inside-it.ch

PRÄSENTIERT:

LAYER 2-VERSCHLÜSSLER FÜR CARRIER ETHERNET WANS UND MANS

MARKTÜBERSICHT

ETHERNET-VERSCHLÜSSER FÜR CARRIER ETHERNET, MPLS UND IP-NETZWERKE

Version 6.1 (Kurzfassung), 8. Juni 2017

www.uebermeister.com
cjaggi@uebermeister.com

INHALTSVERZEICHNIS

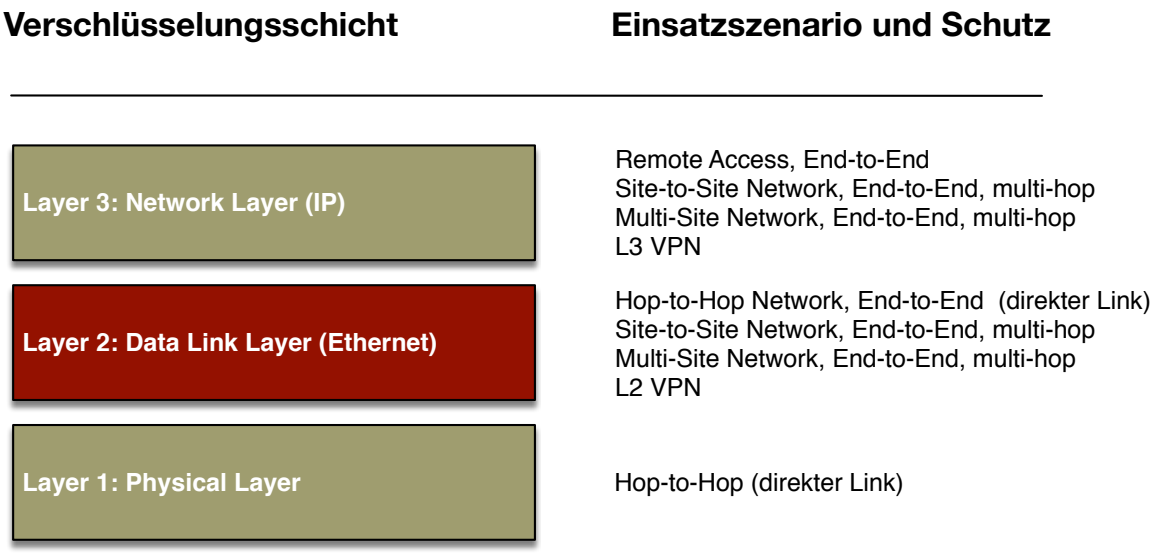
KAPITEL 1: EINLEITUNG

KAPITEL 2: MARKTÜBERSICHT

Kapitel 1: Einleitung

1. Verschlüsselungsschicht und Sicherheit

Ethernet spielt in der Verbindung von Standorten eine immer wichtigere Rolle. Sowohl bei Nahverkehrsnetzen (Metropolitan Area Networks/MAN) wie bei Weitverkehrsnetzen (Wide Area Networks/WAN). Ethernet befindet sich auf Layer 2 des OSI-Netzwerkmodells. Dies ist eine Schicht unterhalb des Internetprotokolls, das auf Layer 3 angesiedelt ist.



Netzwerkverschlüsselung bringt dann die grösste Effizienz und Sicherheit, wenn sie entweder nativ auf oder unterhalb des verwendeten Layers erfolgt. Bei Verschlüsselung unterhalb des verwendeten Layers kann es zu Abstrichen in Bezug auf Flexibilität kommen.

Die stark steigende Nachfrage nach dedizierten Layer 2-Verschlüsslern hat einen einfachen Grund: Sicherheit und Effizienz gepaart mit Kosteneinsparungen. Über 99 Prozent der Angriffe auf Netzwerke erfolgen auf Layer 3 bis 7. Die Verschlüsselung des standortübergreifenden Datenverkehrs auf Layer 2 gewährt – bei Verwendung von authentisierter Verschlüsselung - einen Vollschutz für das Netzwerk, inklusive Vertraulichkeit, Intrusion Detection, Intrusion Prevention und Firewall. Deshalb gibt es immer mehr Kunden für solche Lösungen, darunter auch solche mit über 500 Layer 2-Verschlüsslern im 24/7/365-Einsatz.

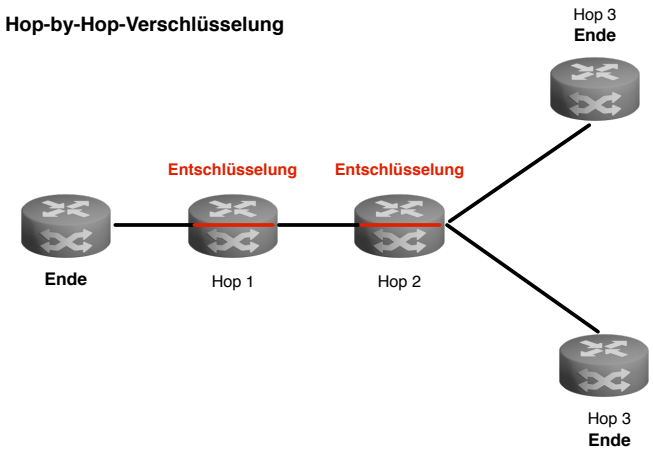
2. Unterschiedliche Ansätze

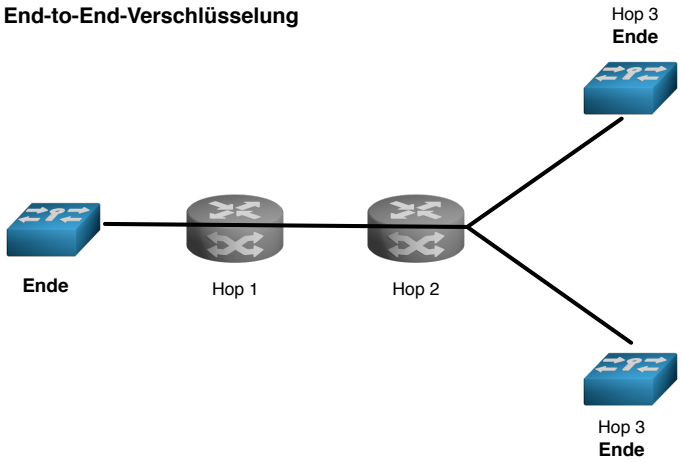
Für Netzwerkverschlüsselung gibt es unterschiedliche Ansätze und Vorgehensweisen. Diese haben eine direkte Auswirkung auf die unterstützten Anwendungsszenarios und auf die Sicherheit.
So gibt es auch unterschiedliche Möglichkeiten, Ethernet zu verschlüsseln. Das geht sowohl auf Layer 1, auf Layer 2, als auch auf Layer 3 oder höher. Am effizientesten ist es auf Layer 1 und auf Layer 2, am flexibelsten auf Layer 2 und Layer 3. Die optimale Kombination von Effizienz und Flexibilität bietet die Verschlüsselung auf Layer 2. Aber auch da gibt es Unterschiede.

2.1. Hop-by-Hop vs. End-to-End

Für die Verbindung von Standorten wird vorzugsweise eine End-to-End-Verschlüsselung verwendet. Eine Hop-by-Hop-Verschlüsselung funktioniert nur in einer beschränkten Anzahl von Szenarien.

Bei einer Hop-by-Hop-Verschlüsselung werden die Daten bei jedem Hop entschlüsselt, in unverschlüsselter Form verarbeitet und dann wiederum verschlüsselt zum nächsten Hop weitergesendet. Anders sieht es bei einer End-to-End-Verschlüsselung aus, bei der die Daten während der gesamten Übertragung zwischen Absender und Ziel gesichert bleiben.





Während in einem lokalen Netzwerk eine Hop-by-Hop-Verschlüsselung vorteilhaft sein kann, ist sie für MAN- und WAN-Umgebungen nur dann einsetzbar, wenn der nächste Hop gleichzeitig auch das andere Verbindungsende ist. Der Einsatzbereich und die Flexibilität von Hop-by-Hop-Verschlüsselungslösungen sind stark eingeschränkt.

2.2. Dediziert vs. Integriert

Dedizierte Geräte lassen sich besser für einen Aufgabenbereich optimieren und absichern. Integrierte Lösungen sind dafür in der Regel günstiger. Bei der Ethernet-Verschlüsselung bauen die integrierten Lösungen auf MACSec, während dedizierte Geräte in der Regel eine für MAN und WAN optimierte Verschlüsselung verwenden. Das Anforderungsprofil für eine MAN- und WAN-Verschlüsselung unterscheidet sich deutlich von der einer LAN-Verschlüsselung, sowohl in Bezug auf die Netzwerkunterstützung wie auch die Sicherheitsanforderungen. Zielgerichtet für den Schutz von Carrier Ethernet-Netzwerken entwickelte dedizierte Lösungen sind in der Regel besser geeignet als MACSec-basierte integrierte Lösungen, da sie von vornherein für die erhöhten Netzwerk- und Sicherheitsanforderungen von MANs und WANs ausgelegt wurden. Mittlerweile gibt es auch die ersten dedizierten Geräte, die auf Basis von MACSec arbeiten. Sie verwenden allerdings die von NSA und IEEE entwickelten IEEE 802.1AEcg-Spezifikationen und FPGAs statt ASICs. Diese Geräte kommen mit mehr Carrier Ethernet-Szenarien klar, liegen aber in Bezug auf Netzwerkunterstützung, Sicherheit und Skalierbarkeit immer noch deutlich hinter den meisten zweckoptimierten Geräten zurück.

Sicherheitslösungen für WANs sollten sowohl von der Funktionalität wie auch von der gewährten Sicherheit her auf die spezifischen Problemstellungen und Gefahrenszenarios von WAN und MAN optimiert sein.

