IDQ

Redefining Security

SWISS QUANTUM

QUANTUM-SAFE SECURITY WHITE PAPER

State-of-the-art Network Encryption

Architecture & best practices

Version 2.0
August 2017

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com

Table of contents

ID Quantique SA

Ch. de la Marbrerie, 3

1227 Carouge

Switzerland

Tel: +41 (0)22 301 83 71

Fax: +41 (0)22 301 83 79

www.idquantique.com

info@idquantique.com

Information in this document is subject to change without notice.

1. Securing Untrusted Layer 2 Networks

Metropolitan and Wide Area Networks interconnect companies' data centers and different sites. Metro and Carrier Ethernet provide the foundation for this interconnection. The setup is simple and fast and the cost/performance ratio of Metropolitan Area Networks (MAN) or Wide Area Network (WAN) shows a noticeable improvement. The problem faced by enterprises is that, while they may be able to trust their own internal networks and data centers, they cannot trust the interconnections provided by the MAN or WAN. To make things worse, there is no built-in security standard for Ethernet and MPLS. While Ethernet encryption at layer 2 – the data link layer – will protect all Ethernet and MPLS payload in a fast, efficient and secure way, there is no interoperability between the different layer 2 encryption solutions on the market. Therefore selecting the right approach to layer 2 encryption is essential, and saves money and headaches.

2. The Different Processing Approaches to Implementing Network Encryption

There is more than one approach to the implementation and deployment of layer 2 encryptors. Network encryption requires network access, which can either be provided by a dedicated appliance or by a host system. The more powerful the processing capabilities available to the encryption process, the faster the encryption. While network encryption can run on any CPU (Central Processing Unit), hardware acceleration will boost the encryption performance tremendously. Direct hardware support can be implemented in a CPU, an ASIC (Application Specific Integrated Circuit) or on a FPGA (Field-Programmable Gate Array). Of those three, only FPGAs can be updated to provide hardware acceleration for new functionalities.

2.1. CPU – The most versatile, but the slowest solution

Network encryption can be run on any CPU, but for sustained bandwidths above 50Mb/sec hardware acceleration is necessary to counteract increased latency and jitter. A few of Intel's current high-end CPUs come with hardwired instruction sets for AES encryption. However, the AES encryption itself is only one of the functions which utilise the hardware acceleration, so that even high-end CPUs with AES hardware support start to stutter at 1Gb/sec in bandwidth and above.

2.2. ASIC – A fast, but non-upgradable and non-extensible solution

Application Specific Integrated Circuits (ASIC) are integrated circuits that combine a collection of functions and are customized for a particular use, such as Cisco's ASIC on a card for MACSEC implementations. These processors are not intended for general-purpose use. For network encryption an ASIC in the form of a security processor can offer hardware acceleration for certain functions. As the functions are delivered in silicon, they cannot subsequently be extended or upgraded by the user. An ASIC-based solution cannot keep up with evolving security threats and security standards, and therefore has a very limited lifespan.

2.3. FPGA – The fast and upgradable solution

Field-Programmable Gate Arrays (FPGA) combine the hardware acceleration of a customized chip with the added benefit of upgradeability. They are optimized for speed, functionality and extensibility with the lowest total cost

of ownership of all the options. Although FPGAs are slightly more costly to manufacture and the costs increase with the number of gates that the FPGA supports, this is mitigated by the reduced operational costs over the lifetime of the unit (TCO). One issue with the use of FPGAs is the management of the heat produced. The heat increases with the utilization rate of the available gates, favoring the use of slightly over-dimensioned FPGAs to reduce that heat. Ample reserves of available gates are also needed to support extensions of the product functionality. Most leading layer 2 encryption vendors, including ID Quantique, favour FPGAs over other deployment methods.

