inside-it.ch

PRESENTS:

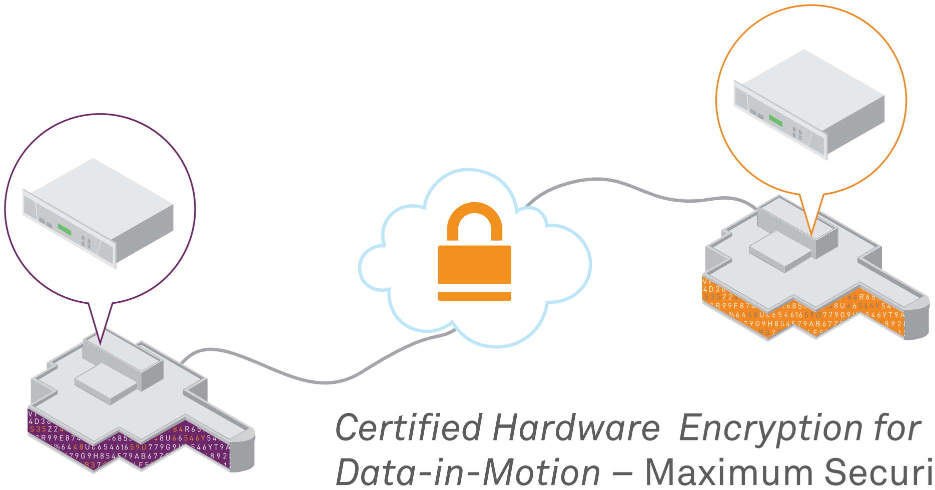
LAYER 2-ENCRYPTORS
FOR
METRO AND CARRIER ETHERNET

EVALUATION GUIDE

(SHORT VERSION)

Version 1.3, January 7, 2015

www.uebermeister.com
cjaggi@uebermeister.com



Introduction

Security is a key issue for any MAN or WAN. This is also true for Metro and Carrier Ethernet. While simplicity, efficiency and lower cost combined with increased availability and improved interoperability drive the adoption of Metro and Carrier Ethernet, finding the right security solution can be a challenge. Similar to MPLS, Sonet/SH and OTN, but in contrast to IP networks, Metro and Carrier Ethernet do not come with built-in network security. Therefore specialized security solutions are needed. Such Ethernet encryptors can be extremely powerful and meet highest security requirements. A comprehensive introduction into Ethernet (layer 2) encryption for Metro and Carrier Ethernet is available here:

http://www.uebermeister.com/files/inside-it/2014_Introduction_Encryption_Metro_and_Carrier_Ethernet.pdf

Only Native Ethernet Encryptors are Real Ethernet Encryptors

Not all devices that are marketed by vendors as Ethernet encryptors are native Ethernet encryptors. And many devices that feature native Ethernet encryption use a technology that was designed for local area networks and is not suitable for MAN and WAN use. There are different ways to encrypt and transport Ethernet, but not all of them are equally efficient and safe. From a network point of view, security should add only minimal overhead, latency and jitter, while being a perfect network citizen. From a security point of view, there is no real security without network and frame overhead. There are native layer 2 Ethernet encryptors available on the market providing the right balance between network and security requirements.
To make things really confusing, there is an IEEE standard to secure and encrypt local area Ethernet networks. Due to its focus on hop-to-hop instead of end-to-end encryption, a key system that is purely port-based and its limitations to point-to-point and point-to-multipoint it is rather unfit for MAN and WAN use. As much one wouldn’t use slippers for a mountain hike, it is not a very smart idea to use MACSec for MANs and WANs. Plagued by its overreaching limitations, its different focus and severe interoperability issues, MACSec is mainly promoted by vendors who do not have a qualified offering in their portfolio. MACSec is an appropriate solution for local area networks (LAN) and, if Ethernet encryption is needed for such an environment, then MACSec is a viable solution. Only if you own and operate the MAN or WAN, or if there is a constellation where hop-to-hop equals end-to-end, MACSec can be made to work properly. As MACSec is limited to transport mode encryption, it does however not meet more than bare-bones security requirements for authenticated encryption.

The Complexity of an Evaluation

Evaluating Ethernet encryptors is complex. Network encryptors a bi-functional: On one hand they are security devices, and on the other hand they are network devices. An Ethernet encryptor combines encryption with switch functionality. The feature set needed can be elusive, depending on the requirement profile in terms of security and switch functionality. Preferably Ethernet encryptors support both, the available network infrastructure and the planned usage scenario. This is provided by an interlocked combination of software and hardware. But beware: It is not just the functionality that counts. As multiple incidents involving FIPS- and Common Criteria-certified encryption products have shown, implementation is the decisive factor. A good Ethernet encryptor doesn't just provide security for the data traffic. It also must be a capable and secure network device. In most cases this prevents the use of virtual appliances and white-box approaches.

Different Customers – Different Requirements

Different customers have different requirements. A specific Ethernet encryptor therefore can fulfill all current and foreseeable requirements for a certain percentage of customers without being a fit in terms of functionality for other customers. A specific Ethernet encryptor might thus be a good fit for one customer while being completely unsuitable for another customer. The Ethernet encryptors available on the market differ in terms of network support, network functionality and security. Although hard to comprehend, there are even still customers who don't have authenticated encryption on their requirement list. Such customers are becoming a rarity though and might be completely extinct within the next couple of years.

For service providers offering encryption as a managed service, things look different, as they tend to cater to a multitude of different customers with different requirements. Thus for providers of managed security and managed encryption either the choice of encryptors or the market potential is limited.

Table of Contents

Protect data center and site-to-site connections from eavesdropping

Encryption and IT security
Made in Germany

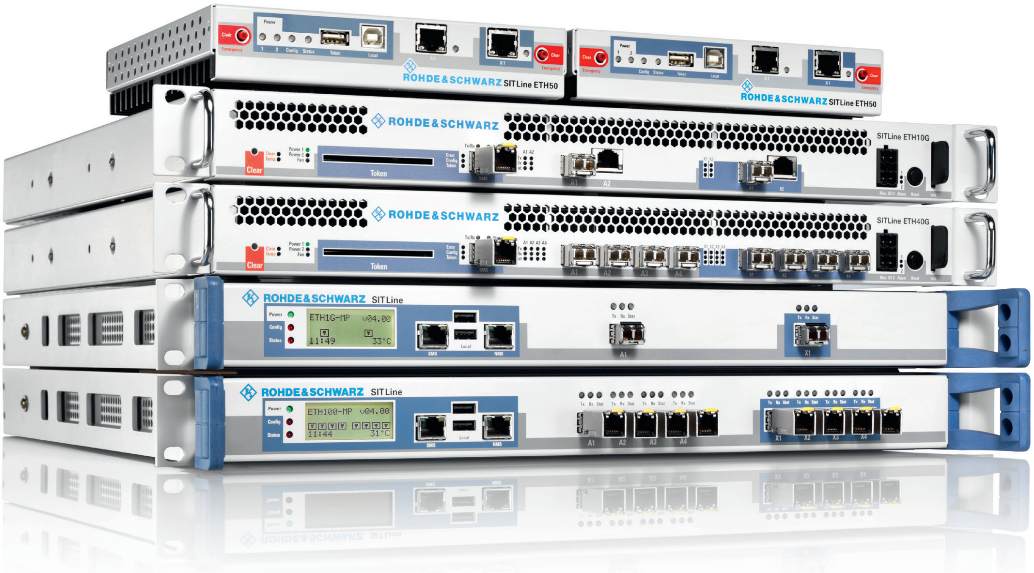
When connecting sites and data centers, confidential information leaves your secured and trusted grounds. Big Data, Mobility and Globalization are driving the amount and the value of your data in motion. But optical and electrical lines can easily be tapped.

R&S®SITLine ETH encrypts your data before transmission – highly efficient, real-time, government-approved.

- Ethernet encryptor appliances for outstanding manageability and security
- Up to 40 Gbit/s throughput per device
- Minimal latency (3µs) for real-time applications
- Support for network topologies using landline, radio relay and satellite links
- Approved for German and NATO RESTRICTED classification levels

Request more information or arrange an appointment with one of our experts:
Phone: +49 (0) 30 65884 223
info.sit@rohde-schwarz.com

www.rohde-schwarz.com/sitline



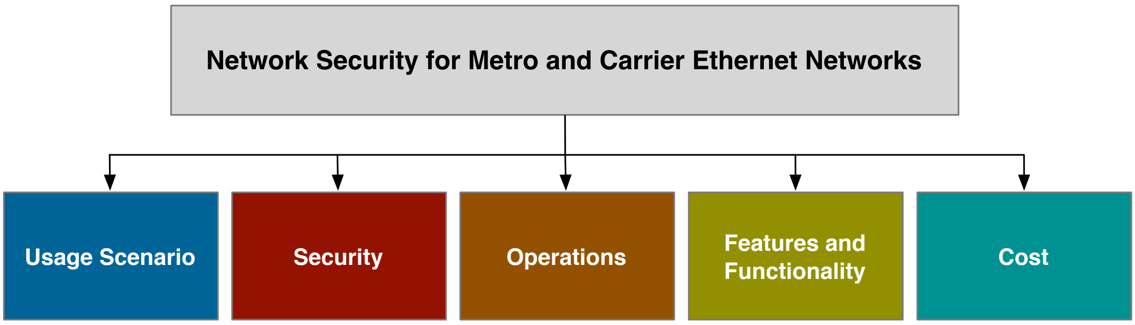
ROHDE&SCHWARZ

Section 1: Approach

Carrier Ethernet offers a simple and cost-efficient way to network sites: Local, regional and international. But it should also be secure in terms of the transmitted data and in terms of the network itself. Nobody should be able to get hold of unsecured data, nobody should be able to modify data in transit and nobody should be able to insert unauthorized data into the network. A combination of network encryption, intrusion detection, intrusion prevention and firewall will accomplish that goal. The use of authenticated encryption at layer 2, such as AES-GCM, can help to provide such an extensive protection without requiring additional expensive devices.