3.Kriterien und Abdeckungsbereich

3.1. Kriterien

Die Gliederung der Marktübersicht orientiert sich an den relevanten Hauptkriterien für eine Vorauswahl:

- Schnittstelle/Verarbeitungsleistung
- Unterstützte Netzwerke und Einsatzszenarien
- Verwendete Plattform (Hardware, Firmware, Schlüsselverwaltung)
- Verschlüsselungsstandards und –verarbeitung
- Verschlüsselungs- und Sicherheitsfunktionen auf der Datenebene
- Verschlüsselungs- und Sicherheitsfunktionen auf der Kontrollebene
- Schlüsselverwaltung und Schlüsselsystem
- Netzwerkfunktionalität und Zusatzfunktionen
- Geräteverwaltung
- Zertifizierungen
- Geräteeigenschaften

Die unterschiedlichen Kriterien und Implementierungsansätze sind erläutert und - wo möglich - mit Links auf neutrale externe Informationsquellen versehen.

Bei der Netzwerkverschlüsselung haben unterschiedliche Kunden oft unterschiedliche Anforderungsprofile. Dies betrifft sowohl die Eigenschaften und das Nutzungsszenario des verwendeten Nah- und Weitverkehrsnetzes als auch die gestellten Sicherheitsanforderungen. Es gibt verschiedene Lösungsansätze, um den jeweiligen Erfordernissen gerecht zu werden.

Für End-to-End-Verschlüsselung von Ethernet-Netzwerken gibt es keinen offiziellen Standard. Die verschiedenen Anbieter verwenden sowohl auf der Kontroll- wie auch auf der Datenebene unterschiedliche Ansätze. Das führt dazu, dass das Marktangebot ziemlich unübersichtlich ist. Diese Marktübersicht versucht, die verschiedenen Lösungsansätze aufzuzeigen und einigermassen vergleichbar zu machen.

3.2. Abdeckung

Für die Marktübersicht standen für alle wichtigen, aber nicht für alle Anbieter von Lösungen die nötigen Details zur Verfügung. Deshalb sind zwar nicht alle Anbieter von Lösungen vertreten, aber trotzdem sämtliche marktrelevanten Angebote aufgeführt. Entscheidend für die Marktrelevanz sind fünf Faktoren: Die Akzeptanz im Markt, die installierte Basis, die laufenden Verkäufe, der technische Stand der Produkte und die Angebotsbreite.

So sind in dieser Marktübersicht keine Anbieter vertreten, bei deren Produkten essentielle Sicherheitsfunktionen wie authentisierte Verschlüsselung fehlen, die Verschlüsselung nicht nativ auf Layer 2 erfolgen kann oder das Angebot die gängigsten Bandbreitenszenarios – von 100Mb bis 10Gb – nicht abdecken kann. Ebenfalls nicht berücksichtigt sind Carrier-Geräte, bei denen die Verschlüsselung erst nach Übergabe des unverschlüsselten Netzwerkverkehrs an den Carrier erfolgt. Darunter fallen unter anderem Ethernet Access Devices.
In Bezug auf MACSec ist die Auswahl auf IEEE 802.1AEcg-Geräte beschränkt, da dieser Standard im Gegensatz zu integrierten Lösungen gleich wie die Ethernet Security Specifications (ESS) der NSA auf kundenseitige Appliances setzt. IEEE 802.1AEcg weicht von IEEE 802.1AE MACSec in etlichen Bereichen ab und definiert fünf unterschiedliche Geräteklassen. Im Gegensatz zu integrierten MACSec-Lösungen sind in einer Appliance die Funktionen dediziert und klar abgrenzbar.

3.3. Zielsetzung

Diese Marktübersicht soll das aktuelle und geplante Marktangebot an Appliances aus Herstellersicht in Bezug auf die gebotene Funktionalität widerspiegeln. Dazu zeigt sie verschiedene Ansätze und Möglichkeiten auf, wie man ein Carrier Ethernet-MAN oder -WAN absichern kann. Die Funktionalitätsanforderungen werden durch das Einsatzszenario des Anwenders bestimmt. Produktfunktionalität und gebotene Sicherheit bilden zusammen mit den Anschaffungs- und Betriebskosten die wichtigsten Evaluationskriterien. Die getroffene Wahl hat Auswirkungen auf die Sicherheit, die Kompatibilität, die Effizienz, die Flexibilität und die Folgekosten.

Diese Marktübersicht macht keine Empfehlungen in Bezug auf Anbieter und Plattformen. Sie bietet hingegen die Informationen, welche für das Anlegen einer Shortlist für eine Evaluation benötigt werden.

Die Markübersicht ist eines von drei Dokumenten und steht in einer Reihe mit einer Einführung in die Grundlagen der Verschlüsselung von Metro und Carrier Ethernet-Netzwerken und einer Evaluationshilfe:

http://www.uebermeister.com/files/inside-it/2016_Einführung_Verschlüsselung_Metro_und_Carrier_Ethernet.pdf

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

Kapitel 2: Marktübersicht

1. Anbieter und Produkte

Diese Übersicht umfasst sämtliche marktrelevanten Anbieter von autonomen Layer 2-Verschlüsslungsgeräten, die mit ihrem Produktangebot mindestens den Bandbreitenbereich von 100Mb/sec bis 10Gb/sec abdecken. Zusätzlich muss das Produktangebot den aktuellen Sicherheitsstandards entsprechen, was Geräte ohne authentisierte Verschlüsselung und ohne "Perfect Forward Secrecy (PFS)" ausschliesst. Auch die Verfügbarkeit für kommerzielle Kunden ist eine Voraussetzung. Fast alle Geräte verfügen über eine Zertifizierung oder eine Zulassung für den behördlichen und militärischen Einsatz zur Absicherung von Netzwerken mit klassifizierten Daten. Sie gehören aber zur Klasse der "Commercial Off-the-Shelf (COTS)" Systeme, die sowohl im staatlichen wie auch im kommerziellen Sektor eingesetzt werden können.
Die Beschränkung auf autonome Geräte erfolgt aufgrund der deutlich besseren Sicherheit, der konsistenteren Verarbeitungsgeschwindigkeit und der Herstellerunabhängigkeit in Bezug auf Switches und Routers. Zudem gibt es zum heutigen Zeitpunkt keinen Hersteller, der eine skalierbare integrierte Ethernet-Multipunkt-Verschlüsselung für Multi-Hop-Netzwerke anbietet.

Nachfolgend die Liste der Anbieter in alphabetischer Reihenfolge:

atmedia
(http://www.atmedia.de)

Gemalto
(https://safenet.gemalto.com/data-encryption/network-encryption)

IDQuantique,
(http://www.idquantique.com)

Rohde & Schwarz Cybersecurity
(https://cybersecurity.rohde-schwarz.com/de/produkte/sichere-netzwerke/rsrsitline-eth-ethernet-verschluesselung)

Secunet
(http://www.secunet.com/de/themen-loesungen/hochsicherheit/sina/sina-l2-box/)

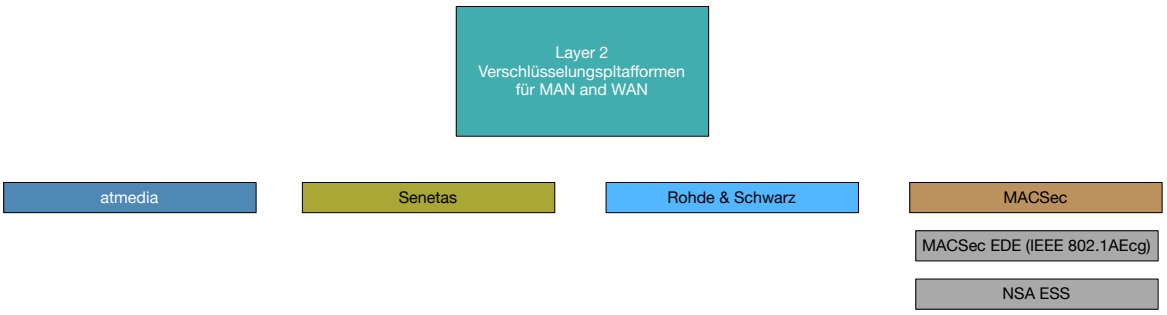
Securosys
(https://www.securosys.ch/layer-2-encryptor-centurion)

Senetas
(http://www.senetas.com)

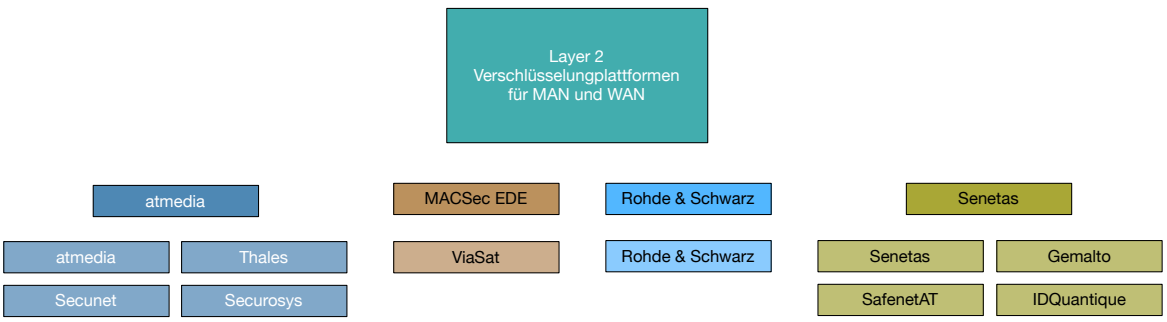
Thales
(https://www.thales-esecurity.com/products-and-services/products-and-services/network-encryption-appliances/datacryptor-5000-series)

ViaSat
(https://www.viasat.com/products/data-in-transit-encryption-for-enterprises)

Die Angebote basieren jeweils auf einer der etablierten Plattformen:



Auf Anbieter und Plattform aufgeschlüsselt ergibt das folgendes Bild:



Der gemeinsame Nenner der Produkte beschränkt sich vorwiegend auf die Tatsache, dass alle Carrier Ethernet-Netzwerke nativ und authentisiert verschlüsseln können. Bis auf die Verwendung von AES-GCM tun das alle Plattformen unterschiedlich und auch die Netzwerkunterstützung ist stark plattformabhängig. Nicht nur die Sicherheitsanforderungen, sondern auch die Netzwerke entwickeln sich wegen neuen Technologien, sich ändernder Kundenanforderungen und neuen Carrier-Angeboten laufend weiter. FPGA- und CPU-

basierte Verschlüssler können per Firmware- resp. Software-Update an neue Sicherheits- und Netzwerkanforderungen angepasst werden. Je grösser die Flexibilität eines Verschlüsslers desto höher ist die Zahl der unterstützten Einsatzszenarios.

