PROTELION
GOVERNMENT SOLUTIONS

PROTELION SECURITY ARCHITECTURE

PROTELION TECHNOLOGY FOR THE FUTURE

Today's world is based on IP-VPN technology and will accelerate in this direction. Protelion Security Technology has been designed and developed by our engineers for the future. Our technology is also constantly evolving, guaranteeing customers the usability of the systems for the years to come. It is important for customers to use future-oriented technology in order to protect their investments and to have the possibility of continuous adaptation.

PROTELION VPN TECHNOLOGY

Protelion has developed its own VPN Technology that is one of the best and most advanced systems the market knows today. Its implemented security features meet the highest standards and comply easily with the government and military requirements for top secrete communication. The Protelion unmatched VPN Technology has been tested and verified by numerous customers and implementation scenarios throughout the world and has been proven secure, highly robust and utmost resilient against many kinds of cyber-attacks. Even sophisticated malware like Pegasus or Predator cannot install itself on our especially hardened communication devices.

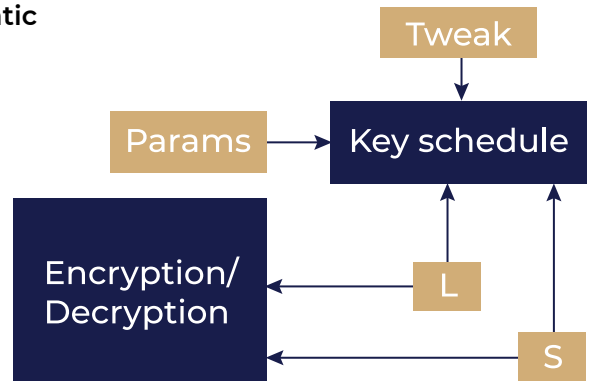
SECURITY MANAGEMENT CENTER

Protelion VPN Technology, with its inherent idea and policy of managing and handling every single security parameter and encryption keys in a Security Management Center (SMC), which is mandatorily under full control of the customer, gives back the sovereignty and integrity of all data and information to the customer. In general it can be said - if you don't have the keys, it's not your data.

ENCRYPTION

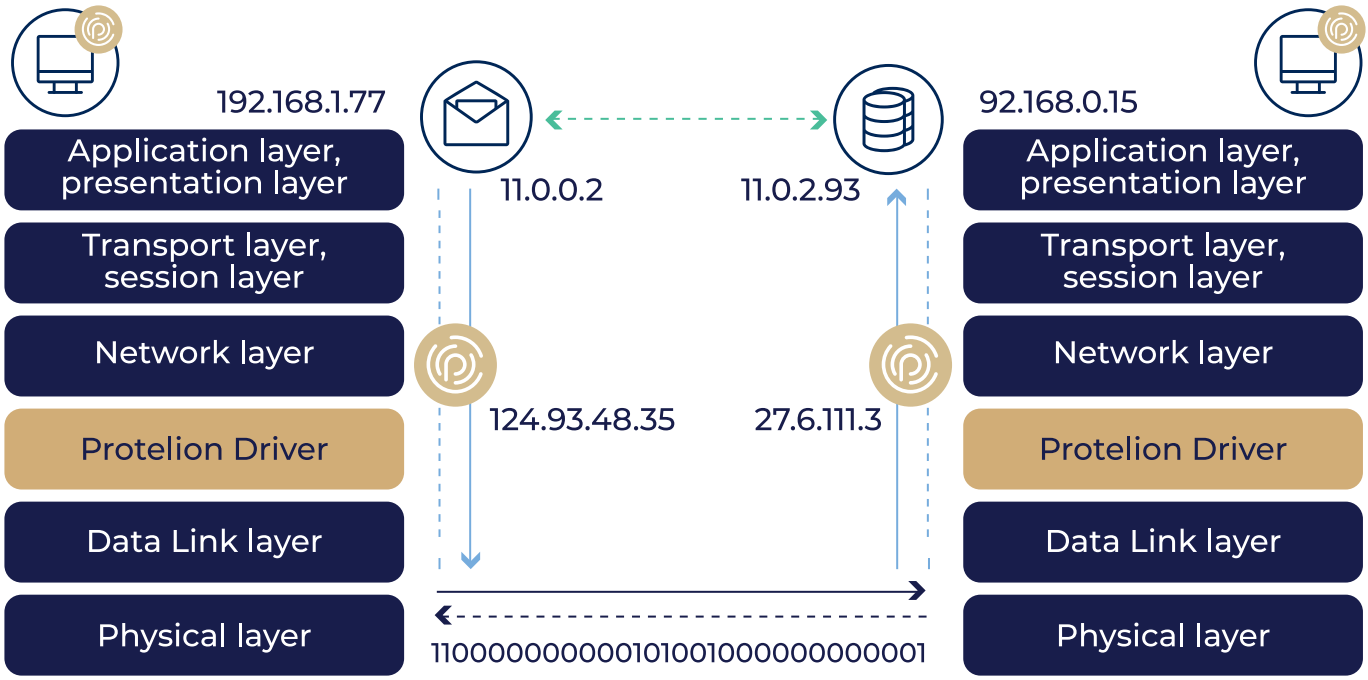
The Protelion VPN Technology security is based on our own implementation of the well-known and security proofed AES-256 with its unique security key generation and distribution. Our AES-256 is certified by NIST and complies with modern military grade required encryption security. The Protelion Technology offers more over a highly advanced customizable and proprietary CROC algorithm that outmatches standard AES-256 ciphers and is under control of the customer. The customizable CROC Block Cipher comes in three different designs, as CROC-D (default version), CROC-T (Tweakable by the customer) and CROC-C which includes a completely new design of the Block cipher's S-Boxes and L-Registers. This is an amazing additional security value and furthermore a precious independence issue of the manufacturer, hardly any solution on the market can provide and definitely not at comparable prices to ours.