There are many products that are marketed as Ethernet encryptors and there are many different ways to encrypt Ethernet. There are huge differences in terms of security and network compatibility, though. The best solution is always a product that combines maximal network compatibility with optimal network security and is available at reasonable cost.

Finding the right solution is not trivial. Starting point is always the usage scenario. It is defined by two factors: (1) The existing and the planned MAN/WAN and (2), the transport networks. The next step is the determination of the security requirements and the business needs. Based on this information it is possible to define the required feature set in order to be able to select suitable products. The closing factors are the acquisition and operating cost of the suitable products.
The approach consists of the definition of the requirement profile, the finding of suitable products and the selection of the most efficient solution.

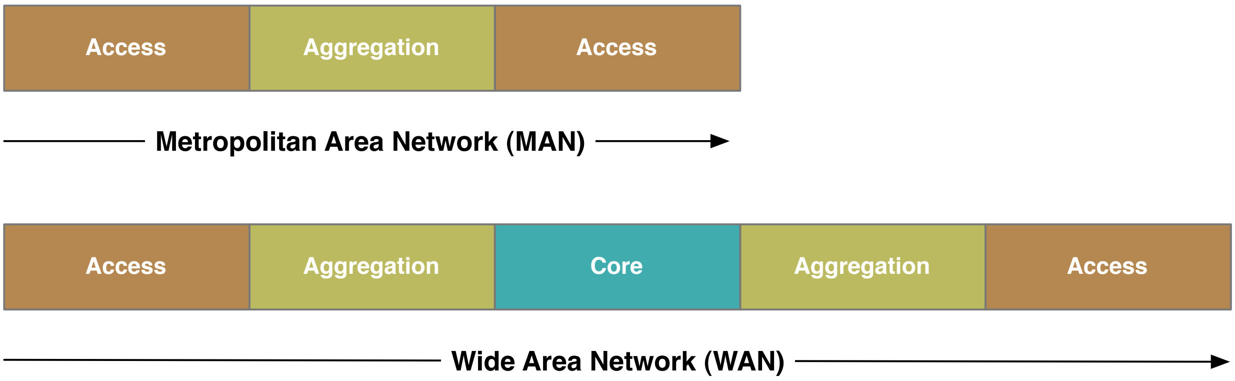

Network Security for Metro and Carrier Ethernet Networks
Usage Scenario
Security
Operations
Features and Functionality
Cost

Section 2: Usage Scenario

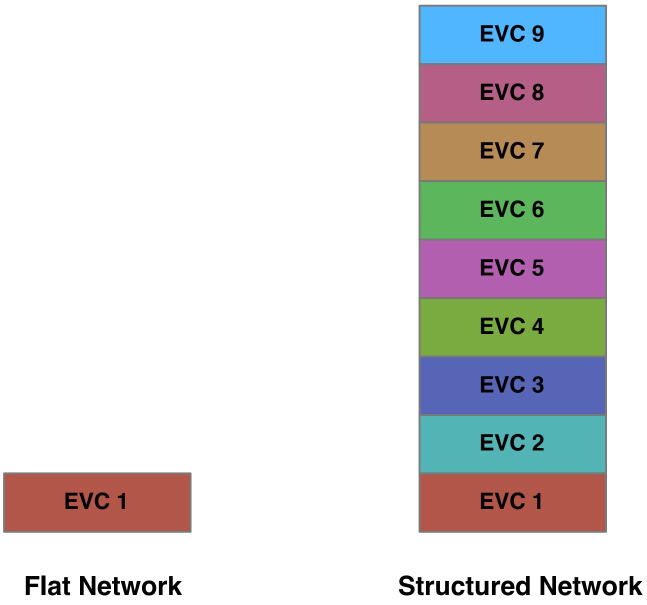
To identify the requirement profile it is best to start with the usage scenario of the MAN or WAN. This allows define the needed feature set of the encryptor.

1. MAN or WAN?

Carrier Ethernet in a MAN usage scenario often differs from Carrier Ethernet in a WAN usage scenario. A MAN sometimes requires less network functionality requirements for an encryptor than a WAN.



Carrier Ethernet networks can be segmented and structured using VLANs and Ethernet Virtual Channels (EVC).



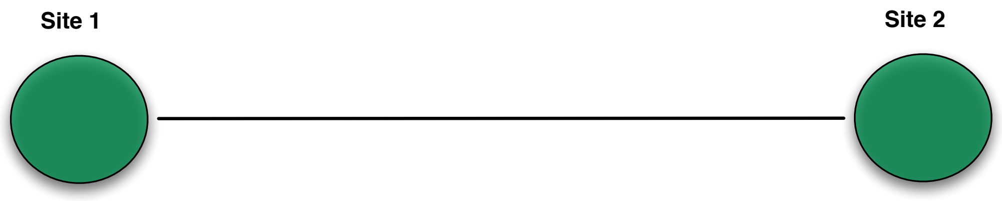
An Ethernet Virtual Channel (EVC) is a virtual Ethernet network that can contain multiple VLANs. In many cases it is preferable, or even necessary, to use multiple

Ethernet Virtual Channels. This allows an efficient structuring and segmentation of the network. SLAs are normally tied to EVCs. The use of multiple EVCs makes it possible to use different SLAs based on actual requirements, thus optimizing the cost profile per EVC.

2. Network Topologies and Usage Scenario

2.1. Point-to-Point

If the network is limited to the interconnection of two sites, the scenario is simple. Securing point-to-point connections is not as difficult as a fully meshed environment. Due to the homogeneity of the connection there are no excessive requirements for the feature set of the key management.

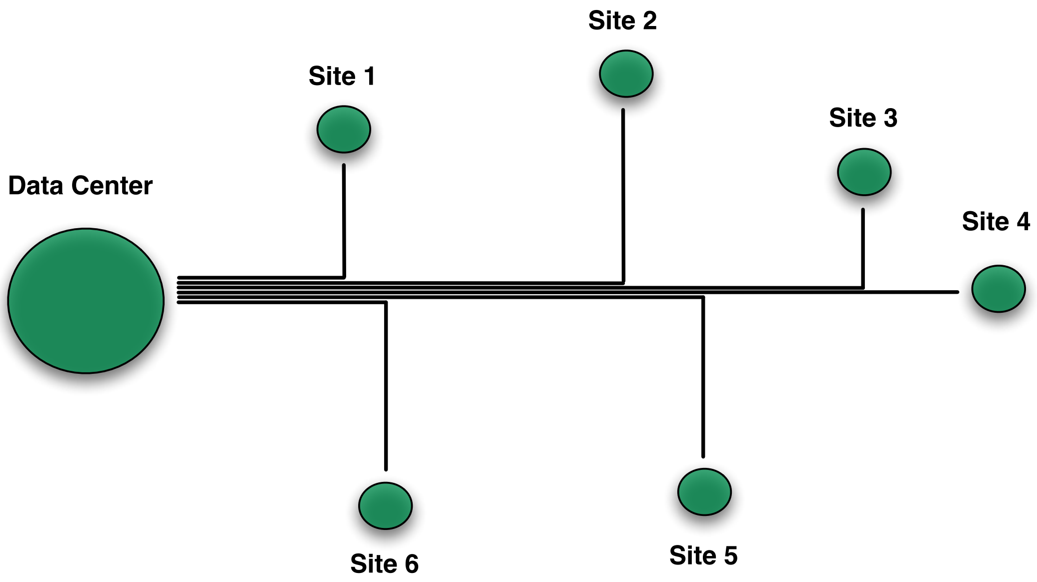


Like many other business processes, network security can be outsourced to a specialized service provider. In such a case there is a requirement for a tenancy capability that supports key ownership by the tenant. If the key ownership or the control over the encryption were to be with the service provider, there would be a severe security risk. The key owner can decrypt everything; therefore the key ownership must be with the tenant. The party that controls the activation of the encryption should also be the tenant. The service provider should not have the capability to switch the encryption on and off without the explicit authorization to do so by the tenant.

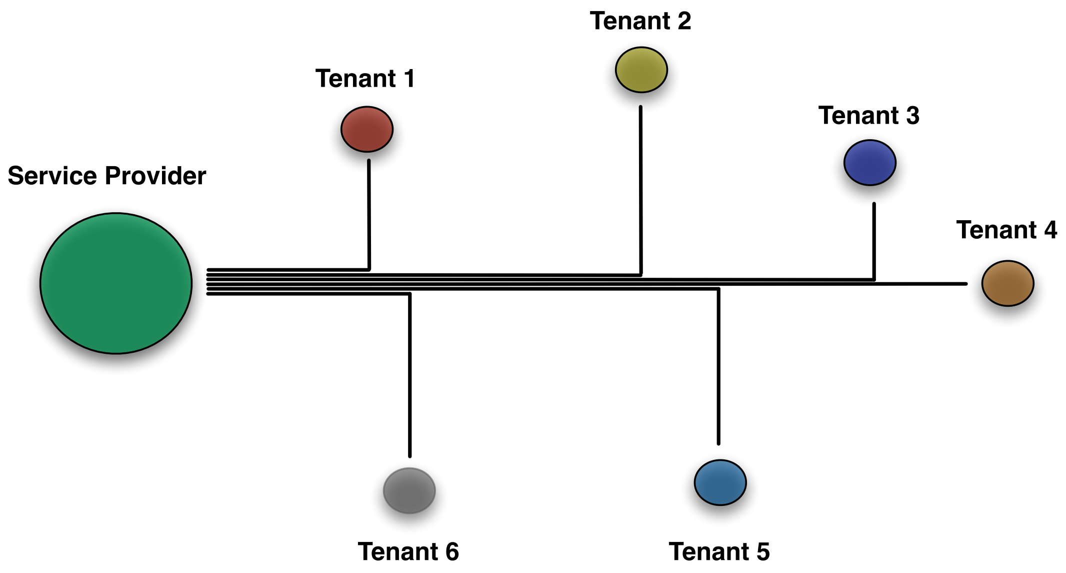
2.2. Point-to-Multipoint

Point-to-Multipoint topologies are multiple point-to-point connections or single point-to-multipoint connections that originate at the same central source. They are often used to connect a data center with multiple sites. Compared to separate point-to-point connections the network and encryption cost are lower and there are more usage scenarios, but the complexity can be much higher.