Nachstehend eine detaillierte Aufschlüsselung der verschiedenen Angebote. Sie gibt Einblick in die wichtigsten technischen Eigenschaften und Funktionalitäten der Produkte.

2. Netzwerkstandards und Plattformen

2.1. Ethernet-Schnittstelle und Durchsatzrate

Der vom Produkt unterstützte Ethernet-Netzwerkstandard bestimmt den theoretischen Datendurchsatz des Verschlüsslers. Für Ethernet sind das die IEEE 802.3-Standards 10Mb/s Ethernet, 100Mb/s Ethernet, 1Gb/s Ethernet, 10Gb/s Ethernet, 25Gb/s Ethernet, 40Gb/s Ethernet, 50 Gb/s Ethernet und 100Gb/s Ethernet. Nebst diesen gibt es noch Standards für 2.5Gb/s und 5Gb/s und es wird künftig auch IEEE-Standards für höhere Bandbreiten geben.

Von der unterstützen Bandbreite zu unterscheiden ist die Netzwerkschnittstelle. Diese kann elektrisch (RJ-45) oder optisch (SFP, SFP+, XFP, QSFP) sein.

https://de.wikipedia.org/wiki/RJ-Steckverbindung
https://de.wikipedia.org/wiki/Small_Form-factor_Pluggable
https://en.wikipedia.org/wiki/XFP_transceiver
https://de.wikipedia.org/wiki/Small_Form-factor_Pluggable#QSFP

Die unterstützte Bandbreite ist neben der Schnittstelle auch von der Softwarelizenz abhängig. So kann ein 100M-Verschlüssler mit einem 1G-Verschlüssler identisch, aber aufgrund der Softwarelizenz auf 100Mb/s beschränkt sein. Auch 10G, 40G und 100G-Verschlüssler können in der Bandbreitenunterstützung softwaremässig beschränkt werden. Einige der Verschlüssler – vorwiegend 40G- und 100G-Geräte – verfügen über mehrere Ports, die einzeln oder zusammengefasst verschlüsselt werden können.

Entscheidend für den effektiven Datendurchsatz sind nicht allein die Netzwerkschnittstelle und die unterstützte Bandbreite, sondern auch die Effizienz des Frame Forwarding, der Paketoverhead und die Verarbeitungsleistung des Verschlüsslers. Letztere wird durch Parameter wie Verschlüsselungsstandard, Verschlüsselungshardware, Verschlüsselungsmodus und Betriebsmodus beeinflusst.

Layer 2-Verschlüssler gibt es auch als virtuelle Appliances. Bei diesen hängt die gewährte Sicherheit und Leistungsfähigkeit von der Laufzeitumgebung ab. Die Eigenschaften der verfügbaren Hardware sind entscheidend. Ohne dedizierte und optimierte Hardware bleibt zwar ein Grossteil der Funktionalität vorhanden, doch werden nicht mehr alle wichtigen Funktionen direkt hardwaremässig unterstützt. Dies führt zu Einbussen in Bezug auf Sicherheit und Leistungsfähigkeit. Es gibt nur wenige Fälle, in denen die Verwendung einer virtuellen Appliance Sinn macht. Das sind meist diejenigen, bei denen es nicht anders geht. Es muss dann aber auch darauf geachtet werden, dass stets genügend Verarbeitungskapazität für die Verschlüsselung zur Verfügung steht und für Zufallszahlenerzeugung und Schlüsselspeicher die benötigte Hardware zur Verfügung steht. Theoretisch lässt

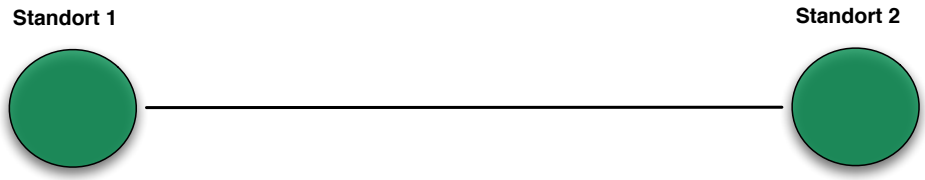
sich mit einer virtuellen Appliance zwar selbst eine 100G-Verbindung absichern, die von einer spezialisierten Appliance gewährte Sicherheit und Kosteneffizienz wird allerdings nicht erreicht.

2.2. Unterstützte Netzwerktopologien

Das Schlüsselsystem und die zur Verfügung stehende Verschlüsselungsmodi bestimmen die Verwendbarkeit für die unterschiedlichen Netzwerktopologien und Carrier Ethernet Standards.

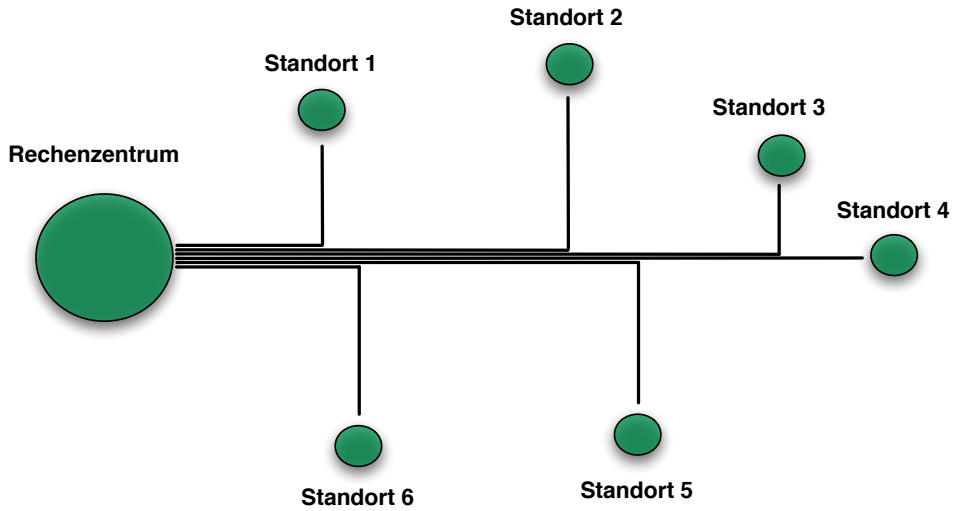
2.2.1. Punkt-zu-Punkt

Bei einer Punkt-zu-Punkt-Verbindung sind nur zwei Standorte involviert.



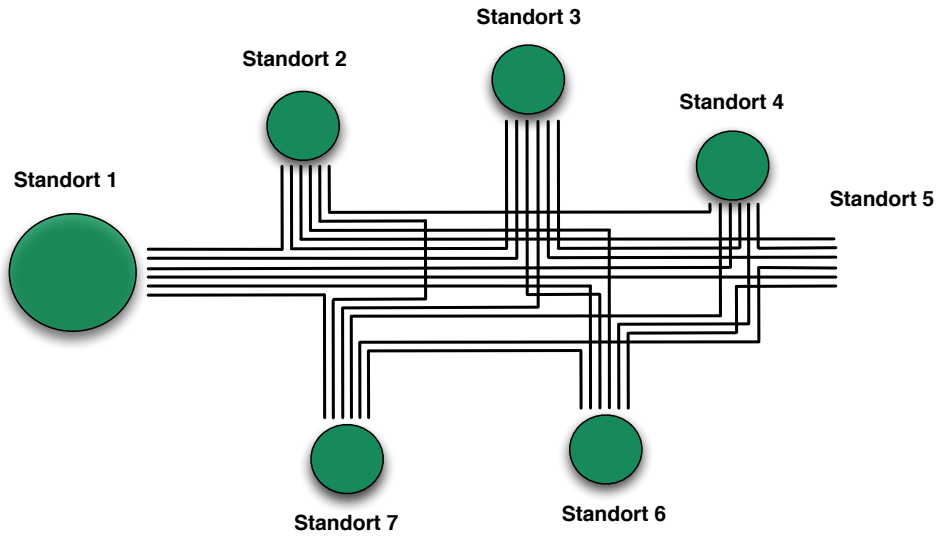
2.2.2 Punkt-zu-Multipunkt

Bei einer Punkt-zu-Multipunkt-Topologie sind mehrere Standorte mit einem zentralen Standort verbunden.



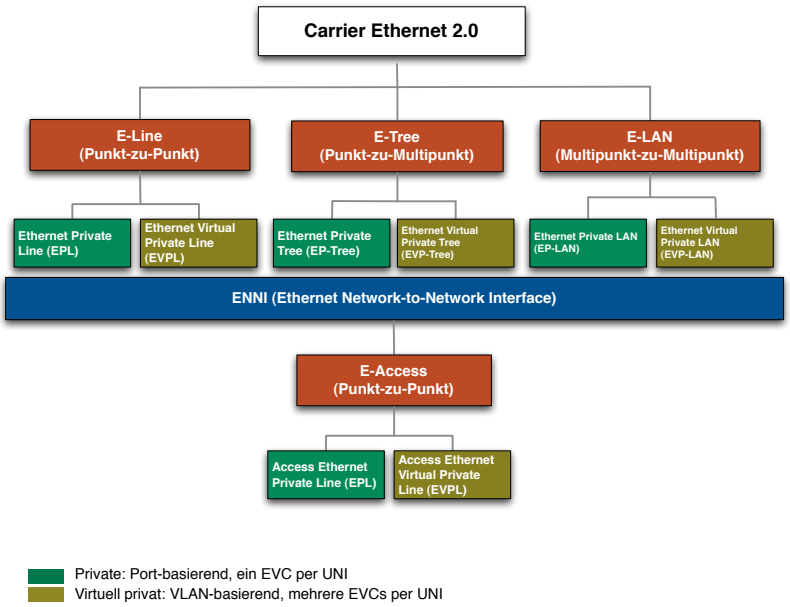
2.2.3. Multipunkt-zu-Multipunkt

Bei einer Multipunk-zu-Multipunkt-Topologie sind mehrere Standorte untereinander verbunden.



