Solution Brief

CypherPlug – IP Traffic Encryption in a Smart SFP

Challenge: The rise in cyber threats and resulting increased regulation for protecting digital assets and communications have made encryption a mandatory element in almost every network. The challenge arises when considering brownfield deployments and existing network elements – how are they to be protected? By adding routers with IPsec VPN capabilities is a complex and costly process.

Solution: Instead of replacing equipment, network operators can immediately provide robust encryption protection with the CypherPlug®. This add-on is a miniature network security device that encrypts traffic over any layer 2 or layer 3 packet network. Departments who share the same network can each configure different encryption keys on the CypherPlug to maintain secure and unique communications.

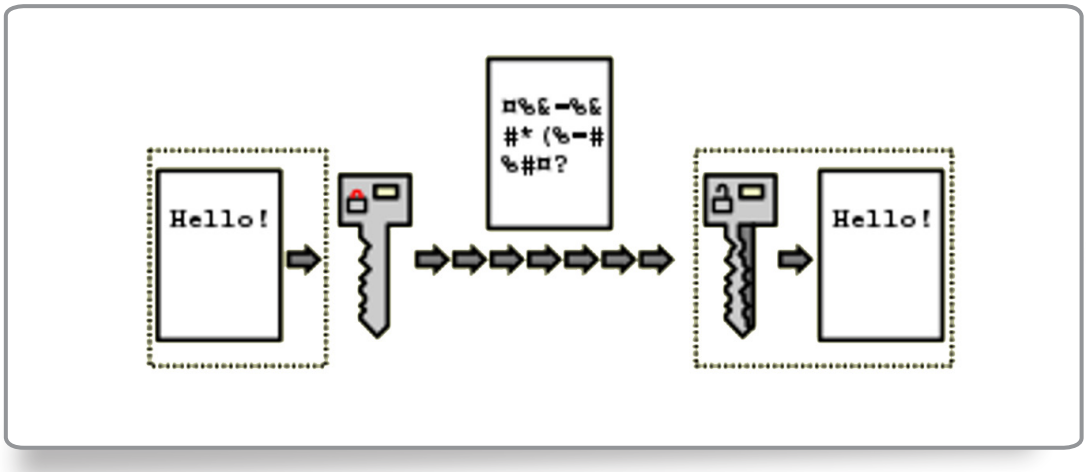
RAD

Your Network's Edge®

Solution Brief
CypherPlug – IP Traffic Encryption in a Smart SFP

How is Encryption Performed?

At its most basic level, encryption is the process of protecting information or data by using mathematical models to scramble it that only the parties who have the key can access it. That process can range from simple to very complex. Mathematicians and computer scientists have invented specific forms of encryption that are used to protect information and data that consumers and businesses rely on every day.



Encryption works by encoding "plaintext" into "ciphertext," typically using cryptographic mathematical models known as algorithms. To decode the data back to plaintext it requires the use of a decryption key. This is a string of numbers, or a password created by an algorithm. Secure encryption methods employ numerous cryptographic keys, making it nearly impossible for an unauthorized person to guess the correct one or use a computer to determine it through a brute-force attack. This involves trying every possible combination.

Encryption performs four important functions:

1. Confidentiality: Keeps the contents of the data secret
2. Integrity: Verifies the origin of the message or data
3. Authentication: Validates that the content of the message or data has not been altered since it was sent
4. Nonrepudiation: Prevents the sender of the data or message from denying they were the origin

The two most common types of encryption algorithms are *symmetric* and *asymmetric*.

Symmetric encryption, also known as a shared key or private key algorithm, uses the same key for encryption and decryption. Symmetric key ciphers are considered less expensive to produce and do not require as much computing power to encrypt and decrypt, resulting in a shorter delay in decoding the data. The drawback is that if an unauthorized person gets their hands on the key, they will be able to decrypt any messages and data sent between the parties. As such, the transfer of the shared key needs to be encrypted with a different cryptographic key, leading to a cycle of dependency.

Asymmetric encryption, also known as public-key cryptography, uses two separate keys to encrypt and decrypt data. One is a public key shared among all parties for encryption. Anyone with the public key can then send an encrypted message, but only the holders of the second, private key can decrypt the message. Asymmetric encryption is considered more expensive to produce and takes more computing power to decrypt as the public encryption key is often large, between 1,024 and 2,048 bits. As such, asymmetric encryption is often not suited for large packets of data.

Common Encryption Algorithms: Advanced Encryption Standard (AES): AES was adopted by the US government in 2001 and is the most used encryption method today. It was designed on a principle called a "substitution-permutation network" that is a block cipher of 128 bits and can have keys at 128, 192, or 256 bits in length.

Twofish: Used in both hardware and software, Twofish is considered the fastest symmetric encryption method. While Twofish is free to use, it's not patented nor open source. Nevertheless, it's used in popular encryption applications like PGP (Pretty Good Privacy). It can have key sizes up to 256 bits.

The most common methods of asymmetric encryption include:

RSA: Stands for Rivest-Shamir-Adelman, the trio of researchers from MIT who first described the method in 1977. RSA is one of the original forms of asymmetric encryption. The public key is created by the factoring of two prime numbers, plus an auxiliary value. Anyone can use the RSA public key to encrypt data, but only a person who knows the prime numbers can decrypt the data. RSA keys can be very large (2,048 or 4,096 bits are typical sizes) and are thus considered expensive and slow. RSA keys are often used to encrypt the shared keys of symmetric encryption.