CROC Block Cipher Schematic



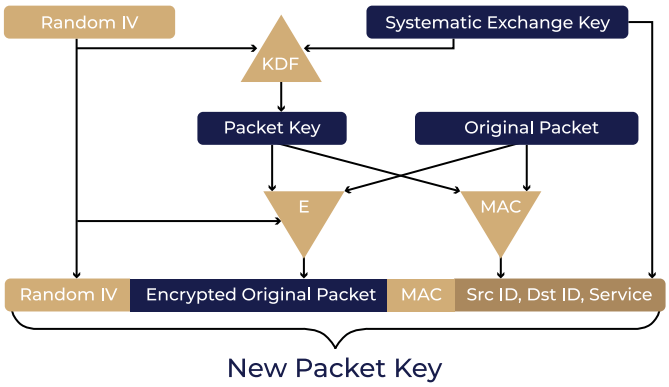
OSI IP LAYER3

Protelion VPN Technology Encryption works on the OSI IP Layer3 and therefore guaranties the support of any IP feature and any channel or transportation medium that works with the IP Protocol.



IP TRAFFIC ENCAPSULATION

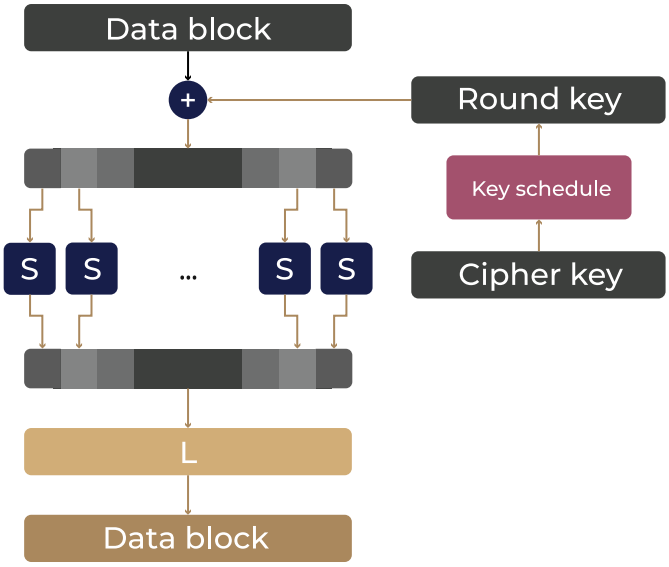
The Protelion VPN Technology uses tunnel respectively encapsulation technology and provides therefore by its AES-256 or CROC based encryption perfection in data integrity protection and resistance against man in the middle attacks. It also allows for traffic verification/ filtering and identification of user and IP packet sources for more security in the communication protocol and provides unmatched security and protection.