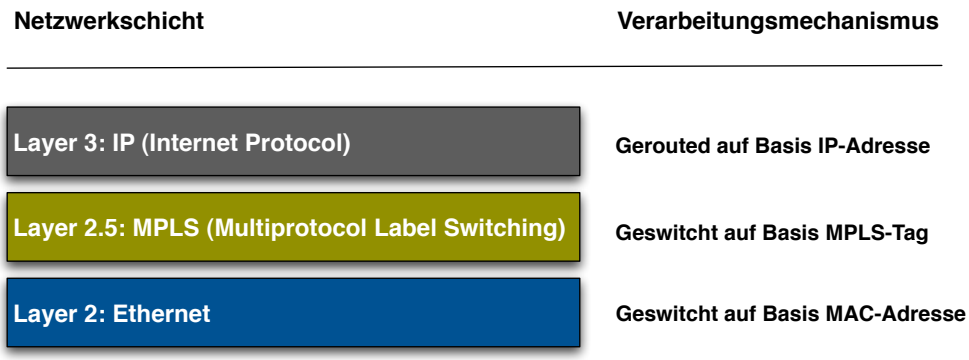
2.3. Unterstützte Metro und Carrier Ethernet Topologien

Die direkte Unterstützung unterschiedlicher MEF-Topologien hängt vom verwendeten Verschlüsselungsmodus und vom Schlüsselsystem ab.



2.4. Unterstützte Netzwerke für die Verschlüsselung

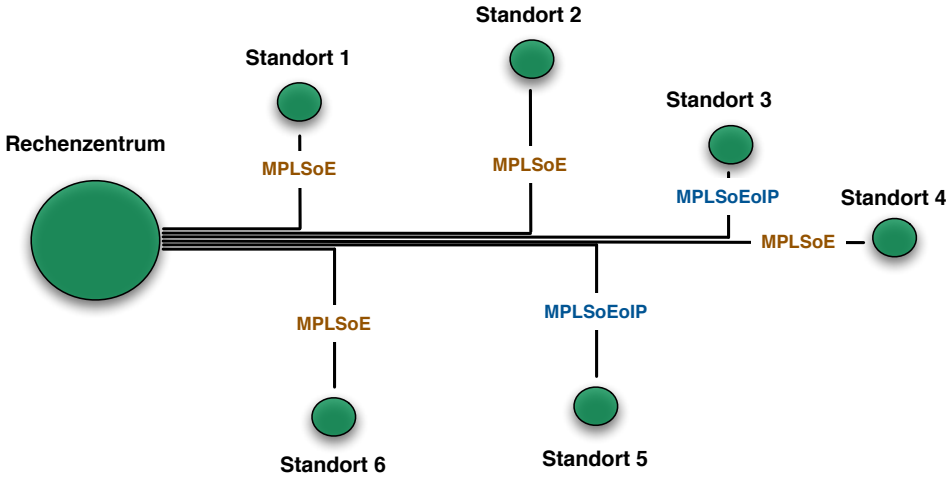
Carrier Ethernet kann man als Layer 2 VPN sehen, als Netzwerkdienst für MPLS und IP-Netzwerke und als Verbindung zum Internet. Und als Kombination der vorgenannten. Die meisten Angebote legen ihren Fokus auf die Unterstützung von Ethernet und Layer 2 VPNs. Jedes der Netzwerke – Ethernet, MPLS, IP – hat seine eigenen Anforderungen und Eigenschaften. Da diese Netzwerke jeweils voll unterstützt und abgesichert werden müssen, kommen bei MPLS- und IP-Netzwerken meist Layer 3-Verschlüsslern zum Einsatz. Es gibt wenige Angebote, die alle Netzwerke von Layer 2 bis Layer 3 voll unterstützen und absichern, da sich die Netzwerke doch stark unterscheiden.
Für die Absicherungen von MPLS-Netzwerken ist in den meisten Fällen eine Auslieferung auf Layer 3 (IP) nötig. MPLS befindet sich auf Layer 2.5 und lässt sich sowohl auf Layer 2 (bei Verwendung von MPLSoE) wie auch auf Layer 3 (bei Verwendung von MPLSoIP) verschlüsseln. MPLS wird auf Basis des MPLS-Tags geswitcht und die Absender-Adresse des Ethernet-Frames ändert sich bei jedem MPLS-Switch. Das Schlüsselsystem darf deshalb nicht von der Absenderadresse des Ethernet-Frames abhängig sein. Für die IP-Verschlüsselung auf Layer 3 braucht es eine vollständige Layer 3-Infrastrukturunterstützung für IPv4 und IPv6 im Verschlüssler.
In der Praxis die gleichzeitige Absicherung gemischter Umgebungen durch einen einzigen Verschlüssler erst wenig verbreitet. Oft wird jeweils ein anderer Verschlüssler für Layer 2 und für Layer 3 verwendet.



2.5. Unterstützte Netzwerke für den Transport von verschlüsselten Frames

Es gibt etliche Ethernet-Verschlüssler, die zwar als Ethernet-Verschlüssler vermarktet werden, aber eigentlich nur Ethernet verschlüsseln und es über ein IP-Netzwerk transportieren können (EoIP). Das ist nur dann sinnvoll, wenn kein natives Ethernet für den Ethernet-Transport zur Verfügung steht oder wenn die Verbindung zu einem inneren Netzwerk führt, das hinter einer Firewall steckt. Bei mehreren nativen Ethernet-Verschlüsslern gibt es EoIP als Zusatzfunktion, es ist aber nicht die Hauptfunktion.

Manchmal kommt es vor, dass zum Transport nur ein MPLS-Netzwerk zur Verfügung steht. In diesem Fall wird der verschlüsselte Ethernet-Frame über MPLS geführt (EoMPLS). Da der verschlüsselte Ethernet-Frame als MPLS-Nutzlast geführt wird, ist dies für einen nativen Ethernet-Verschlüssler und für MPLS ohne weiteres Zutun transparent. Komplexer wird es, wenn es darum geht, ein MPLS-Netzwerk zu verschlüsseln, bei denen es Standorte mit Layer 2-Anbindung und Standorte mit Layer 3-Anbindung gibt.

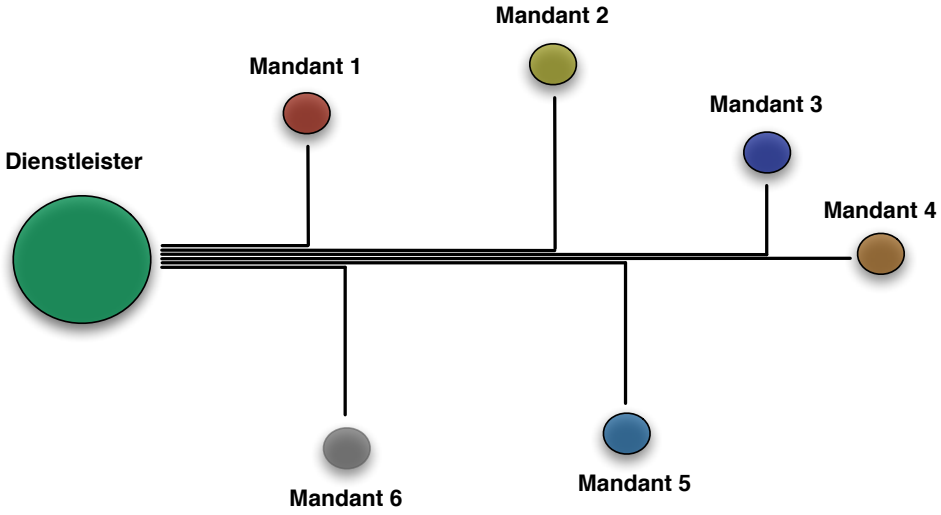


Getunnelt kann ein Ethernet-Netzwerk über eine grosse Zahl von Netzwerken, auch Netzwerke auf höherer Ebene, transportiert werden.

Bei IP-Verschlüsselung erfolgt diese nativ. Da es keine Abhängigkeiten von Layer 2/Ethernet gibt, stehen sämtliche Transportnetzwerke, die IP unterstützen, zur Verfügung.

2.6. Betriebsszenarien

Verschlüssler können eigenständig oder für Kunden betrieben werden. Für letzteres ist eine Mandantenfähigkeit gefordert, welche durch die Verwaltungssoftware unterstützt sein muss. Diese kann sowohl Managed Encryption Services wie auch Managed Security Services ermöglichen. Ein weiteres Szenario ist die Anbindung mehrerer unterschiedlicher Kunden. Dies bedingt eine Mehrmandantenfähigkeit, welche sowohl durch die Verwaltungssoftware als auch durch die Schlüsselverwaltung unterstützt sein muss.



Bei zertifikatsbasierten Authentisierungslösungen für mehrmandantenfähige Systeme braucht es Vertrauen zwischen der CA des Dienstleisters und den CAs der Mandanten. Dies schränkt die Mehrmandantenfähigkeit ein.
Deutlich einfacher geht das, wenn die Authentisierung über Pre-Shared Secrets erfolgt. Jeder Mandant einzeln kann mit dem Dienstleister eines oder mehrere Pre-Shared Secrets teilen und durch Ändern seines Pre-Shared Secrets jederzeit eine künftige Authentisierung verunmöglichen.

2.7. Verwendete Plattformen

Es gibt mehr Anbieter als Plattformentwickler. Nur drei der Anbieter entwickeln ihre Plattform komplett selbst: Atmedia, Rohde & Schwarz und Senetas. Alle anderen Angebote nutzen eine der vier marktrelevanten Plattformen: Atmedia, IEEE 802.1AEcg/NSA ESS, Rohde & Schwarz und Senetas.
Bei IEEE 801.2AEcg handelt es sich um eine IEEE-Plattform, die auf MACSec aufbaut und sich bei den Ethernet Security Specifications der NSA bedient. Die Plattform hat erst wenige Anhänger auf Anbieter- und Kundenseite gefunden, was angesichts der unnötigen Komplexität, der reduzierten Sicherheit und der Konkurrenz durch integrierte MACSec-Lösungen wenig erstaunt. Die anderen drei Plattformen wurden von vornherein auf die speziellen Anforderungen von Carrier Ethernet ausgelegt und optimiert. Angebote, die auf diesen Plattformen basieren, bilden auch die grosse Mehrheit der sich weltweit im Einsatz befindlichen Layer 2-Verschlüssler. Die Marktdurchdringungsrate liegt zurzeit bei über 90%. Nicht jedes Produkt, das auf der gleichen Plattform basiert, ist zwangläufig identisch. Einige Anbieter unterscheiden ihr Produkt nicht nur durch die Frontplatte, sondern integrieren zusätzlichen Code, um das Produkt zu differenzieren oder um Zertifizierungsvorgaben zu erfüllen. Bei den Zertifizierungen und Zulassungen ist zu beachten, dass eine

Zertifizierung oder Zulassung nicht für die Plattform, sondern nur für das Produkt erteilt wird. Selbst wenn der Plattformentwickler für seine eigenen Produkte eine Zertifizierung und Zulassung erhält, so gelten die nur für seine Produkte. Die Produkte anderer Anbieter können Zertifizierung und Zulassung selbst dann nicht einfach übernehmen, wenn sie die identische Version der Hardware und der Firmware verwenden.