3. Choosing the Right Form of Deployment

Due to the lack of vendor compatibility in network encryption, an enterprise needs to find a vendor who offers a complete range of products able to cover all their layer 2 network encryption needs. It is also essential to remember that only a dedicated appliance will work with other network equipment from different vendors, such as switches or any active network elements. Here are the different options:

3.1. Dedicated Appliance

Most leading layer 2 encryptors, including those of ID Quantique, come as independent and dedicated appliances that are placed between the trusted internal network and the untrusted external network. They create a clear physical and logical separation between the internal and the external network. Only dedicated appliances work independently of any other network device and are entirely built for purpose. High-end appliances come with hardware acceleration based on FPGAs and are currently capable of encrypting up to 100Gb/sec sustained full-duplex network traffic even in complex multipoint networks.

Advantages	Disadvantages
Bump-in-the-wire technology, integrating seamlessly into existing network	Needs rack space as dedicated hardware appliance
Compatible with existing network equipment for lower operational costs	Slightly higher initial costs than an integrated appliance
Supports multi-vendor network environments to reduce customer lock-in	
Integrates all required functionalities in a dedicated secure appliance (network encryption, key management, etc.)	
Best performance in terms of throughput and latency for FPGA-based appliances	
Designed for security, with tamper-evident chassis and tamper-proof key (FIPS 140-2 Level 3 and CC EAL 2+)	
Physical separation of trusted and untrusted networks	
Separation of duties between network and security functions for best practices	
Extensive configurable functionalities for improved security and compliance (audit reporting, role management, etc.)	
FPGA- and CPU-based appliances are upgradable, increasing lifetime and functionalities of the appliance	
Longer MTBF for better cost amortization	
Lower installation, maintenance and operational costs than integrated appliances	
Lowest total cost of ownership for mid- and longer-term cost savings	

3.2. Integrated Network Appliance: Add-on Card for Encryption

Layer 2 encryption functionality is also available as an add-on card for switches (such as those of Cisco) or certain multiplexers. Adding a board with specialized hardware to support the encryption requires a slot in the chassis, tamper-proof key storage and shielding from the rest of the chassis. The functionality of such add-on cards is often limited due to space, heat and cost constraints. This approach ties the encryption to the device that hosts the add-on card.

Advantages	Disadvantages
Combines core functionality (switching, routing) with add-on functionality (network encryption)	The total cost of ownership is higher than for dedicated devices (see 4.5. Cost below). There are multiple hidden costs after initial purchase, including cost of the add-on card/blade for indispensable hardware acceleration, cost of slot in chassis, change of hardware for future upgrades
Small upfront cost savings over separate dedicated appliance	Mostly no retrofit for existing network equipment, requires purchase of new network equipment
Less space required for data center and remote locations	Cost, heat and space constraints limit scope of encryptor network compatibility and upgradability
Fulfills basic compliance requirements	Often lacks the necessary internal shielding and tamper-proof key storage
	Lifespan of encryptor limited by lifetime of host network device
	Vendor- and model-specific add-on cards/blades produce a vendor lock-in
	Vulnerability of host network device extended to network encryption
	Network and network security consolidated in a single device, forcing changes in best business practices (ie. no separation of duty)
	Lower performance and potential packet loss at high bandwidths due to competition for limited resources (eg. encryption & switching)
	Higher operating and maintenance costs lead to higher total cost of ownership
	Lower, if not no security certification

3.3. Integrated Network Appliance: Encryption on NIC

Another way to implement layer 2 encryption functionality is directly on the network interface card (NIC) using an ASIC (Application Specific Integrated Circuit). This is the approach used by the Cisco Nexus 7000. While providing hardware acceleration for the encryption, such a solution is not designed for security as it lacks tamper-proof key storage and efficient shielding.

Currently on the market there are only network interface cards that support MacSec. MacSec is a proprietary hop-to-hop Ethernet encryption protocol designed to protect links on internal Local Area Networks, which brings significant limitations to real-life WAN and MAN environments. Firstly, MacSec cannot support a multipoint scenario, or be used securely on managed networks, as each switch opens up (decrypts) the packet and then encrypts it again before sending it on. Secondly, there are compatibility issues with existing (or future) network equipment especially in VLAN topologies, as the MacSec tag is placed in front of the VLAN tag. Using a proprietary protocol forces vendor lock-in for other networking equipment, increasing the cost of ownership.