If the network security or the encryption is outsourced to a specialized service provider, the same criteria concerning tenancy support exist as with point-to-point connections.

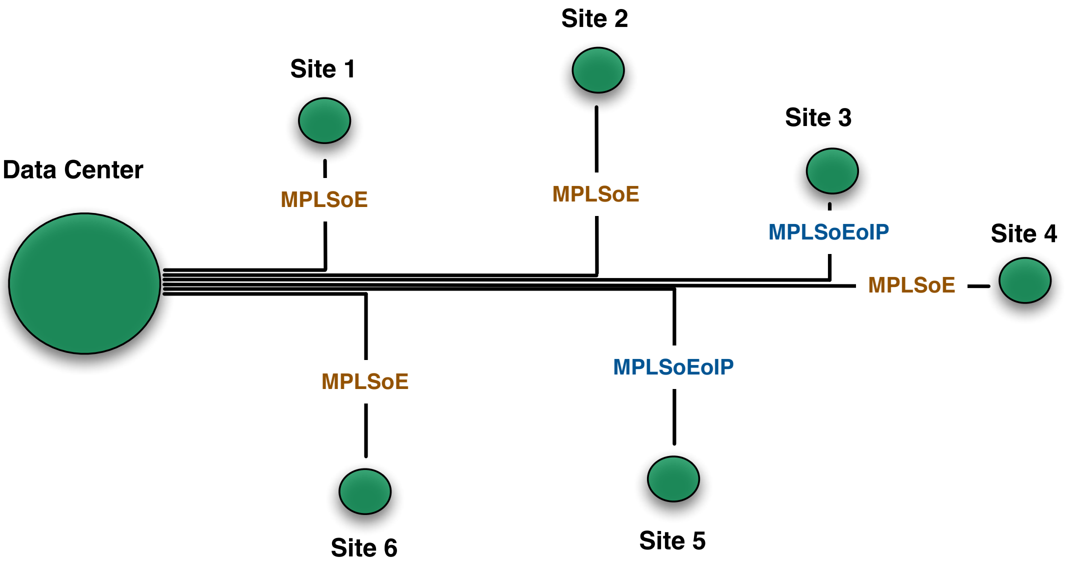


The picture looks different if there are multiple tenants.



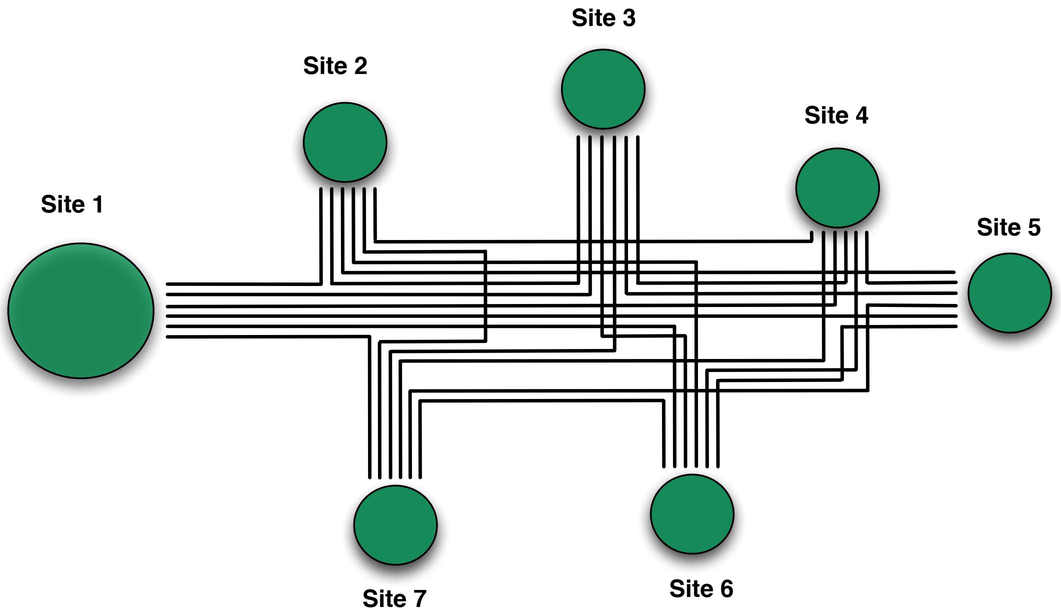
In such a scenario single tenancy support is not sufficient. Instead multi-tenancy capability is required. Each tenant needs ownership of his keys and ownership of his encryption.

In point-to-multipoint scenarios, there are sometimes use cases in which not all sites are connected through Carrier Ethernet. One such use case is MPLS networks in which the vast majority of sites are connected using Carrier Ethernet (MPLSoE), but in which a small number of sites is only reachable through IP. In such a case it is helpful, if an encryptor also supports Ethernet over IP (EoIP). This allows the use of MPLSoE across the entire network, including the sites that can only be reached through IP.



2.3. Multipoint-to-Multipoint

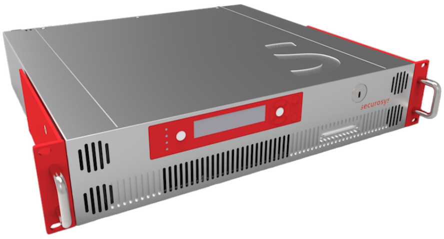
Contrary to a point-to-multipoint topology, a multipoint-to-multipoint topology supports the direct connection between all sites. There is no single central site. Each site in a multipoint-to-multipoint can communicate directly with all other sites in the network. Such meshed networks can be structured and segmented using different VLANs and EVCs.



While a single-tenancy operation of the security of such a meshed network is not more complex in terms of feature requirements than a point-to-point or point-to-multipoint network, multi-tenancy is a challenge. It would require a complete virtualization of the encryptors. Hardware can only be virtualized up to a certain degree in a way that doesn't compromise security, performance and operations.

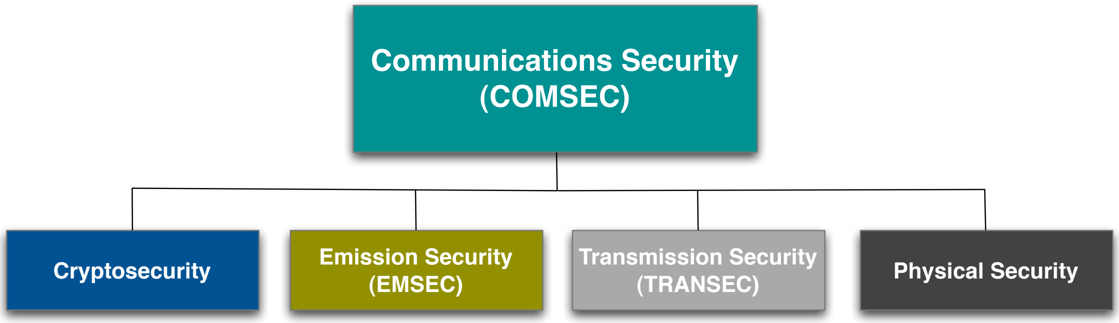
Key questions:

- What is the topology of the network to be protected?
- Is it a MAN ar a WAN?
- Will the network be extended in the foreseeable future and if yes, will that have implications on the network topology?
- Are Carrier Ethernet connections available at all sites or is there a limited number of sites that can only be reached through IP?
- Is Ethernet connectivity a requirement for some applications?
- Is the network security or encryption self-managed or outsourced to a service provider?
- Is network security or encryption offered as service for customers? If yes, are there multiple tenants per network?



Section 3: Security

Communications security comprises different aspects that in their entirety are known as COMSEC.

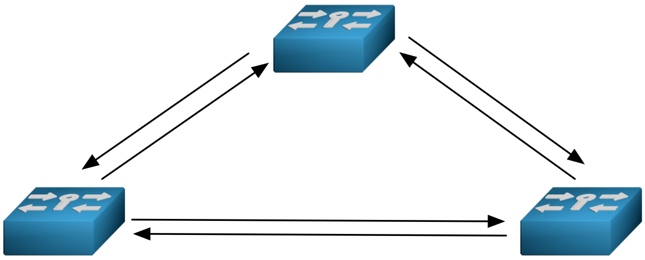

Communications Security (COMSEC)
Cryptosecurity
Emission Security (EMSEC)
Transmission Security (TRANSEC)
Physical Security

Full COMSEC requires a combination of software and hardware. There is no full communications security without hardware.

1. Cryptosecurity

Superficially crypto security consists mainly of a block cipher, an operating mode and keys. The current standard with Ethernet encryptors is AES as block cipher, GCM as operating mode and a key length of 256 bits.
A closer look reveals the complexity of crypto security, Key management is multi-layered and requires initial secrets on each of the involved encryptors. The first challenge is to get the initial secrets onto the encryptors. As communication involves more than a single party, all participating encryptors must authenticate themselves mutually. Once that is accomplished there is a connectivity association between each of the participating encryptors on which security associations can be established.