2.8. Unterstützte Betriebsmodi

Layer 2-Verschlüssler sollten mindestens zwei unterschiedliche Betriebsmodi unterstützen: Punkt-zu-Punkt (Line Mode), und Multipunkt-zu-Multipunkt (Mesh). Diese Betriebsmodi sollten in allen Umgebungen voll und eigenständig unterstützt werden. Da Punkt-zu-Punkt ein Subset von Multipunkt ist, kann natürlich jeder Multipunkt-Verschlüssler auch im Multipunkt-Modus für Punkt-zu-Punkt eingesetzt werden. Es gibt Hersteller, die das als Punkt-zu-Punkt-Modus sehen.
Speziell im Multipunkt-Betrieb muss der Verschlüssler wissen, welche Frames er wie verschlüsseln soll. Dabei helfen ihm Parameter wie VLAN-ID, MPLS-Tag, MAC-Adresse, QoS etc. Die Herausforderung für die Hersteller liegt dabei darin, dass der Betrieb im sicheren Multipoint-Modus, sowohl das Software- wie auch das Hardware-Anforderungsprofil drastisch erhöht. Ein weiterer Problemkreis stellt die Verschlüsselung von Multicast- und Broadcast-Paketen dar, vor allem wenn primär ein paarweises Schlüsselsystem und kein Gruppenschlüsselsystem verwendet wird.

3. Verschlüsselung der Datenebene

3.1. Verschlüsselungsstandard

Alle auf dem Markt befindlichen Verschlüssler für den kommerziellen Markt, die bis in den Gigabit-Bereich verfügbar sind, verwenden AES mit einer Schlüssellänge bis zu 256 bit. Während bis vor sieben Jahren vorwiegend Cipher-Block-Chaining oder der nahe verwandten Cipher-Feedback-Modus verwendet wurden, hat sich in den letzten Jahren die Verwendung einer authentisierten Verschlüsselung mittels AES-GCM weitflächig durchgesetzt. GCM steht für Galois Counter Mode und bietet neben Authentisierung auch Integritäts- und Replayschutz. Dadurch wird nicht nur Vertraulichkeit gewährleistet, sondern auch Intrusion Detection, Intrusion Prevention und ein Layer 2-Firewall in die Verschlüsselung integriert.

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation
http://en.wikipedia.org/wiki/GCM_mode

Der früher oft verwendete CBC hat neben der fehlenden Authentisierung den Nachteil des Paddings, d.h. von zusätzlichem Overhead, der dann auftritt, wenn er nicht in Kombination mit Ciphertext-Stealing verwendet wird. Die korrekte Implementierung von Ciphertext-Stealing ist komplex, weshalb die meisten Hersteller, die CBC verwenden, auf die Implementierung von Ciphertext-Stealing verzichten.

http://en.wikipedia.org/wiki/Cipher_block_chaining
http://en.wikipedia.org/wiki/Ciphertext_stealing

Der verwendete Verschlüsselungsstandard hat einen direkten Einfluss auf das Frame-Format, den Frame-Overhead und die Sicherheit. Industrieweit hat sich wegen dem integrierten Replay- und Integritätsschutz AES-GCM als Standard durchgesetzt. Auch der IEEE-Standard für Hop-by-Hop-Ethernet-Verschlüsselung für LANs (MACSec) setzt auf AES-GCM. Dieser führt zu einem Frame-Overhead von 24-32 Bytes, was im Vergleich zur gewonnenen Sicherheit und zur Verschlüsselung mit IPSec auf Layer 3 (bis 73 Bytes) wenig ist. Bei Verwendung von optimierter Layer 3-Verschlüsselung kann der Overhead auf 46 Bytes verringert werden.

3.2. Verschlüsselungshardware

Es gibt unterschiedliche Ansätze einen Verschlüssler zu bauen, wobei der Ansatz eine direkte Auswirkung auf Kosten und Leistungsfähigkeit hat. Diejenigen Hersteller, welche die Verbindungen unabhängig von der Paketgrösse mit voller Leitungsgeschwindigkeit

verschlüsseln, haben alle eine jahrelange Erfahrung und ein Hardware-Design, bei dem die Verschlüsselung hochoptimiert in FPGAs erfolgt. Dies erhöht den Entwicklungsaufwand und die Produktionskosten, bietet aber mehr Flexibilität und bessere Performance. FPGA ist aber nicht gleich FPGA, denn Leistungsfähigkeit und Gatecount sind je nach Modell unterschiedlich und die Verschlüsselung ist nur eine der Aufgaben der FPGAs. Ein kostengünstigerer, aber weniger flexibler Ansatz ist die Verwendung von spezialisierten Sicherheitsprozessoren, welche die eigentliche Verschlüsselung übernehmen. Noch kostengünstiger, aber dafür flexibler ist das Verwenden von Software auf einer CPU, wo aber die Leistungsfähigkeit von der CPU abhängt und die Latenzzeiten erhöht sind.

3.3. Verarbeitungsweise

Grundsätzlich gibt es zwei unterschiedliche Verarbeitungsmethoden, die jeweils ihre Vor- und Nachteile haben: Cut-Through und Store & Forward. Bei der Cut-Through-Methode beginnt der Verschlüssler mit der Verschlüsselung bevor der ganze Frame eingelesen ist. Dies führt zu kürzeren Latenzzeiten, hat aber auch zur Folge, dass ungültige Frames nicht weggeworfen, sondern verschlüsselt zum Zielverschlüssler geschickt werden, der sie dann entschlüsselt und sie an den nächsten Switch weiterleitet, von dem sie dann weggeworfen werden. Probleme können sich auch bei mangelnder Integrität beim Entschlüsseln ergeben. Werden Teile des entschlüsselten Frames bereits weitergeleitet, bevor die Integrität überprüft worden ist, so können diese nicht mehr zurückgeholt werden. Im besten Fall wirft sie dann der nächste Switch fort.
Bei der Store & Forward-Methode wird der ganze Frame eingelesen, bevor mit der Verschlüsselung oder der Entschlüsselung begonnen wird. Damit wird die Latenz erhöht und ist von der Grösse des Frames abhängig. Ungültige Frames können so entdeckt und weggeworfen werden. Das fördert sowohl die Netzhygiene als auch die Sicherheit.

3.4. Latenz

Die durch den Verschlüssler hervorgerufene Latenz bewegt sich im Bereich von Mikrosekunden pro Gerät. Entscheidend ist der effektive Wert pro Gerät und nicht die Latenz, welche durch die eigentliche Verschlüsselung verursacht wird. Produktarchitektur und verwendete Komponenten spielen dabei eine grosse Rolle, wobei die Latenz bei praktisch allen aktuellen Anbietern von Geräten in der Gigabit-Klasse maximal 40 Mikrosekunden beträgt. Faktoren die auf dem gleichen Gerät zu unterschiedlichen Latenzzeiten führen, sind der Datendurchsatz, der gewählte Verschlüsselungsmodus und der Betriebsmodus. Die Latenz sollte immer auch im Verhältnis zur Gesamtlatenz der jeweiligen Standortkoppelungen betrachtet werden, da grössere Distanz zwangsläufig zu erhöhter Latenz führt.

3.5. Verschlüsselungsoffsets

Je nach Struktur des ankommenden Frames und nach gewünschter Einschränkung fängt die Verschlüsselung relativ zum Beginn des Frames früher oder später an. Während bei einer Hop-by-Hop-Verschlüsselung in einem LAN nur die MAC-Adressen unverschlüsselt bleiben müssen, sieht das bei einem MAN oder WAN anders aus. Dort sollte das VLAN-Tag unverschlüsselt bleiben und bei Frames mit MPLS-Tag auch das MPLS-Tag. In der Regel sollte die Verschlüsselung erst mit der Nutzlast beginnen, unabhängig davon, auf welcher Position sich diese befindet. Einfach gestrickte Verschlüssler unterstützen nur ein einziges fixes Verschlüsselungsoffset, das manuell gesetzt wird. Variable Verschlüsselungsoffsets sind deutlich flexibler und passen sich dem jeweiligen Frame an. Dies geht so weit, dass der Verschlüssler selbständig abhängig vom Frame-Inhalt herausfinden kann, wo die Verschlüsselung beginnen soll.

3.6. Die Verschlüsselungsmodi

Die vom Gerät unterstützten Verschlüsselungsmodi gehören zu den wichtigsten Produkteigenschaften eines Layer 2-Verschlüsslers.

- Verschlüsselt man den ganzen Frame, so sind auch die Adressinformationen verschlüsselt. Dann ist zwar alles verschlüsselt, aber Frame kann nur direkt zwischen zwei Verschlüsslern transportiert werden.

- Verschlüsselt man nur die Payload, so sind zwar alle Protokolle oberhalb von Layer 2 komplett abgesichert, doch beschränkt sich der Schutz für Layer 2 Protokolle auf die Frames und die Inhalte.

- Will man Layer 2 selbst auch schützen, analog wie dies ESP IPSec Tunnel Modus mit IP auf Layer 3 macht, so bleibt auch auf Layer 2 keine andere Wahl, als die Frames zu tunneln. Dies führt zu einem Overhead, der exakt der Grösse des Ethernet-Headers entspricht. Dieser Overhead kann dazu führen, dass Pakete grösser werden als das Netzwerk zulässt. Die in Multipunkt-Netzen vorgeschalteten Traffic Shaper sorgen bei IPv4-Netzen dafür, dass die Frame-Grösse die zugelassene MTU nicht überschreitet. Bei IPv6-Netzen erfolgt die Grössenoptimierung zwischen den beiden kommunizierenden IPv6-Geräten, in der Regel sind das Router.