Advantages	Disadvantages
Combines network interface and encryption	Encryption is tied to network interface card
Network access and network security consolidated on a single card	Mostly no retrofit for existing network equipment, requires purchase of new network equipment
Space savings for data center and remote locations	Cost for slot in chassis needs to be taken into consideration
Fulfills basic compliance requirements	Cost, heat and space constraints limit scope of encryptor network compatibility and upgradability
	Lifespan of encryptor limited by lifetime of host network device
	Vendor- and model-specific add-on cards/blades produce a vendor lock-in
	Mostly no retrofit for existing network equipment, requires purchase of new network equipment
	Vulnerability of host network device extended to network encryption
	Higher operating costs and higher total cost of ownership (see 4.5. Cost below)
	Limited deployment options (company operated Vs. managed security service)
	Lower, if not no security certification

3.4. Integrated Security Appliance

While there are currently no integrated solutions that work without add-on cards, such units will undoubtedly become available within the next few years. These will most probably be multi-functional security appliances which can handle different security tasks, including layer 2 encryption. The biggest challenge for integrated security appliances is the need to perform all the different tasks concurrently without either a degradation in performance degradation or a reduction in functionality. An integrated solution tends to do many things, but not everything well. The reason for this lack of excellence is in large part due to the compromises required to make the integrated appliance cheaper than the dedicated appliances it competes with. Tamper-proof key storage and efficient shielding do not come automatically with an integrated security appliance, but are needed to meet security requirements.

Advantages	Disadvantages
Comprehensive security in a single device	No separation of duties and tasks
Addresses major security concerns at the network perimeter	Mixes different network and encryption layers
Cost savings over component-specific appliance purchases	Multi-tasking without sufficient computing power impacts performance
Space savings for data center and remote locations	Increased vulnerability of appliance extended to network encryption
Fulfills basic compliance requirements	Jack-of-all-trades but master of none
	No optimisation of layer 2 encryption
	Mainly based on software

3.5. Virtual Appliance

CPU-based encryption can be deployed as a virtual appliance in the cloud, running on a virtual machine. However, even when it run as virtual appliance in an elastic cloud, it remains CPU-based and comes without hardware acceleration. As a result any virtual appliance suffers from limited throughput and increased latency. Contrary to hardware accelerated deployment methods, virtual appliances cannot provide Gigabit/second throughput with single-digit microsecond latency.

Advantages	Disadvantages
Simple deployment	Higher latency and lower throughput than hardware accelerated solutions
Software only	Security dependent on security of virtual machine
Easy to update	No tamper-proof key storage
Reduced cost	No hardware security
Scalable encryption for cloud-based services that are accessed over Ethernet	
Can be used complementary complementary to dedicated appliances in single network	
Fulfills basic compliance requirements	

4. Dedicated Appliances: Making the Right Business Choice

So why go for a dedicated encryption appliance if you can get encryption as an integrated or add-on function or even as a virtual appliance? There are five reasons: flexibility, security, performance, upgradability and cost.

4.1. Flexibility

Dedicated appliances can be added to an existing network as bump-in-the-wire, saving companies the (often hidden) cost of other network hardware upgrades. There is no need to reconfigure a router, and as there are no dependencies on other hardware there is reduced vendor lock-in.

4.2. Security

Dedicated appliances are designed for security and meet the highest requirements, also in terms of certifications. The systems form a closed and tested environment which has been proven to be secure. Since the unit's interfaces are limited to those which are absolutely necessary, the number of entry points is reduced and the unit's own security is improved. Both the case and key storage are fully secured and the protection includes measures against emissions. Any attempt to tamper with the unit will result in the immediate emptying of the key storage and the notification that an attempt at tampering took place. The casings are tamper resistant.

For integrated appliances it is impossible to provide this level of security. These units have far more interfaces to the outside than a dedicated appliance and thus feature many more entry points for attackers. This increased vulnerability is also illustrated by the number of important security patches for integrated appliances.