Connectivity Association

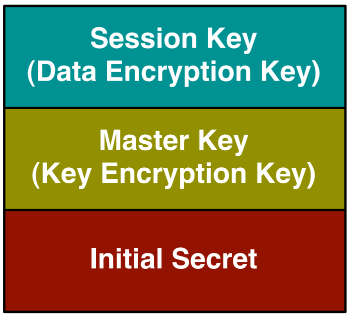


Establishment of permitted device connectivity

Authentication through certtificate or pre-shared key/pre-shared secret

1.1. Key Management

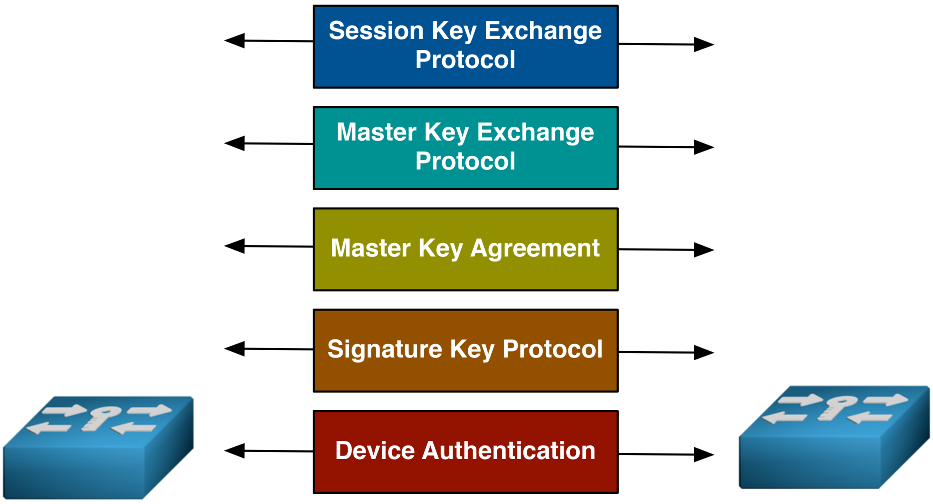
A simplified view of the key hierarchy shows three layers: An initial secret for the authentication, a master key (key encryption key) to encrypt the session key and a session key (data encryption key) to encrypt the data.



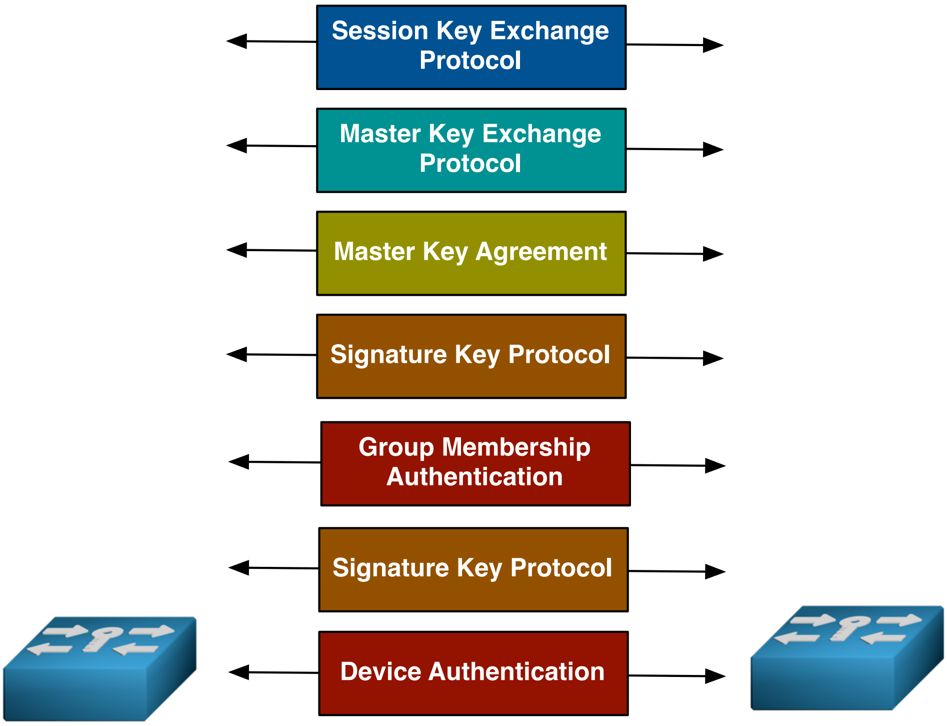
1.1.1. Initial Secrets and Key Hierarchy

In reality things are much more complex. It starts with establishing who may communicate with whom. The connectivity association is the foundation for the security association that determines how the connected devices communicate securely. This is accomplished using an initial secret and a key agreement protocol. The initial secret can be a pre-shared key or a certificate. In the case of elliptic curve cryptography the curve domain is also an initial secret that needs to be present.

In the build-up from initial secret to session key, multiple complex processes take place. Each of them needs to be secure by itself and in the sequence it is being used.



The complexity is even higher for group key systems as not only the device, but also the group memberships needs authentication. This requires an additional initial secret specific to that group.


Session Key Exchange Protocol
Master Key Exchange Protocol
Master Key Agreement
Signature Key Protocol
Group Membership Authentication
Signature Key Protocol
Device Authentication

When looking at group key systems, a focus should be set on verifying that layered connectivity and security associations are supported: Next to the mutual authentication of devices and the device-based connectivity and security association also separate connectivity and security associations must be supported for each group.

Secure keys are dependant on the true randomness that can only be provided by hardware-based real random number generators. Additionally the strength of a key has to be verified before it is employed for usage. Hardware is also needed for the secure key storage, which should be tamper-proof.

1.1.2. Key and Key Exchange

There are two different approaches to key exchange: One is symmetrical and the other on is asymmetrical. The asymmetrical approach needs more computing power but is considered to be more secure. A big jump in security is provided by a combination of asymmetrical and symmetrical key exchange, such as the combination of Diffie-Hellman with symmetrical encryption of the partial keys.

In a symmetrical approach, all keys are directly derived from each other. First, a shared secret is entered into the encryptor. Then the encryptor generates internally a master key and encrypts the master key with the shared secret. The session key is also generated by the encryptor and is encrypted with the master key. Master key and session key are transmitted to the other encryptor in encrypted form. The big issue with this approach is the shared secret. If that shared secret ever becomes known, then all previously recorded data communication can be decrypted.

In an asymmetric approach the partial keys are generated completely inside the encryptor, without any user having access to it. After exchanging the partial keys both sides calculate the same shared secret. Contrary to a symmetric approach, nobody knows the shared secret.
Subsequently the encryptor generates internally the master key and encrypts it with the shared secret. The encryptor also generates the session key and uses the master key to en-crypt it. The transmission of the master and session keys from one encryptor is always encrypted.
Common asymmetrical approaches are Diffie-Hellman and RSA. Diffie-Hellmann uses in its basic variant the discrete logarithm problem, which comes with the disadvantage of needing very long partial keys to be really secure. A more state-of-the-art variant is the use of Diffie-Hellman with elliptic curve cryptography (ECC), which provides better security with shorter partial keys. The security of ECC is heavily dependant on the curves used. Alternatives to the NIST curves, such as the Brainpool curves, should be preferred.
Asymmetrical approaches sign the partial keys that are exchanged to ensure that the correct remote station sends them. There are different ways to accomplish this: Either by using a certificate (X.509) in combination with appropriate procedures (RSA, DSA or ECC) or by encrypting the partial keys with a pre-shared secret.

Most systems use a hybrid approach. Session keys are always symmetric.

1.1.3 Exchange Frequency

The more frequently the sessions keys in use are replaced, the lower the probability that the key will be compromised. The security of the key does not only depend on the secrecy of the key, but also depends on the process used and the parameters chosen. The length of the counter and the ICV play an important role. E.g. in counter mode the key has to be changed before the counter starts back at 0. It is therefore required that the system automatically changes the session key after a given number of minutes.
The same is true for the key encryption key (master key), which is used to encrypt the session keys. The exchange frequency is lower as it is only used to encrypt the session key and thus is used less often and encypts less data. The regular exchange of master keys should take place automatically after a certain period of time. Key exchanges using Diffie-Hellmann are compute-intensive. Sufficient processing power of the encryptor is a requirement for keeping the lifecycle of a master key low, especially in large, complex networks.

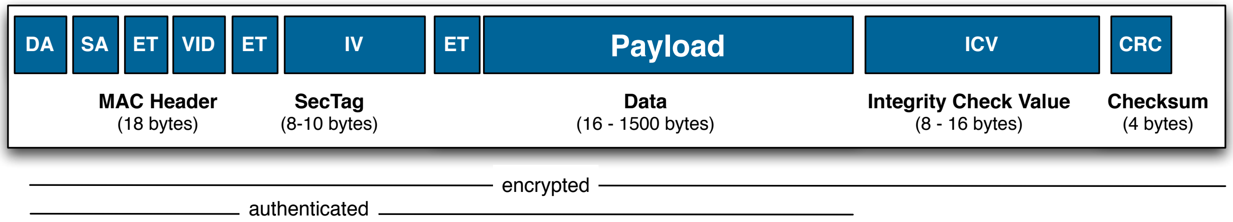
Key Type	Change Frequency
Session Key (Data Encryption Key)	every 1 - 60 minutes
Master Key (Key Encryption Key)	every 1 -24 hours
Initial Secret	every 12 - 24 months

A further aspect of the key management can be found in the key assignment. In Ethernet networks the key assignment can be either based on the port or on the VLAN-ID. VLANs are groups. Therefore a group key system is required for VLAN-based key assignment.

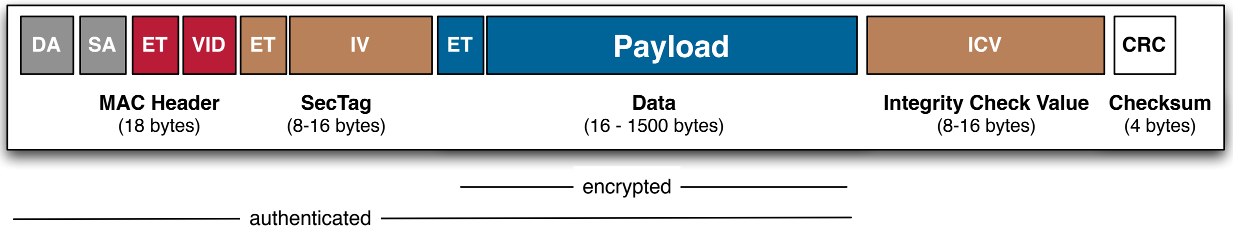
1.2. Encryption Mode

For Ethernet there are three different encryption modes: Frame, transport and tunnel. Each of these modes exists in an authenticated and an unauthenticated variant. The selection of the appropriate mode depends on the network and the security requirements. Unauthenticated encryption has quickly fallen out of favor as it can only provide confidentially of the data. It is however not capable of protecting the network as it misses the intrusion detection, intrusion prevention and firewall functionality provided by auuthenticated encryption. It is highly recommended to use a solution that incorporates authenticated encryption.