Der Verschlüsselungsmodus hat nicht nur Auswirkungen auf den Schutz, sondern auch auf die Betriebskosten, die Latenzzeiten und auf die Hardware- und Software-Erfordernisse. Bei jedem Verschlüsselungsmodus spielt auch der verwendete Verschlüsselungsstandard eine Rolle. Zusammen bestimmen sie das Frame-Format, das wiederum die Schnitt-

stelle zwischen Verschlüssler und Netz und dem verschlüsselten Frame und dem unterliegenden Netz bildet. Nicht alle Hersteller unterstützen alle Verschlüsselungsmodi. Zudem ist der Replay- und Integritätsschutz unterschiedlich ausgestaltet.

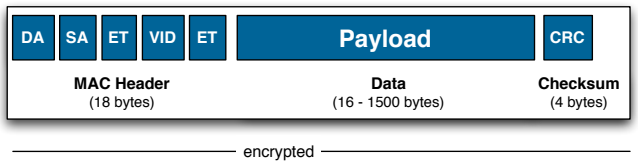
Der verwendete Verschlüsselungsmodus hat meist auch eine Auswirkung auf die Skalierbarkeit. Ein Multipunkt-WAN könnte theoretisch aus tausenden Standorten bestehen, deren Verkehr untereinander jeweils von einem Verschlüssler pro Standort abgesichert wird. Da eine vernünftige Segmentierung Grundlage für einen reibungslosen Betrieb, Effizienz und optimale Sicherheit ist, wird man ein solches WAN aber in der Praxis nicht antreffen, Es gibt wohl Verschlüssler, die theoretisch eine unlimitierte Zahl an Peers erlauben, doch ist in der Praxis eine Unterstützung von 500 Peers mehr als genügend. Bei den meisten breitbandigen Multipunkt-WANs beträgt die Anzahl der Peers sogar deutlich weniger als hundert.

Beim Verschlüsselungsmodus gilt es die optimale Balance zwischen Sicherheit, Kosten, Netzwerkkompatibilität und Overhead zu finden. Wichtiger Faktor dieser Balance ist auch der verwendete Verschlüsselungsstandard. Die Nutzung von authentisierter Verschlüsselung ist seit Jahren der Normalfall. Auf sie sollte nicht verzichtet werden. Der damit verbundene Overhead ist im Vergleich zur gewonnenen Sicherheit gering.

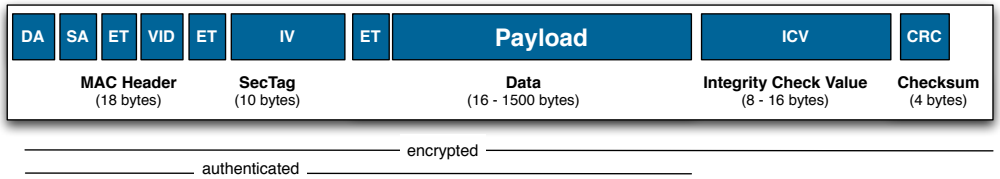
Bei den nachfolgenden Darstellungen von Frames ist das Verhältnis zwischen Header/CRC und Payload stark zuungunsten des Headers und der CRC Checksum verfälscht.

3.6.1. Frame-Modus

Beim Frame-Modus wird der ganze Inhalt des Frames verschlüsselt, inklusive Header und FCS Prüfsumme. Es sind keine Netzwerkadressen sichtbar und es werden auch keine sichtbaren Netzwerkadressen hinzugefügt.



Frame-Modus ohne authentisierte Verschlüsselung



Frame-Modus mit authentisierter Verschlüsselung

Vorteile:

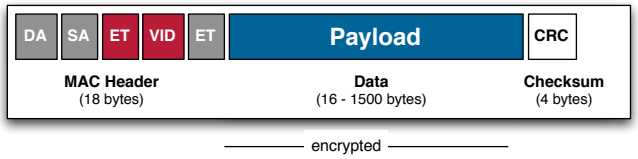
- Der ganze Frame ist komplett verschlüsselt
- Das Abhören der Leitung zeigt nichts über das Netzwerk und die Daten auf
- Authentisierte Verschlüsselung erzeugt im Vergleich zur gewonnen Sicherheit unterdurchschnittlich wenig Overhead (24-32 Bytes); dies variiert je nach Schutz und Hersteller
- Bei Verzicht auf authentisierte Verschlüsselung kein Verschlüsselungs-Overhead auf Frame-Ebene

Nachteile:

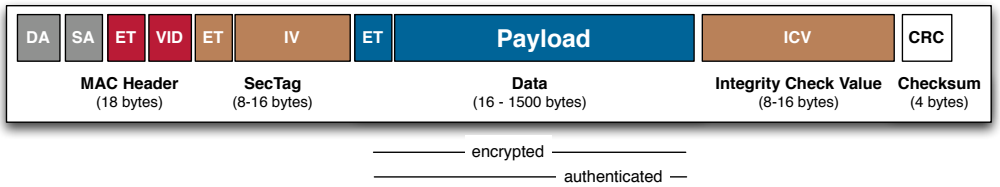
- Braucht eine transparente (eigene) Linie
- Kann nicht geswitcht werden
- Hat höhere Betriebskosten
- Inkompatibel zu Managed Ethernet Services

3.6.2. Transport-Modus

Beim Transportmodus wird nur die Nutzlast verschlüsselt, d.h alle Informationen, die sich im Header befinden, bleiben unverschlüsselt. Bei den Verschlüsslern, die diesen Modus unterstützen, lässt sich in der Regel festlegen, ab wo im MAC Header verschlüsselt werden soll (Encryption Offset). So können z.B. die Felder für EtherType, das VLAN Tag und ein MPLS Tag unverschlüsselt gelassen werden, damit sich die Pakete transparent zu MPLS und VLANs verhalten.



Transport-Modus ohne authentisierte Verschlüsselung



Transport-Modus mit authentisierter Verschlüsselung

Vorteile:

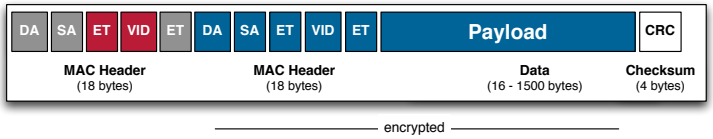
- Die Nutzlast ist komplett verschlüsselt
- Authentisierte Verschlüsselung erzeugt im Vergleich zur gewonnen Sicherheit unterdurchschnittlich wenig Overhead (24-32 Bytes); dies variiert je nach Schutz und Hersteller
- Bei Verzicht auf authentisierte Verschlüsselung geringer Verschlüsselungs-Overhead
- Kann geswitcht werden
- Kann transparent zu VLAN und MPLS sein
- Kompatibel mit Managed Ethernet Services

Nachteile:

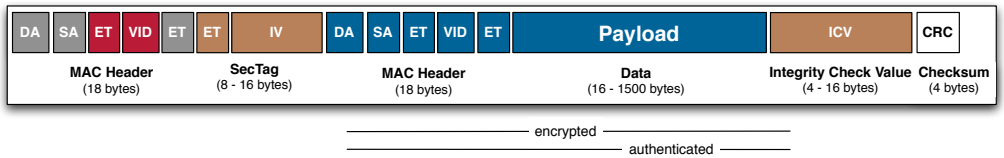
- Nur die Nutzlast von Layer 2-Paketen ist geschützt
- Das Abhören der Leitung zeigt die LAN-Struktur auf, da der Header nicht verschlüsselt ist
- MACSpoofing ist möglich, sofern nicht der Header oder Teile davon auch signiert sind

3.6.3. Tunnel-Modus

Beim Tunnel-Modus wird das gesamte Original-Paket verschlüsselt und mit einem neuen Header und mit einer neuen Prüfsumme versehen. Absender resp. Empfänger sind die beiden Verschlüssler zwischen denen die Pakete ausgetauscht werden. Beim neu erzeugten Paket handelt es sich um ein normales Ethernet-Paket, welches das Originalpaket als Payload mitführt. Es entsteht dabei ein Overhead von bis zu 18 Bytes. Die Latenzzeit aufgrund der vermehrten Verarbeitungserfordernisse im einstelligen Mikrosekunden-Bereich. Es gibt zwei gebräuchliche Varianten für den Tunnel-Modus: Einerseits das Generieren eines neuen Tunnel-Headers mit den MAC-Adressen der Verschlüssler als Absender- respektive Destinationsadresse und andererseits das Generieren eines neuen Tunnel-Headers mit einer systemspezifischen Absenderadresse unter Beibehaltung der ursprünglichen Destinationsadresse.



Tunnel-Modus ohne authentisierte Verschlüsselung



Tunnel-Modus mit authentisierter Verschlüsselung

Vorteile:

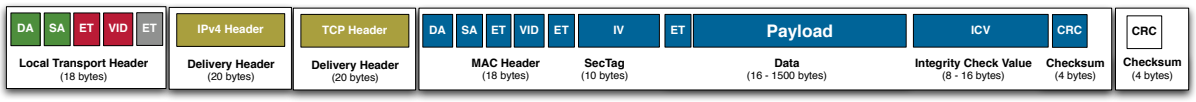
- Das Original-Paket ist komplett verschlüsselt
- Das Netzwerk ist inklusive Layer 2 voll abgesichert
- Authentisierte Verschlüsselung erzeugt im Vergleich zur gewonnen Sicherheit unterdurchschnittlich wenig zusätzlichen Overhead (24-26 Bytes); dies variiert je nach Schutz und Hersteller
- Kann geswitcht werden
- Transparent zu VLAN und MPLS
- Kompatibel mit Managed Ethernet Services

Nachteile:

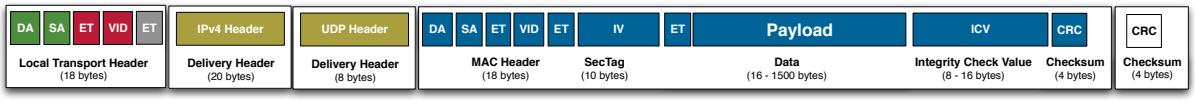
- Verschlüsselungs-Overhead von bis zu 70% auf Paketebene (bei 64 Byte Frames; im Schnitt aber weniger als 10%)
- Deutlich erhöhte Anforderung an den Verschlüssler führt zu verminderter Skalierbarkeit
- Vorwiegend auf den Einsatz im Punkt-zu-Punkt- und Punkt-zu-Multipunkt-Betrieb optimiert

3.6.4. IP-basierter Tunnel

Ethernet-Frames können auch über IP transportiert werden, wobei der Ethernet-Frame als IP-Nutzlast getunnelt wird.