4.3. Performance

Dedicated appliances are optimized for performance. There is no competition for the available resources between different functionalities.

Integrated appliances are optimized for specific performance features which can hardly ever be fully exploited in parallel. For example when an integrated unit needs to do a lot of switching, the throughput of encrypted data is reduced and the latency increased in unpredictable ways. Also, cost considerations often favor the use of ASICs (Application Specific Integrated Circuits) over FPGAs. Those ASICs support only a limited set of functions and if functions are used that are not implemented in the hardware, they are then executed in software which leads

to a performance loss. As ASICs are not field-upgradeable, no new functions can be added without changing the ASIC itself.

4.4. Upgradability

Dedicated layer 2 encryptors tend to be specified and dimensioned in a way that allows the extension of new functionalities at a later point in time. This is an essential requirement to keep the device state-of-the-art for the years to come. Amply dimensioned FPGAs (Field Programmable Gate Array) fit the requirement, but they also increase the initial cost. Underpowered FPGAs are quickly saturated and draw a high amount of power, which leads to extensive heat development. Dedicated Layer 2 encryptors' upgradable platforms now support new algorithms and a larger key size. This allows for a flexible re-programming in field.

Hardware upgradability and expandability are cost drivers and thus not that high on the priority list for developers of integrated appliances. They focus on initial cost containment rather than on mid- to long-term cost efficiency for the customer.

4.5. Cost

Encryption implemented as a supplementary function in integrated appliances can use a lot of the basic network and management infrastructure provided by the main functionality of the device. There is no cost for an additional casing, an additional redundant power-supply or a network processor. This reduces initial cost and price, but it ties the encryption to the proprietary integrated appliance. The average product life of a dedicated encryption appliance exceeds that of an integrated appliance by 2-3 years, leading to lower cost of the dedicated encryption appliance over the entire product life. The initial cost savings of the integrated appliance turn into higher cost over time. When combined with the changes to network configuration required for integrated devices (often hidden or under-scoped at the time of the original purchase), it is clear that the total cost of ownership for dedicated devices is significantly lower.

Another aspect that is often not taken sufficiently into consideration is the vendor lock-in: Although dedicated layer 2 encryptors from different vendors are not compatible, this is compounded if the encryption is integrated with the switch or router, leading to double vendor lock-in. Changing the vendor at a single site will exclude that site in terms of encryption from the MAN/WAN. It is mandatory to use the same vendor for encryption and for switching at all sites, resulting in a double lock-in. This means that it is no longer possible to seek cost reductions through a change of suppliers, such as from Cisco to Juniper, HP, Ciena or Huawei, as all integrated appliances would need to be exchanged at the same time. A 2010 Gartner report estimates a 15-25% price premium over 5 years for having an all-Cisco network. A single-vendor network also suffers from increased operational complexity. Only dedicated encryption appliances are completely independent of switches and routers and thus reduce vendor lock-in. Introducing a second network vendor reduces lock-in, improves network performance and reduces cost.

"ID Quantique was the only company to provide the product performance and speed and flexibility of service required to meet our encryption needs during the transition to a new data center and headquarters."

Business and IT Services manager of a Private Bank

5. Conclusion

Purpose-built and dedicated layer 2 encryptors constitute the best solution for securing layer 2 Metro and Wide Area Networks. They come without dependencies and keep their focus sharply on their sole task, thus operating as efficiently as possible. Processes and management are simple, straightforward and completely optimized for the job at hand, and the separation of duties between network and security matches business and compliance requirements. As well as providing clear benefits in performance and security, dedicated encryption appliances also have a positive mid- and long-term impact on flexibility and cost, offering a lower total cost of ownership over the lifetime of the product. FPGA- and CPU-based solutions can be updated with software to ensure that they constantly evolve to meet new business and technical requirements.

While there are different ways to integrate layer 2 encryption into other appliances and to perform encryption as a side-job, none of these approaches provide the security, efficiency or cost-effectiveness of a purpose-built encryption appliance. For high-performance, low latency solutions, a dedicated hardware encryptor is a must.

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com