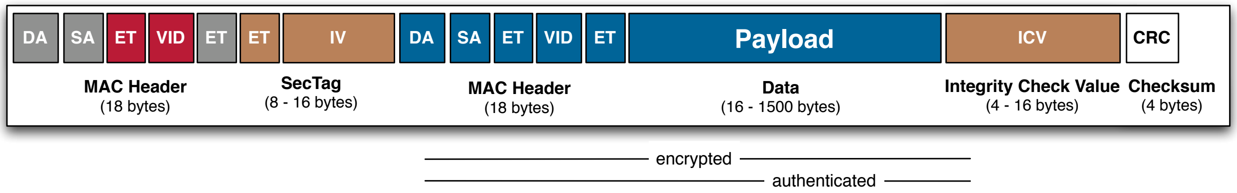
The frame mode encrypts the entire frame. It is the preferred solution if there is a direct connection without additional hops between the encryptors of in cases where the original frame is tunneled.



Transport mode is compatible with all Carrier Ethernet networks.



Tunnel mode is used if security requirements mandate the hiding of internal Ethernet metadata. Only the outside ports of the encryptors remain visible. It is also the default mode for Traffic Flow Security (TFS).

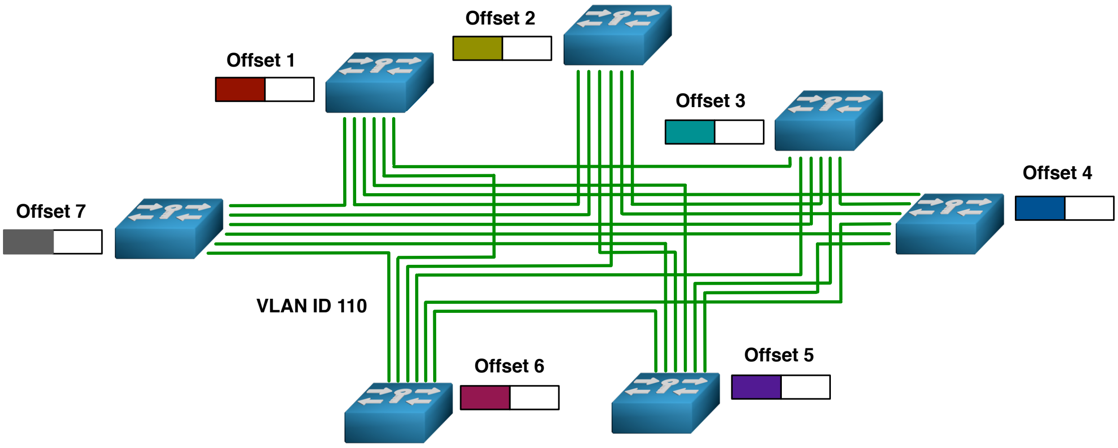


1.3. Impact of the Encryption Mode on Functionality Requirements

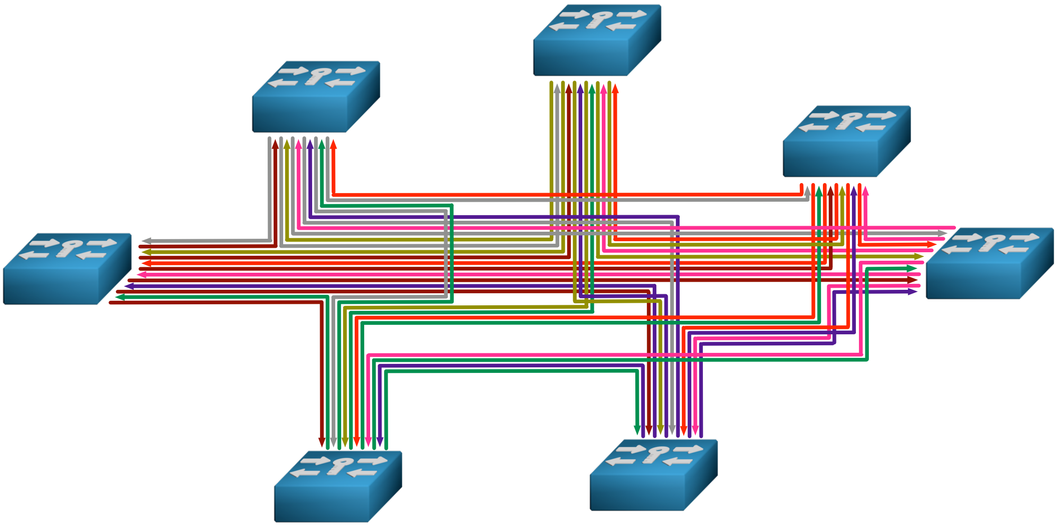
Authenticated encryption and tunnel mode increase the frame size. Most Carrier Ethernet networks accept frames of a size of 1600 bytes without any problem. There can be issues though with Carrier Ethernet networks that do not meet the recommendations of the Metro Ethernet Forum (MEF).
Frame sizes can especially matter in the case of transport of Ethernet over IP (EoIP) when the supported MTU is exceeded. An encryptor should be able to compensate for this by fragmenting oversized frames. This requires additional encryptor functionality.

Authenticated encryption creates an additional challenge for group key systems. The cause for it is the counter that ensures that only frames in the right order or with small deviation from the correct order are accepted. As in a group normally many group members can use the same key for encryption within the group, special measures are needed to ensure the continuity of the counter.

There are different ways to address this issue. One way is to assign a different counter offset to each participating group member. This offset is carried along in the SecTag. All receiving group members thus know which offset was used for a frame and take the specific offset into account when checking the correct frame order.



Another approach is to base the key assignment on the address of the sending encryptor in a group and to use the same key for all outgoing frames from that encryptor in that group. For every encryptor in a group outgoing frames are point-to-multipoint connections, and if the same key is used, then the frame order is kept. The corresponding security association is transported along with the frame in the SecTag. This allows the receiving group members to identify the key to use for decryption.



1.4. Impact of the Initial Secret on Multi-tenancy

The initial secret can consist of a X.509 certificate or a pre-shared secret. Certificates are issued and managed by a Certificate Authority (CA). In a multi-tenancy environment where the key ownership lies with the tenant, the initial secret, in form of a certificate, should be issues by the CA of the tenant. In such a case the encryptor of the service provider would have to accept not only certificates from his own CA, but also certificates issued and managed by the CAs of the individual tenants. This issue is less pronounced if pre-shared secrets are used.

2. Emission Security (EMSEC)

Electronics causes emissions. Specialized devices can under certain circumstances be used to extract data out of the mostly electromagnetic emissions. Under the name TEMPEST, NSA has published specifications concerning spy methods based on the recording of electromagnetic emissions, noise and mechanical vibrations. These specifications also include appropriate countermeasures against such spy methods. The protection for encryptors can be accomplished with special casings and additional infrastructure security.

3. Transmission Security (TRANSEC)

Snooping on networks cannot be prevented. Authenticated encryption can ensure the confidentiality of the data and – by using tunnel mode – hide relevant meta-data. The network traffic itself remains visible. Traffic Flow Security (TFS) prevents the discovery of the traffic patterns on the network by the means of traffic analysis by obfuscating the network traffic. There are different ways to implement TFS. Older approaches use a combination of frame encryption and fixed frame sizes. As this only works on direct point-to-point connections and has severe negative impact on overhead and latency, smarter approaches have been developed. State-of-the-art solutions allow the obfuscation of network traffic in all three encryption modes – frame, transport and tunnel – and support all network topologies: Point-to-point, point-to-multipoint and multipoint-to-multipoint. Using a combination of selective grouping of frames and the adding of fake traffic they prevent any successful traffic analysis. The selective grouping of frames works in any tunnel mode and brings additional benefits as it can be used to increase the network efficiency: Grouped frames only have to be authenticated once and the interframe gap between the grouped frames falls away. However the efficiency of grouping is highest if all frames are between the same two points and decreases with the number of destination addresses served by an encryptor.

4. Physical Security

In case of an attempted tampering the encryptor must be capable to immediately destroy the content of the key storage including the initial secret. Encryptors should be located in a protected place.

Key questions:

- How much security do I need?
- Is the encryptor tamper-resistant??

- How does the key management work? Is it symmetric, asymmetric or hybrid?
- How are the initial secrets entered into the encryptor?
- Are random numbers generated in special hardware?
- How are the keys generated, checked and exchanged?
- Is the key storage tamper-proof?
- Does the encryptor support authenticated encryption?
- Does the encryptor feature a group key system?
- Does the encryptor have to support single or multi-tenancy?
- Which encryption modes do I need: Frame, transport or tunnel?
- Do I need the capability to obfuscate my network traffic?
- Do I need emission security?

Section 4: Operations

Dedicated encryptors are often promoted as “deploy & forget“. One shouldn’t equate that to “plug & play“ though. An encryption appliance is a specialized and dedicated computer in a fit-for-purpose casing that needs to be configured. Once an encryptor is properly configured and there are no modifications required by operations, it will do its job without requiring any intervention except for the periodic exchange of the initial secret. The maintenance window needed for the change of the initial secret and for the passwords can also be used for firmware upgrades. Site interconnections do not change that often and a good encryptor doesn’t need unplanned security updates. Firmware upgrades tend to provide additional functionality and not security fixes, as the security of the devices is in most cases defense-grade.
From an operations point of view, the following areas are most relevant: Configuration, use, monitoring and maintenance.