Ethernet over IP (EoIP) über TCP mit authentisierter Verschlüsselung

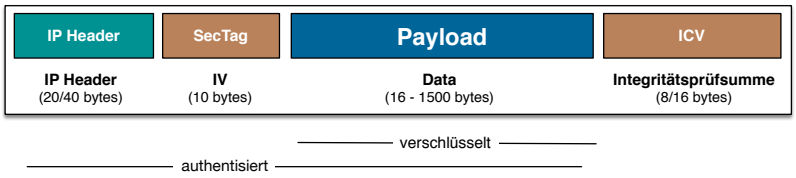


Ethernet over IP (EoIP) über UDP mit authentisierter Verschlüsselung

Da die Verschlüsselung nicht direkt auf Layer 2 erfolgt, bringt dieser Ansatz einen grossen Overhead und höhere Latenzzeiten mit sich. Sinnvoll sind IP-basierte Tunnel nur dort, wo keine Ethernet-Layer 2- Verbindungen vorhanden sind. Erfolgt der Transport über IP, so muss auch der Schlüsselaustausch über IP möglich sein.

3.6.5. Native IP-Verschlüsselung

Von Layer 2 aus lassen sich auch reine IP-Netzwerke nativ verschlüsseln. Dabei gilt es allerdings die Eigenheiten von IP-Netzwerken genügend zu berücksichtigen.



Im Vergleich zu IPSec-basierten Lösungen liegt der Verschlüsselungsoverhead in der Regel tiefer und es stehen von vornherein Gruppenschlüsselsysteme zur Verfügung. Entsprechend kommen Verschlüssler mit nativer IP-Unterstützung vorwiegend bei MPLS- und IP-Netzwerken zum Einsatz, bei denen eine sichere und leistungsfähige Alternative zu GET VPN benötigt wird.

3.7. Grösse des Replay-Fensters

Authentisierte Verschlüsselung verwendet einen Counter. Ankommende Frames müssen im Normalfall einen Zählerstand aufweisen, der um eins höher ist als der Zählerstand des vorherigen Frames. Insbesondere bei Nah- und Weitverkehrsnetzwerken kann es durchaus vorkommen, dass die Reihenfolge nicht eingehalten wird. Je nach Netzwerkqualität braucht es deshalb ein Fenster, innerhalb dessen Breite Frames akzeptiert werden, auch wenn sie nicht in der richtigen Reihenfolge ankommen. Dieses Fenster sollte schmal genug sein, um keine Replay-Attacken zuzulassen. Das Replay-Fenster kann entweder durch die maximal erlaubte Abweichung des Zählerstandes, durch Zeit in Sekunden oder eine Kombination der beiden definiert werden. Eine weitere Möglichkeit ist die Zuweisung von Replay-Fenster auf CoS-Werte.

3.8. Selektive Verschlüsselung

Es gibt Szenarien, in denen gewisse Frames nicht verschlüsselt werden dürfen oder anders behandelt werden müssen. Das können z.B. die Frames eines VLANs sein, das zur Anbindung an das Internet verwendet wird, oder Frames mit einem MPLS-Tag. Als Auswahlkriterien stehen die im Frame vorhandenen Informationen zur Verfügung: VLAN-ID, MPLS-Tag, Ethertype und MAC-Adresse. Auch die Zugehörigkeit zu einer definierten Gruppe kann als Kriterium dienen. Vorstellbar ist auch die Verwendung zusätzlicher Kriterien wie QoS-Parameter und Paketgrösse. Viele Metro Ethernet Services bauen auf VLAN-IDs auf und die selektive Verschlüsselung nach VLAN-IDs ist für bestimmte Services Voraussetzung. So erlaubt sie das Konsolidieren von Anschlussleitungen, was zur Vereinfachung und zur Kostenersparnissen führt. „MPLS Awareness“ gekoppelt mit selektiver Verschlüsselung aufgrund der Präsenz eines MPLS-Tag wird benötigt, um mit unterschiedlichen MPLS-Szenarien zurechtzukommen.

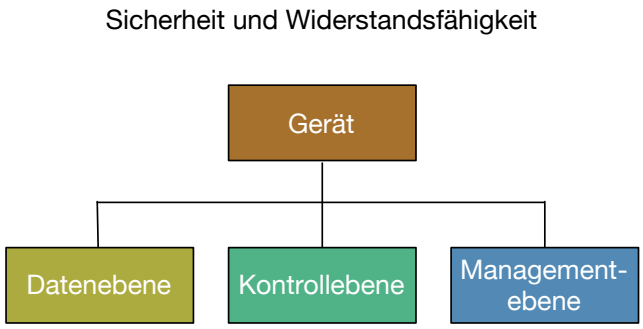
3.9. Traffic Flow Security

Mittels Traffic Flow Security lässt sich der Netzwerkverkehr vernebeln, indem Framegrössen und –sequenzen für den Transport modifiziert werden. Herkömmliche Methoden beschränkten sich auf das Verwenden uniformer Framegrössen und den Betrieb über dedizierte Punkt-zu-Punkt-Verbindungen. Neuere Methoden arbeiten mit variablen Framegrössen und unterstützen alle Einsatzszenarien. Sie können zudem durch gezielte Traffic Flow-Optimierung den IMIX-Durchsatz bei der Verwendung eines Tunnel-Modus (Ethernet-Tunnel oder Ethernet über IP) auf dem gleichen Niveau halten, das eine normale authentisierte Verschlüsselung im Transport-Modus bietet.

Es gibt unterschiedliche Varianten zur Implementierung von Traffic Flow Security, die wiederum eine direkte Auswirkung auf das Netzwerkverhalten und die unterstützten Netzwerktopologien haben. Traffic Flow Security ist ein zusätzlicher Schutz, der vorwiegend dort eingesetzt wird, wo sehr hohe Sicherheitsanforderungen bestehen.

5. Verschlüsselung der Kontrollebene

Netzwerkverschlüssler stehen in der Regel zwischen einem Standort und der Anbindung an das MAN oder WAN. Es genügt nicht, nur die Datenebene möglichst gut abzusichern. Um Daten zu verschlüsseln braucht es Schlüssel und die müssen zwischen den Geräten ausgetauscht werden. Der Schlüsselaustausch ist deshalb ein genauso beliebter Angriffspunkt wie das Gerät selbst, die Managementebene und der Rest der Kontrollebene. Eine Schwachstelle in einem der vorgenannten Bereiche kann die gesamte Sicherheit kompromittieren.



Die Problematik der Absicherung von Kontrollebene, Schlüsseleinigung und Schlüsselaustausch auf Netzwerkebene ist ein Bereich, der in der Vergangenheit zu wenig Beachtung gefunden hat.

5. Umgebungserkennung und Key Server

5.1. Automatische Umgebungserkennung

Das Aufsetzen von Verschlüsslern und Anpassungen an Konfigurationsänderungen wird durch automatische Umgebungserkennung vereinfacht. Mit ihr kann ein Verschlüssler nicht nur andere Verschlüssler im gleichen Netzwerk, sondern auch vorhandene Key Server und VLANs selbständig erkennen. Sind die Verschlüssler aufgesetzt, so sollte man die automatische Umgebungserkennung abschalten können, da sie erst bei Konfigurationsänderungen des Netzwerks wieder benötigt wird.

5.2. Key Server

Als Key Server gilt jedes Gerät, das Schlüssel erzeugt und an andere Geräte weitergibt. Wie diese Generierung und Weitergabe erfolgt, ist unterschiedlich gelöst. Bei symmetrischen Schlüsselsystemen können statt eines Schlüssels die zur Berechnung des Schlüssels notwendigen Informationen generiert und weitergeleitet werden.

5.3. Integrierter Key Server

Verschlüssler mit integriertem Key Server sind nicht auf einen externen Key Server angewiesen. Abhängig vom Einsatzszenario und von Vorschriften ist die Verwendung eines externen Key Servers vorteilhaft oder gar Voraussetzung.

5.4. Unterstützung für externen Key Server

Integrierter und externer Key Server schliessen sich nicht gegenseitig aus. Bei grossen Netzwerken kann es vorteilhaft sein, eine Kombination von integrierten und externen Key Server zu verwenden. Je nach Häufigkeit des Austauschs der Master Keys und der Anzahl benötigter Master Keys, ist der Einsatz von externen Key Server für eine bessere Skalierbarkeit von Vorteil. Ein externer Key Server unterliegt den gleichen Sicherheitsanforderungen wie ein Verschlüssler selbst.

Bei zertifikatsbasierten asymmetrischen Schlüsselsystemen kann die Verwendung eines Hardware Security Module (HSM) als Certificate Authority (CA) unterstützt werden.

Eine andere Art von externem Key Server wird für den Austausch von Quantenschlüsseln (QKD) gebraucht. Dieser muss lokal nahtlos mit dem Verschlüssler verzahnt sein.

5.5. Externer Key Server

Als externe Key Server kommen netzwerkgestützte Key Server und HSM, sowie lokale QKD-Geräte in Frage. Für QKD-Geräte wird zudem eine zusätzliche optische Verbindung benötigt.

5.6. Unterstützung für mehrere, verteilte Key Server

Ein einzelner Key Server kann ausfallen. Gleiches gilt auch für die Verbindungen zu einem Key Server. Mit mehreren, verteilten Key Servern lässt sich eine redundante Architektur aufbauen, die den Betrieb bei Ausfall eines Key Servers oder einer Verbindung so weit wie möglich aufrechterhält. Für die Mehrmandantenfähigkeit, bei der die Schlüsselhoheit bei den Mandanten liegt, ist die Unterstützung für mehrere, verteilte Key Server eine Grundvoraussetzung.