ALGORITHM

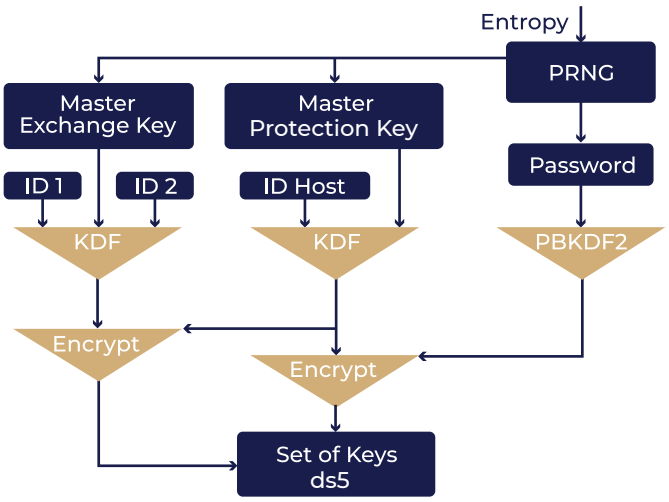
The high security of our AES-256 and proprietary CROC algorithms arises from proper expertise and design, of permutating nonlinear S-parameter transformation boxes and scrambling L-parameter transformation registers, by our world class crypto engineers. A further pillar of the security architecture of our algorithm is the Key scheduler block that is driven by a Random Number Generator based on nonlinear functions that guarantee a non-periodic initial key value for the encryption key generation. This issue is an indispensable condition for a highly secure algorithm implementation.

General Algorithm Structure



ENCRYPTION KEY GENERATION AND DISTRIBUTION MANAGEMENT

The “Encryption Key Generation and Distribution Management” plays an enormously important role in terms of security. Protelion has devoted a great deal of attention to this aspect to guarantee the highest level of security for its customers. Due to the fully symmetric protocol for encryption key generation, distribution and payload encryption using AES-256 or CROC algorithms no session key exchange is necessary and therefore our solutions are first, faster and more reliable than other mechanisms and second, they provide resilience to cryptanalytically relevant quantum computer in the future.



VERIFICATION TOOL

In addition to the AES-256 and the CROC customized algorithm, it is indispensable to provide the customer a tool to verify the implementation of the different ciphers in a particular Protelion product. With that tool, the customer can perform a step-by-step check of the implemented cipher, used tweaks, keys, communication protocol, and more. The verification tool must be independent of the developer and available in source codes to allow the customer to examine, control, and monitor the behavior of the operating units without any interference from the manufacturer.

PHYSICAL SECURITY AND INTEGRITY

All Protelion Armored AR devices are delivered in highly robust and secured casing, meaning they count with temper proof housing, alerts and emergency features as clearing and erasing all sensible data when experienced an unauthorized breach.

UPDATES AND MAINTENANCE

Protelion only distributes certified and verified updates and/or security patches by means of protected downloads from identified servers and only when accessed by the customer with corresponding secure credentials.
Once the corresponding updates and/or actualization files are in the customer's SMC, they will be automatically distributed to the connected devices and infrastructure, via encrypted and protected channels.

TRAININGS

Advanced and regular product training is available in which participants will get to know the Protelion Security Technology Products better and learn how to administrate them properly and include them seamlessly in their own networks. For mastering and customization options and selecting your transformations and parameters for a customized CROC algorithm. Protelion provides special customization workshops. It is an intensive training during which customer experts will be given all required theory and practical exercises to make fault-free customization and be able to run and support a VPN network based on their CROC cipher.

G.PSA.24_v01_BrEng

PROTELION
GOVERNMENT SOLUTIONS

Oberwallstr. 24
D-10117 Berlin,
Germany

+49 30 206 43 66-50

gov@protelion.com

gov.protelion.com

©Protelion GmbH