1. Configuration

Encryptors are network devices and need to be integrated into an existing network. The initial configuration of an encryptor tends to take place locally. There are different approaches to configure an encryptor that all have the same goal: The secure initialization and configuration of an encryptor.
One such approach is to transfer the configuration data using a smartcard. The configuration data is generated at a central location for each of the encryptors and transferred to a smartcard. The smartcards are then transported to the different sites, where the smartcards are inserted into the encryptors. The configuration data is then transferred from the smartcard to the encryptor. A different approach is connecting a PC through a serial or a dedicated managament port with the encryptor combined with local configuration using software. A further approach is the combination of inputs through an encryptor’s front panel and the configuration with the data on a smartcard or using software. Network engineers tend to favor CLIs. Most of the encryptors offer the option of using a CLI.

The creation of user accounts and the assignment of user privileges follows right after the initial configuration of the encryptor. Preferably network management and security management are kept separate. The more granular the role assignments and the user privileges, the better. This permits to adapt the management of the encryptor seamlessly to the existing structures.

2. Use

Complete configuration is a precondition for an encryptor start working. Up to that point, most encryptors block all outgoing traffic. After being properly configured, the encryptors work transparently.
Configuration changes are implemented following the same procedure as the initial

configuration.
Encryptors pass on link loss information they receive. Adding an encryptor to the network will not cause any interruption of the chain of information.

3. Monitoring

SNMP provides monitoring capability concerning current status of the encryptor. System messages can be sent to a Syslog server, whereas local event and audit logs record relevant events in a file that can be accessed when needed.
Encryptors can also monitor each other and inform about the unlikely event of a non-functional encryptor. This functionality is called „Dead Peer Detection“.

4. High Availability

Mission-critical network connections often necessitate full redundancy. There are different approaches to accomplish that goal. Dual homing provides redundancy in terms of the Carrier network, while High Availability (HA) provides redundancy on device level. Some encryptors feature High Availability, which requires a combination of hard- and software. In the unlikely event that an encryptor breaks down, HA allows a backup encryptor to seamlessly take over.

5. Maintenance

Syslog, Event Log and, in worst case, the status LEDs of the front panel, indicate unplanned need for maintenance. Mechanical defects, such as a broken fan, occur as rarely as electronic defects occur. Maintenance is normally limited to the periodic changes of the initial secret and of passwords.

Key questions:

- How static is the number of sites?
- How complex are the configuration and configuration changes?
- How complex is the exchange of initial secrets and passwords?
- How much training is necessary and how extensive is the dependency on external resources?
- How can I integrate the encryptors into my existing network management system?
- How does the user management work? How many roles and hierarchies are supported? How granular is the assignment of user privileges?
- Does the encryptor provide a local event and audit log?
- How extensive is the maintenance requirement?

- Do I need High Availability or is redundancy already provided by other means?

Section 5: Network Overhead, MTU, Latency and Jitter

From a network point of view network overhead, MTU, latency and jitter are essential criteria. Security inevitably leads to network overhead as there is communication between the encryptors causes additional network traffic, even though minimal. Securing each frame increases the frame size and thus is also a cause for network overhead. The increase of frame size is more likely to cause issues than the communication between the enryptors. Authenticated native Ethernet encryption leads to an increase of 24 to 50 bytes per frame, depending on the encryption mode and the length of the SecTag. Under normal circumstances such an increase can be handled without any problem, as Carrier Ethernet should support a minimum MTU of 1600 bytes. Normally Carrier Ethernet also supports jumbo frames of up to 9000 bytes. However there are carriers that neither support an MTU of at least 1600 bytes nor jumbo frames of up to 9000 bytes. In such cases the MTU has to be adapted on the customer side to the size that is supported by the Carrier Ethernet network. That normally happens within the local networks of the interconnected sites. Another solution is the fragmentation of sporadic oversized frames by the sending encryptor and the defragmentation by the receiving encryptor.

FPGA-based encryptors feature a marginal processing time while being easily upgradeable in terms of feature set. The latency caused by the en- and decryption can be neglected. Virtual appliances, on the other hand, take more time to process frames, which can lead to noticeable latency, especially with jumbo frames. FPGA-based encryptors offer a rather uniform latency and thus do not tend to add noticeable jitter. Virtual appliances suffer from the varying availability of shared resources, which causes uneven latency that results in unwanted jitter.

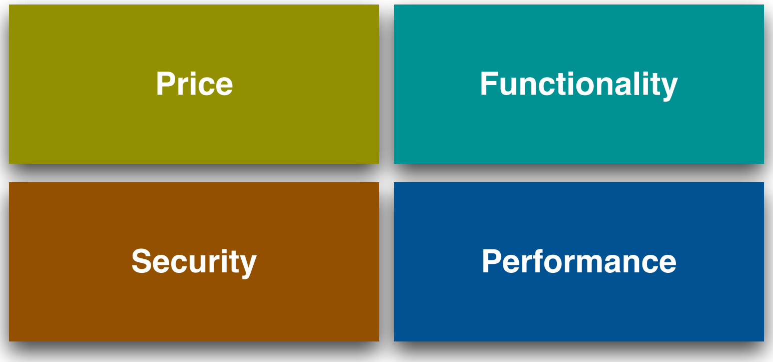
Some encryptors offer special network-oriented functionality next to the standard network and security functionality. These include fragmentation/defragmentation and security overhead optimization; the latter is part of state-of-the-art traffic flow security and selectively bundles smaller frames into a single frame. Both functions are especially relevant if a tunnel is used (Ethernet tunnel mode or EoIP).

Key Questions:

- What size MTU is supported on the Carrier Ethernet network?
- If EoIP is used: What size MTU is supported on the IP network?
- How critical, in terms of latency, are the applications that are used over the network?
- How much may the cost for securing the network be in relation to the network cost? More or less than 15%?

Section 6: Functionality, Security, Performance and Cost

Functionality, security and performance come at a cost. If a low-cost solution is required, then at least security and functionality will be limited.

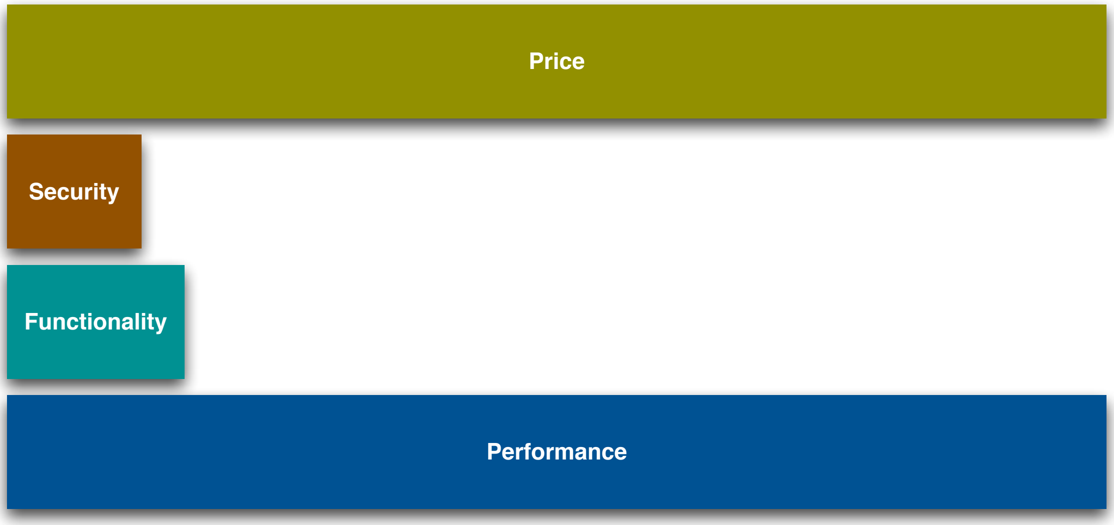


1. Different Approaches

1.1. MACSec as Integrated Solution

Too many people still mistake MACSec as the encryption standard for Ethernet. They forget that MACSec has been developed for Ethernet LANs and not for Ethernet WANs. One of the development objectives was to create a cheap and fast solution that can be implemented on an Ethernet chip. MACSec also led the way in terms of authenticated Ethernet encryption back in 2006. In order to save costs, many compromises were made in terms of requirements for key security and in terms of the key management. The result is a low price combined with high performance, low functionality and limited security. MACSec uses a hop-to-hop encryption and is not suited for the end-to end encryption that is a required for Carrier Ethernet. If there are additional network devices between the two encrypting MACSec devices – what normally is the case – they rather should not be aware of MACSec. Otherwise one of the following scenarios could happen: If connectivity and security association are missing, there is a reasonable probability that the receiving network device will not accept the frames. If the frames are accepted, there is the risk that the receiving network device will recognize the MACSec Ethertype and will try to decrypt the frame even if there is no security association with the sending device. Without security association, there is no key to decrypt the frame and the frame will probably be thrown away.

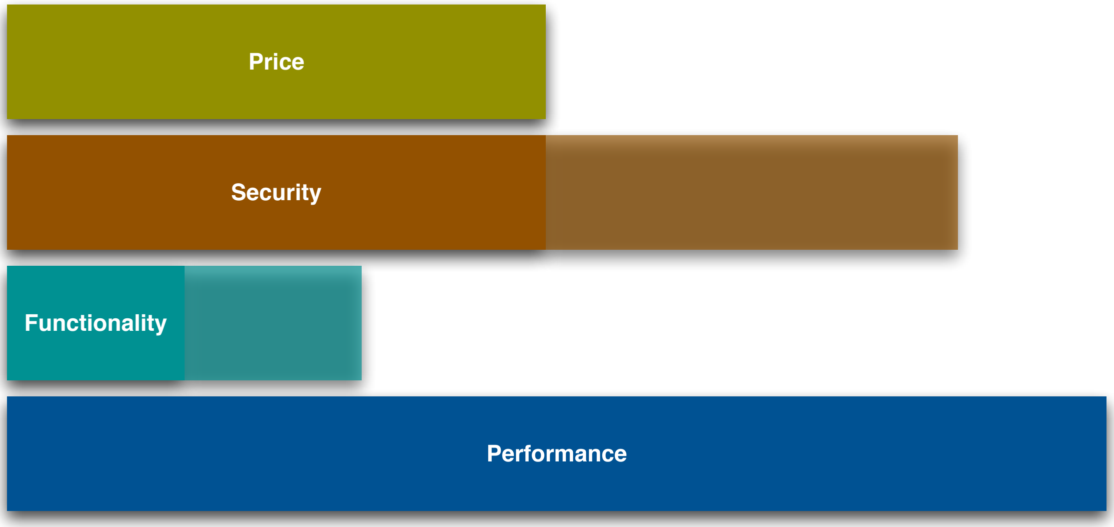
MACSec as integrated solution



1.2. MACSec as Dedicated Appliance

The result would be different if MACSec were to be implemented in a dedicated appliance, although it doesn't make much sense to use a dedicated appliance for LANs. However, NSA developed a specification - ESS (Ethernet Security Specification) - for such a dedicated and secure appliance that additionally includes traffic flow security. Despite the limited functionality such an appliance has a cost profile that approaches the one of a specialized and fully featured appliance.