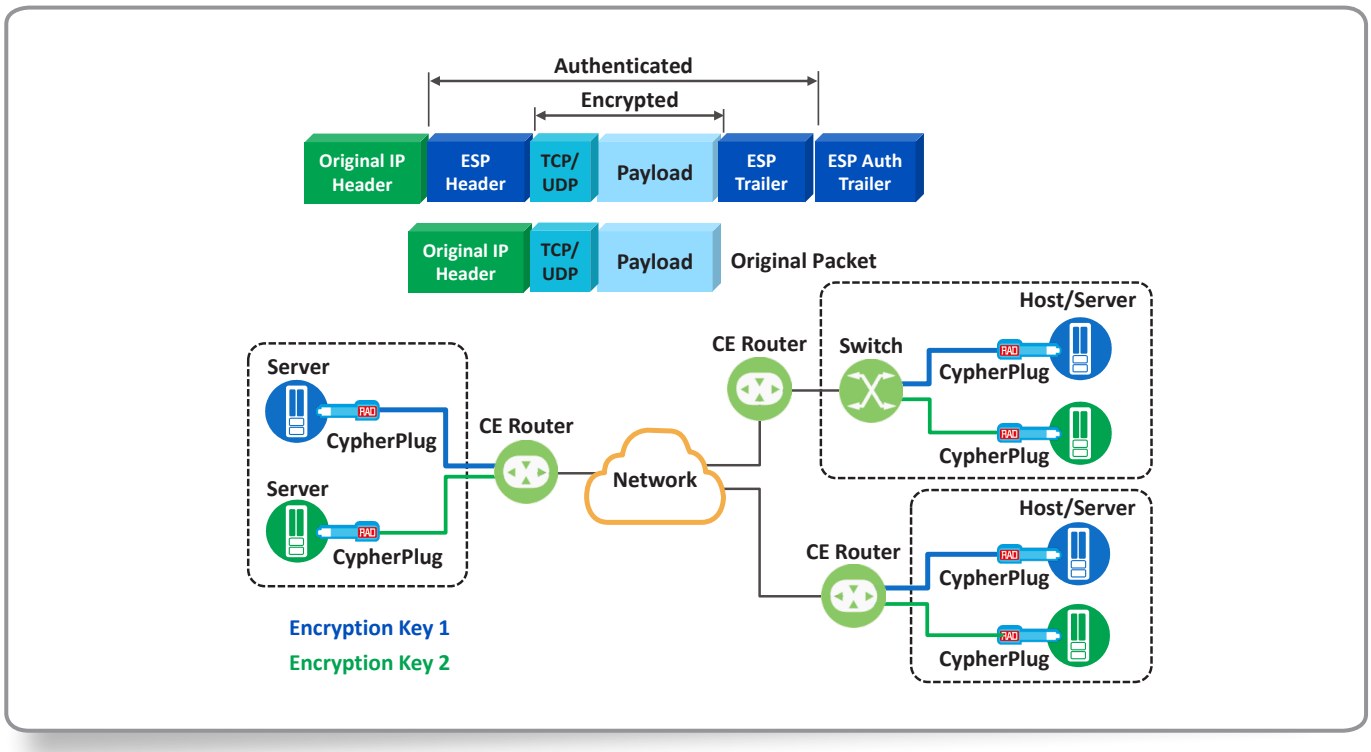
Solution Brief

CypherPlug – IP Traffic Encryption in a Smart SFP

Elliptic Curve Cryptography (ECC): An advanced form of asymmetric encryption based on elliptic curves over finite fields. The method provides the robust security of massive encryption keys, but with a smaller and more efficient footprint. For instance, a "256-bit elliptic curve public key should provide comparable security to a 3,072-bit RSA public key." Often used for digital signatures and to encrypt shared keys in symmetric encryption.

Once IP connectivity is provided to an enterprise/organization, there is a need to isolate via encryption groups (e.g. departments) within this organization that are connected over a shared IP transport. The common way to achieve this is by adding to the CE router IPsec tunnels, extra virtual routing and forwarding (VRFs), etc. Alternatively, each department can be build its own overlay encrypted solution, whether by owning their own router/SD-WAN solution or via application encryption.

Encryption with CypherPlug®



Solution Brief

CypherPlug – IP Traffic Encryption in a Smart SFP

CypherPlug is a smart SFP sleeve for payload encryption, layer 1, layer 2, and layer 3 headers are kept with the original value. Any standard MSA compatible 100 Mbps or 1 GbE SFP can host Cypherplug and enables full reuse of customer equipment and seamless deployment over network infrastructure types. Therefore, by providing end-to-end static transport mode IPsec encryption (see diagram above), the CypherPlug provides security for various organizations. It also addresses the data privacy requirements of government, military, healthcare, and finance organizations. In addition, it is used as part of asset protection by utilities.

- The SFP sleeve is easily pluggable into standard MSA compatible SFP ports of switches and routers. This eliminates the use of external power and reducing space, cabling and other installation costs compared to other solutions.
- The main benefit of the CypherPlug is that it is built based on FPGA (hardware-based packet processing engine) which supports 1G wire-speed encryption. Furthermore, it enables easy customization to additional or different customer requirements. Due to the encryption being performed in hardware the encryption latency is a few tens of microseconds depending on the packet length.
- Moreover, static key management allows for the complete separation of the control and data planes, ensuring that they are isolated from each other.
- Due to complete separation of the control pad and the data planes, CypherPlug the keys secret without exposing them to field technicians.
- Providing Plug & Play, point-to-point and point to multipoint IPsec, CypherPlug provides significant benefits over router IPsec, namely that no VPN reconfiguration is required.

To learn how CypherPlug can help secure your network, contact us at: market@rad.com.

Your Network's Edge®