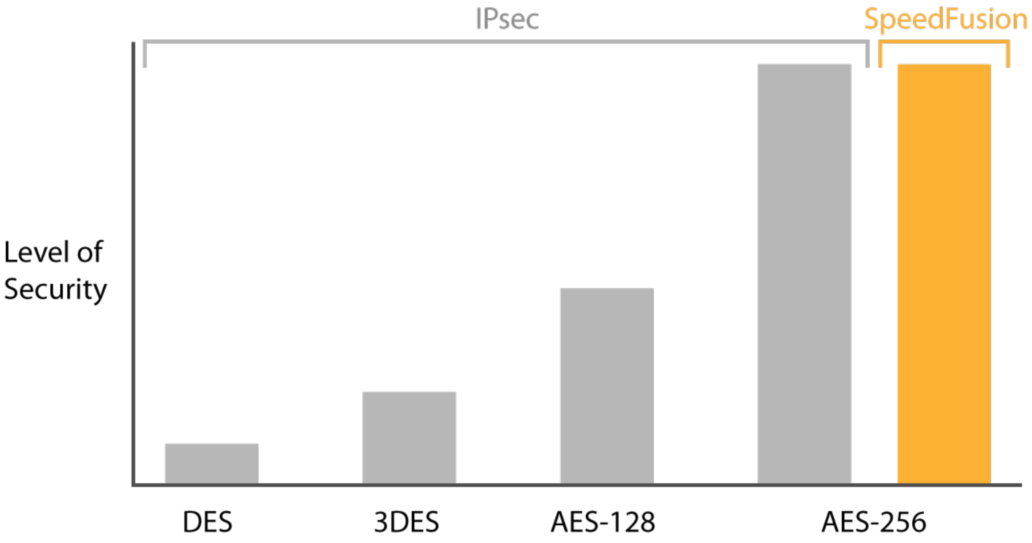
Thousands of organizations use SpeedFusion bandwidth bonding to affordably achieve greater throughput, resilience and reliability for encrypted site-to-site connectivity.

The ability to combine bandwidth from multiple WAN connections has opened a wide range of deployment possibilities such as vehicular video streaming, media broadcast, field surveillance systems or temporary site connectivity and is seemingly supplementing private leased lines such as MPLS and VSAT.

Many business applications need more than additional bandwidth. The transfer of sensitive customer, sales and operational data demands the highest data security available.

SpeedFusion is capable of achieving levels of security, that surpass the most stringent requirements. In this white paper, we are going to discuss SpeedFusion from a security perspective and its advantages compared with IPsec (Internet Protocol Security) standards.

1. SpeedFusion provides the Highest Security Level by default



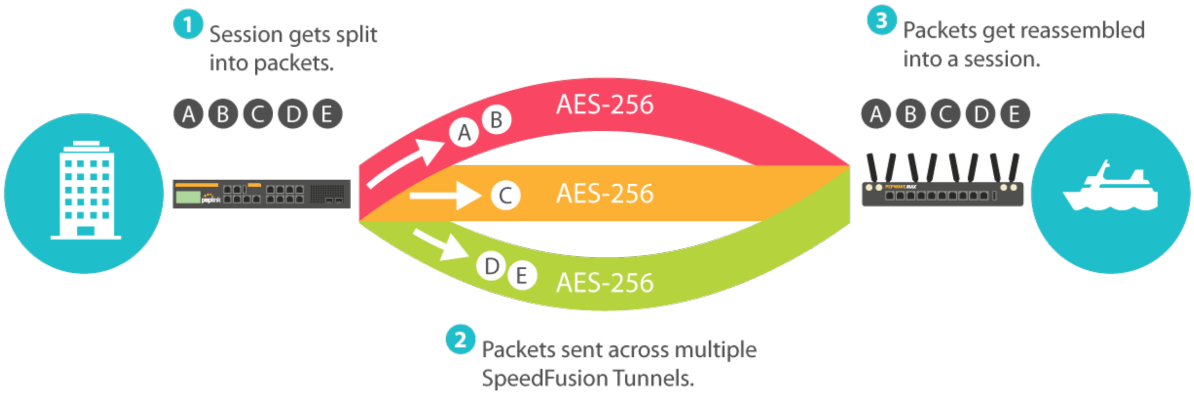
IPsec has evolved over a long period of time. Therefore it has to support older encryption standards such as DES, 3DES, and AES-128. However, older standards and particularly DES are outdated and easily compromised.

This leaves networks using older IPsec security standards susceptible to attacks. Peplink's SpeedFusion packet level VPN bonding is purely based on AES-256 encryption, the same encryption standard approved and used by the U.S. Military. Its considered the only secure way for mission critical data communication.

2. Additional Layer of Protection makes Eavesdropping Virtually Impossible

On top of AES-256 encryption, SpeedFusion is based on patented, packet level bandwidth bonding technology across multiple physical WAN interfaces.

This technology separates a session into individual sub-packets and sends these partial data across different WAN connections. Once these sub-packets are received at the destination (once again via multiple WAN connections) they are reassembled into the original data stream. Network devices on both sides see the full session independent of WANs in use.


1 Session gets split into packets.
A B C D E
A B
AES-256
C
AES-256
D E
AES-256
3 Packets get reassembled into a session.
A B C D E
2 Packets sent across multiple SpeedFusion Tunnels.

SpeedFusion creates an additional layer of security by routing sub-packets of traffic across multiple physical media types across different telecommunication providers.

If a potential intruder were to compromise a single sub-VPN tunnel, the data captured would still be unusable since it only contains a small (useless) portion of the data transmission. Up to 13 WAN connections can be used on each side via SpeedFusion bonding and encryption.

This additional layer of physical security makes eavesdropping virtually impossible. Each additional WAN interface used in a deployment multiplies the security level compared with single channel IPSec. Multiple encrypted tunnels make SpeedFusion a much better choice than IPSec or any other single-tunnel based VPN technology.

3. FIPS 140-2 Certification - Guaranteed Military-Grade Security

Security cannot be trusted without independent validation and approval. FIPS 140-2 is a validation program for certifying cryptographic products for use in government agencies jointly developed by the U.S. and Canadian governments. It is a highly rigorous process that can take years to complete.

Peplink has started the independent validation process more than 24 months ago and has passed all FIPS 140-2 compliance levels. Peplink is determined to provide its customers the ultimate approval on security and is expecting to receive the official FIPS 140-2 Accreditation Certificate in Q1 2017.