MACSec as dedicated appliance



While the security is much improved compared to an integrated solution, primarily due to encryption in an FPGA, a secure key generation, a secure key storage and the traffic flow security, there remains a dependency on the security of the key server. ESS deviates from the published MACSec specifications by supporting different encryption offsets. While this support increases the functionality, it also reduces the interoperability with standard MACSec devices. The key system remains limited to point-to-point and point-to-multipoint. There also shouldn't be a MACSec capable network device located between two ESS devices.

1.3. Virtual Appliance

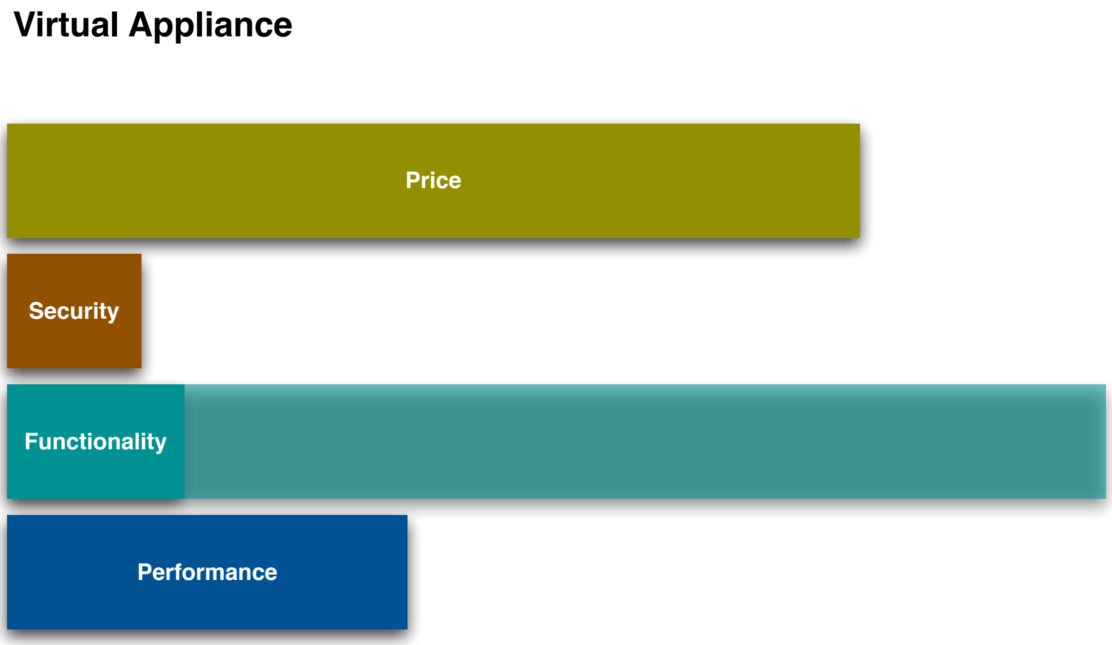
Another approach that promises lower cost is virtualization: The encryptor as a virtual appliance in a virtualized environment: A reincarnation in the world of network function virtualization (NFV). What looks promising at first sight starts losing its appeal at second sight. Key security remains an unresolved issue, both, in terms of key generation and in terms of key storage. While the functionality of a virtual appliance might be high, latency and jitter might have a negative effect of network and application performance, especially at higher speeds.

Theoretically any encryptor that is based on a x86-CPU can also run on a virtual x86-CPU as an application on a virtual machine (VM). There are fundamental differences, though, between a real and a virtual appliance that need to be considered. The virtual appliance has no physical device protection, no hardware entropy source for the generation of true random numbers and no tamper-proof key storage. The lack of physical device protection must be compensated for by an equivalent protection of the server, while the hardware needed for key generation and key storage can be provided through a local smart card or a network-based hardware security module (HSM). The local smart card is connected to the host through a USB interface, so that the virtual appliance running on the host can use it. In this manner, the required security and the needed protection are available when using a virtual appliance, but only if the corresponding hardware is real and not just virtual.

The performance of the virtual appliance is determined by a range of factors, including the hardware characteristics of the host system, the performance of the hypervisor, the number of other virtual machines running on the host, and the CPU, memory and I/O use by the other virtual machines. Virtualization splits real hardware resources and only makes them available to one single virtual machine at any given time. Running multiple real-time services concurrently on multiple virtual machines on a single host obviously will have a negative impact on latency and jitter.
The security of the virtual appliance is dependent on multiple external factors: On one hand, the server hosting the virtual appliance must be protected from unauthorized access, while on the other hand the security risks created by the guest operating system, the hypervisor and the other virtual machines running on the host must be properly addressed.

The use of virtual encryptors is thus limited to specific scenarios. A typical example would be a virtual appliance on a host that runs virtualized firewalls next to the virtualized encryptor. The bandwidth that can be encrypted at line rate on current hardware is limited to 70-120 Mbits/sec. The applications used in the scenario should also support the increased latency and jitter compared to dedicated appliances, so that unwanted side effects are avoided.

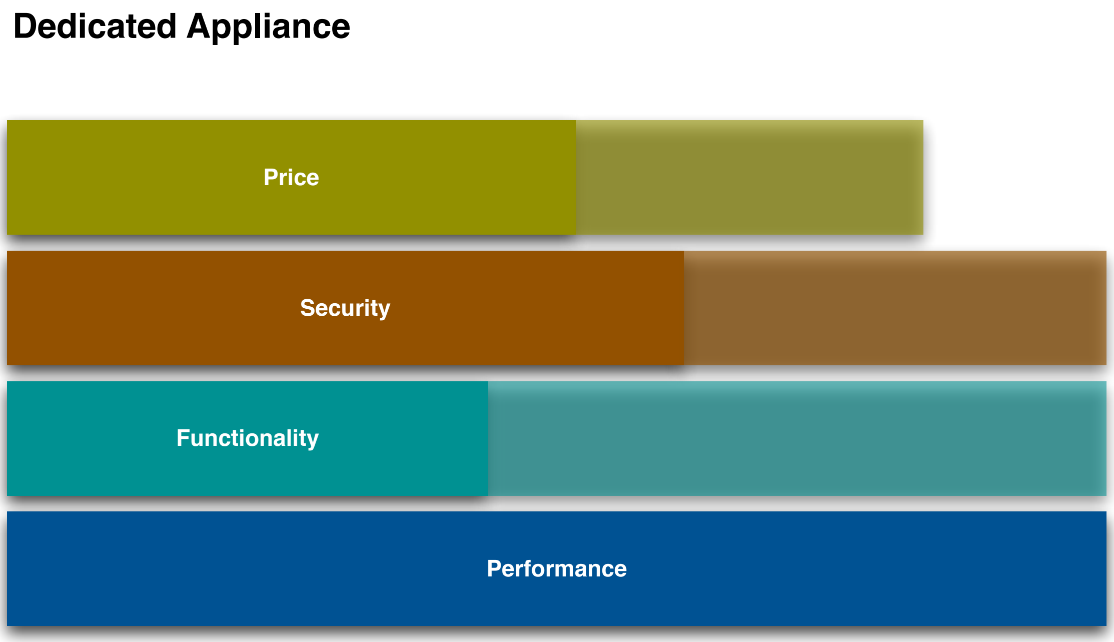
In terms of performance of virtual encryption appliances, it is important to understand that higher line rates mean higher latency and jitter. This is similar to software-based IPSec encryption implementations. The largest impact is felt by real-time services, such as IP telephony. That is where the comparison to IPSec ends, as virtual Ethernet encryptors can natively encrypt Ethernet and cryptographically separate VLANs.



White-box solutions for encryption appliances based on a dedicated x86-CPU do currently not exist. Due to the extensive hardware requirements for a secure encryption appliance and the interdependencies between hardware and software, such a white-box approach would most likely fail to produce a noticeable benefit in terms of cost savings.

1.4. Dedicated Appliance

A dedicated and specialized appliance has a different profile. The price is somewhat higher than a dedicated appliance based on MACSec. The performance is top and secure keys and a key management that supports multipoint-to-multipoint are standard. The main differences between the different offers are the supported encryption modes, traffic flow security and the key management. In terms of functionality, the biggest differences can be found in the network support provided and the capability to handle multi-tenancy.



2. Considerations

Cheap and secure are mutually exclusive. Functionality doesn't come for free either. If price and performance are the main criteria while security and functionality requirements are low, then MACSec-based integrated appliances are a low-cost option. Due to the limited functionality MACSec can lead to higher network cost, which are noticeable in OpEx, but not in CapEx.
High security combined with extensive functionality and high performance is only available with specialized encryptors. The use of such appliances can also be sourced as managed service. This allows forgoing CapEx and shifting cost to OpEx.

3. Evaluation

In order to be able to properly assess the different alternatives and offers, it is mandatory to know the own requirements concerning network and security. The following checklist might be of help to define the requirements and facilitate a target-oriented evaluation of the solutions available on the market.

Annex:

Checklist for the Evaluation of Encryptors for Metro and Carrier Ethernet

Version 1.01

Section 1: Network and Usage Scenario

1. Supported Network Topologies

What is the topology of the network to be secured?

Point-to-point (2 sites) □
Point-to-multipoint (multiple sites) □
Multipoint-to-multipoint (multiple sites) □

Will multiple topologies be layered? □

Are topology changes within the next five years likely? □

2. Number of Sites

How many sites will be connected with each other?

2 □
2-10 □
11-25 □
26-50 □
50+ □

3. Network – Ethernet Only or Mixed?

Is the network a closed Carrier Ethernet network or will there additionally be access to IP and MPLS at different sites?

Closed Carrier Ethernet-network □
Access to other networks (MPLS, IP) □

4. MTU

What is the size of the MTU supported by the carrier for Carrier Ethernet? .... bytes
What is the size of the MTU supported by the carrier for IP? .... bytes

5. Supported Usage Scenarios

Will the encryptors be self-managed and self-maintained or is part of the operations outsourced?

Self-managed □
Managed Encryption Service (single-tenancy) □
Managed Encryption Service (multi-tenancy) □
Managed Security Service (single-tenancy) □
Managed Security Service (multi-tenancy) □

5. Supported Networks

Ethernet □
MPLS over Ethernet (MPLSoE) □
Ethernet over IP (EoIP) □
MPLS over Ethernet over IP (MPLSoEoIP) □
IPv4 for EoIP □
IPv6 for EoIP □

6. Maximum Supported Bandwidth

100 Gb/sec full-duplex □
40 Gb/sec full-duplex □
10 Gb/sec full-duplex □
1 - 2 Gb/sec full-duplex □
100Mb/sec – 1 Gb/sec full-duplex □
10 - 100 Mb/sec full-duplex □

Increase of supported bandwidth via software licence □

Section 2: Communication Security

1. Security Requirements

Different security requirements can have an impact on the required functionality.

1.1. Low

No hardware-based true random number generator and no hardware-secured key store □
No authenticated encryption □
Integrated appliance □

1.2. Medium

Dedicated appliance □
Hardware-based true random number generator and secure key storage □
Authenticated Encryption □
Additional authentication per group □

1.3. High

Dedicated appliance □
Hardware-based true random number generator and secure key storage □
Authenticated encryption □
Additional authentication per group □
Support for frame and tunnel mode □
Traffic Flow Security (TFS) □
Emission protection □

2. Cryptosecurity

2.1. Key Generation

Hardware-based true random number generator □
Software-based pseudo random number generation □

2.2. Key Storage

Tamper-proof key storage □
Unsecured key storage □

2.3. Key Exchange

There are different ways to exchange keys. Each vendor can show the lifecycle of a key in detail. He won't do so normally though, unless asked specifically for it.

Asymmetric keys with symmetric encryption of the partial keys □
Asymmetric keys without symmetric encryption of the partial keys □
Authenticated key exchange □
Selection of curves for Elliptic Curve Cryptography □
Key exchange in-band □
Key exchange out-of-band □

2.4. Encryption Algorithm and Operating Mode

AES-GCM (authenticated encryption) □
AES (unauthenticated encryption) □
Other authenticated encryption algorithm □

2.5. Key Size

128 Bit (for low security requirements) □
256 Bit (for medium and high security requirements) □

2.6. Encryption Modes

Depending on security requirements and network support, different encryption modes come into play.

Frame mode (for direct links and for EoIP) □
Transport mode □
Tunnel mode (to hide the Ethernet meta-data)) □

2.7. Content of the SecTag

The SecTag contains additional information, such as a proprietary EtherType, a counter, a counter-offset or a security association. The shorter the counter the more often key changes have to take place.

Proprietary EtherType □
Size of counter □

2.8. Key Managment and Frame Content

Key Management can use the address information, the EtherType of the unencrypted frame and the additional data for its operation. Each key management works differently. Vendors will gladly tell how their implementation works and how things are tied together.

2.9. Operating Modes of the Key System

Depending on the usage scenario, pairwise key systems or group key systems are preferable. A good encryptor should provide both possibilities. In the case of group key systems it is important how groups are defined by default and how they can be defined.

Pairwise key system □
Group key system □

2.10. Key Assignment

Depending on network and topology, either a port-based or a VLAN-based key assignment is required.

Port-based □
VLAN-based □
Group-based □

2.11. Scaleability

Scalability not only depends on the number of sites to be interconnected, but also on the number of VLANs/groups. As each VLAN can be a group and should be authenticated individually, the number of certificates supported by an encryptor might be a more limiting factor than the number of sites that are interconnected.

< 50 Groups/VLANs □
> 50 Groups/VLANs □

2.12. Key Server

Key server can either be embedded within the encryption appliances or be dedicated or virtualized appliances themselves. Single dedicated key server appliances create a single point of failure. In lager networks, hybrid configurations consisting of at least two dedicated key server appliances and additional distributed embedded key servers tend to be the preferred solution.

Embedded key server □
Dedicated key server □
Hybrid combination of dedicated and embedded key servers □

3. Transmission Security, Emission Security and Physical Security

Without transmission security, traffic flow analysis will allow the analysis of the traffic flow, providing indications what happens and when on the network. For mission-critical site interconnects with high security requirements, traffic flow security is a very useful feature. Emission security is primarily of high importance if physical security does not properly secure the area with the encryptors and prevent the leak of electromagnetic emissions.

Traffic flow security □
Emission security □

Section 3: Network

For a network encryptor, network functionality is equal in importance to security functionality.

1.1. Encryption Offset

Ethernet frames can carry different content. Depending on the network, an encryptor should not automatically start encryption after the first VLAN-ID. Encryption offsets allow the encryptor to adapt to the network and prevent the encryption of parts that will later on be needed by the network.

Fixed user-selectable encryption offset □
Fixe user-selectable encryption offset per VLAN or group □
Automatic setting of the encryption offset depending on content □

1.2. Conditional Encryption

Depending on usage scenario and position of the encryptor in the network, not all frames should be encrypted. This exception can be based on VLAN-IDs, frames with a specific EtherType or frames with a MPLS tag

Exemption based on MAC-Adresse □
Exemption based on VLAN-ID □
Exemption based on EtherType □
Exemption based on group membership □
Exemption based on presence of MPLS tag □
Exemption based on a combination of criteria □

1.3. Latency and Jitter

Latency and jitter are not well-liked and depend to a large degree on the encryption hardware that is used. FPGA and ASIC process data faster than a CPU and thus have a lower latency. But only FPGA and CPU allow for an upgrade of the functionality without requiring a change of hardware. Virtual appliances have a tendency to create jitter at higher bandwidth.

FPGA & CPU □
ASIC & CPU □
CPU □

1.4. MTU

The behavior of an encryptor in terms of MTU concerns multiple aspects. One of them is the maximum frame size that is supported and another one is the behavior in the case of oversized frames.

Support for jumbo frames □
Fragmentation/defragmentation of oversized frames □

1.5. Ethernet Flow Control

Ethernet Flow Control is part of the standard functionality of a decent switch, especially the support of "pause". It allows to manage overly extensive data coming from a source.

Support of Ethernet Flow Control (Pause) □

1.6. Out-of-Sequence Handling

In theory, all frames in a network arrive in the sequence they were sent. In reality it happens from time to time, that the sequence is changed by a device the frames are passing through. This can create issues when authenticated encryption incorporating a counter is being used. Therefore an encryptor should have a function to establish a certain tolerance for re-ordered frames. Such a tolerance is predominantly defined in a number of frames. A different approach is to define the tolerance in time, such as a number of seconds.

Handling of out-of-sequence frames □

Section 4: Operation

1. Configuration

The different vendors handle configuration and configuration changes differently. Without asking questions you will miss out on important info. One aspect that often is often lost is the effort needed for the periodical change of the initial secrets and of passwords.

2. User Management

The granularity of the user management is a critical factor for security.

Role-based access □
Identity-based authentication of the user □
Number of hierarchy levels □
Number of roles □
Strict internal separation of users □
Separate role for security officer □

3. Device Management

For device management there is a difference between configuration and monitoring. It is however of equal importance for both scenarios that the encryptor features secure versions of the protocols used. E.g. SNMPv3 instead of the antiquated and insecure SNMPv1.

3.1. Out-of-Band-Management

An additional management port provided by the encryptor is required for out-of-band management.

Additional special management port □

3.2. In-Band-Management

If the administration takes place over the network, different networking and security technologies come into play. It is important not to limit the focus to the version of a technology, but to have a close look at its implementation.

SSH □
SNMPv3 □
TLS □
Proprietary protocols and solutions □

4. Monitoring and Behavior in Case of Link or Peer Loss

Encryptors can be monitored using SNMP. If a link loss occurs or if a peer dies, the encryptor must pass on this information.

4.1. Monitoring

Using SNMP and appropriate network software that is normally provided with the device, operations can be monitored live

Remote Monitoring □

4.2. Link Loss Forward

Link loss forwarding depends on the type of link used. There are different technologies for optical links and for electrical links.

Optical loss pass-through (only for optical links) □
Link loss carry forward (for electrical connections) □

4.3. Dead Peer Detection

If a peer dies, then this fact should be detected and communicated.

Dead Peer Detection □

5. Logs

Encryptors support a variety of logs for different purposes: Syslog for integration with Syslog servers, an event log for local analysis and an audit log for the auditors.

Syslog support □
Event log (local) □
Audit log (local) □

Section 5: Certifications and Cost

1. Certifications

Most of the certifications provide as much security and network functionality as the paper they are printed on. Included in that group are FIPS, and to a large degree also Common Criteria. Currently by far the greatest credibility for security is offered by a BSI certification. When in doubt, it is a safe bet to put substantially more trust into a BSI certification than in a Common Criteria certification or even a FIPS certification.

2. Cost

If a usage period of five years is planned, then also the cost should be calculated for such period. The best way to compare cost is comparing monthly cost, which then also can be seen in relation to the network cost. Different warranty periods and different support contracts make any comparison based on initial cost nearly useless. If encryption or security is provided by a service provider, then the cost will also be shown on a monthly or quarterly basis.