5.7. Unterstützung für das Ausweichen auf Ersatz-Key Server

Bei Gruppenschlüsselsystemen, bei welchen sich alle Mitglieder einer Gruppe den gleichen Schlüssel für das Verschlüsseln und Entschlüsseln verwenden, braucht es einen Key Server für die Gruppe, der den Gruppenmitgliedern diesen gemeinsam verwendeten Schlüssel zur Verfügung stellt. Fällt dieser aus, so ist kein Schlüsselwechsel mehr möglich. Um dies zu vermeiden braucht es die Möglichkeit, dass innerhalb einer Gruppe, mehrere Mitglieder hierarchisch abgestuft die Funktion des Key Servers für die Gruppe übernehmen können.
Bei Gruppenschlüsselsystemen, bei denen ein Key Server nur die Schlüssel zum Entschlüsseln der von ihm verschlüsselten Frames verteilt, braucht es keinen Ersatz-Key Server für die Gruppe, da auch keine verschlüsselten Frames mehr verschickt werden.

6. Schlüsselverwaltung

Die Schlüsselverwaltung ist das Herzstück jeder Verschlüsselungslösung, Sie bestimmt massgeblich den Einsatzbereich und die Funktionalität.

6.1. Grundausstattung

Wirklich zufällige Zufallszahlen, sichere Schlüsselaufbewahrung und autonomer Betrieb gehören zur Grundausstattung einer Lösung, die sichere Standort-Vernetzung bieten will. Bei virtuellen Appliances ist dies nur über die Verwendung von Zusatzhardware machbar, z.B. via Smartcard.

6.1.1. Hardware-basierter Zufallszahlengenerator

Sichere kryptographische Lösungen brauchen als Ausgangsmaterial wirklich zufällige Zufallszahlen. Software kann keine echten, sondern nur Pseudo-Zufallszahlen generieren. Sichere Lösungen verwenden einen echten hardware-basierten Zufallszahlengenerator, der zur Schlüsselgenerierung verwendet wird.

http://en.wikipedia.org/wiki/Hardware_random_number_generator

6.1.2. Sicherheit der Schlüsselaufbewahrung

Von den Schlüsseln hängt die Sicherheit des Systems ab. Mit den Schlüsseln lässt sich alles entschlüsseln. Deshalb müssen alle Schlüssel und Anfangsgeheimnisse (Pre-Shared Secret, Zertifikat, private Schlüssel, etc.) sicher aufbewahrt werden. So sicher, dass bei Manipulationsversuchen der Schlüsselspeicher unwiderruflich gelöscht wird. Das geht nur mit Hardware.

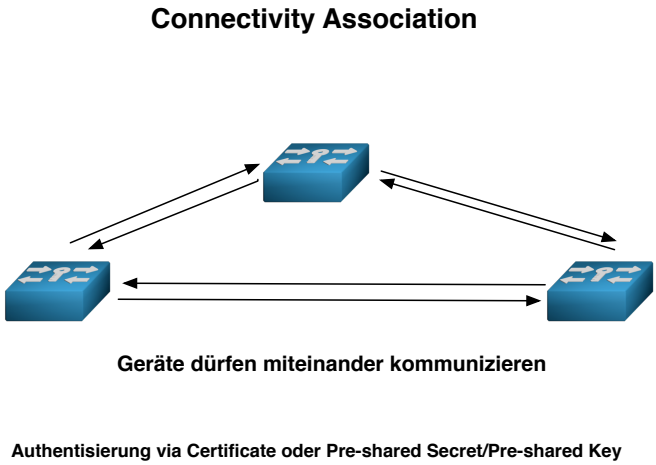
http://en.wikipedia.org/wiki/Tamper_resistant

6.1.3. Autonomer Betrieb

Der autonome Betrieb bedingt, dass der Verschlüssler seine Arbeit selbständig, ohne Zuhilfenahme externer Ressourcen, erledigen kann. Jede externe Ressource stellt wiederum ein Risiko und eine Abhängigkeit dar. Nicht als externe Ressource zählen dedizierte Key Server, Certificate Authorities und dediziertes Security Management. Diese sollten aber redundant ausgelegt sein, um bei Ausfall einen nahtlosen Weiterbetrieb zu garantieren.

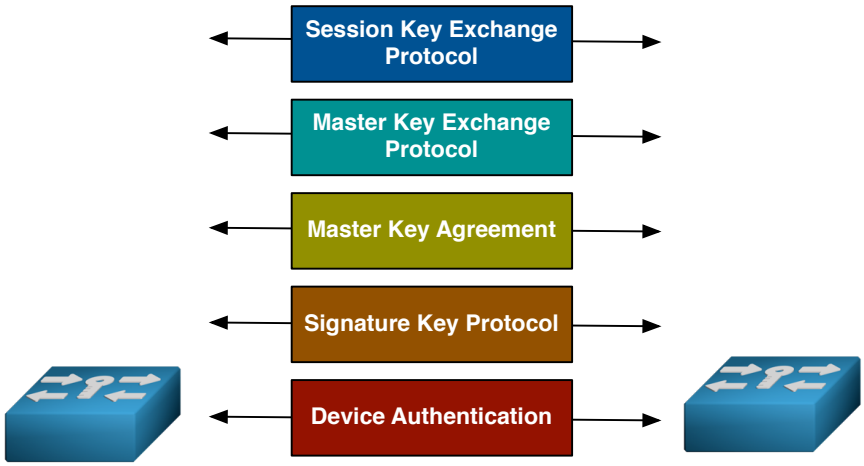
6.2. Verbindungsaufbau

Für eine Kommunikation braucht es mehr als eine Partei. Die beteiligten Verschlüssler müssen sich deshalb gegenseitig finden, erkennen und authentisieren. Ist dies erfolgt, so besteht zwischen den beteiligten Verschlüsslern jeweils eine Connectivity Association. Sie dürfen und können miteinander kommunizieren.



Ist die Connectivity Association erstellt, so braucht es zusätzlich eine Security Association, die festlegt, wie die beiden Beteiligten sicher miteinander kommunizieren. Dafür wird ein Anfangsgeheimnis benötigt. Dabei kann es sich um einen Pre-Shared-Key oder ein Zertifikat handeln. Bei Verwendung von elliptischen Kurven gehört auch die Kurven-Domain dazu. Die Anfangsgeheimnisse sind im sicheren Schlüsselspeicher abgelegt.

Vom Anfangsgeheimnis bis zum Session Key laufen mehrere komplexe Prozesse ab, die sowohl in sich selbst wie auch in der Abfolge sicher sein müssen.



Die meisten Verschlüssler verwenden eine hybride Herangehensweise, bei der eine Kombination aus asymmetrischer und symmetrischer Verschlüsselung zum Einsatz kommt. Der Datenverkehr wird dabei symmetrisch verschlüsselt.

6.3. Authentifizierung /Anfangsgeheimnis und Signaturprotokoll

Die Verschlüssler müssen sich gegenseitig authentifizieren können. Dies kann über Zertifikate (asymmetrisch) oder Pre-Shared Secrets (symmetrisch) erfolgen.

http://en.wikipedia.org/wiki/Shared_secret
http://en.wikipedia.org/wiki/X.509

Bei Pre-Shared Secrets kann die Authentifizierung entweder per Verschlüsslerpaar, per Netzwerk oder per Gruppe aufgesetzt werden.

Pre-Shared Secret respektive Zertifikat dienen zur Signatur, mit welcher der Absender verifiziert werden kann. Mit ihnen unterschreiben die Schlüsselaustauschverfahren die ausgetauschten Schlüssel oder Teilschlüssel um sicherzustellen, dass sie auch von der richtigen Gegenstelle stammen.

http://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm
http://en.wikipedia.org/wiki/Digital_Signature_Algorithm
http://en.wikipedia.org/wiki/RSA
http://crypto.stackexchange.com/questions/14654/digital-signature-using-symmetric-key-cryptography

Die Signatur in Kombination mit dem entsprechenden Signaturprotokoll ist Basis für den Schlüsselaustausch.

6.4. Schlüsselaustausch

Für den Schlüsselaustausch kommen sowohl symmetrische wie auch asymmetrische Verfahren In Frage. Der Einsatz eines asymmetrischen Verfahrens erfordert deutlich mehr Rechenleistung, gilt aber dafür entsprechend auch als sicherer. Es wird von gewissen Kreisen vermutet, dass sich die bei asymmetrischen Verfahren verwendeten mathematischen Probleme mittels spezieller Algorithmen mit einem Quantencomputer relativ schnell lösen lassen und dass mit der Verfügbarkeit innert wenigen Jahren gerechnet werden muss. Eine entscheidende Verbesserung der Sicherheit, die auch allfälligen Angriffen durch Quantencomputer standhält, bietet die Kombination von asymmetrischen und symmetri-

schen Verfahren, wie z.B. die Kombination von Diffie-Hellman mit symmetrischer Überschlüsselung der Teilschlüssel. Dabei erfolgt die Signatur mit einem symmetrischen 256-bit AES-Schlüssel, der den asymmetrischen Schlüsselaustausch resistent gegen allfällige Schwachstellen und Angriffe von Quantencomputer macht.

6.4.1. Symmetrischer Schlüsselaustausch

Bei einer symmetrischen Vorgehensweise sind alle Schlüssel direkt voneinander abgeleitet. Zuerst wird beim Verschlüssler ein Pre-Shared-Secret eingegeben. Der Master Key wird intern im Verschlüssler erzeugt und mit dem Shared Secret verschlüsselt. Der Session Key wird ebenfalls vom Verschlüssler erstellt und mit dem Master Key verschlüsselt. Master- und Session Key werden jeweils in der verschlüsselten Form über die Leitung zum anderen Verschlüssler übertragen. Das grosse Problem bei dieser Vorgehensweise liegt darin, dass wenn das Shared Secret irgendwann bekannt wird, jede früher aufgezeichnete Kommunikation entschlüsselt werden kann. Es besteht also keine Perfect Forward Secrecy (PFS).

http://en.wikipedia.org/wiki/Symmetric_key_algorithm
http://en.wikipedia.org/wiki/Symmetric_key_management

6.4.2. Asymmetrischer Schlüsselaustausch

Bei einer asymmetrischen Vorgehensweise werden die Teilschlüssel vollständig im Verschlüssler generiert, ohne dass der Benutzer einen Zugriff darauf hätte. Aus den jeweils ausgetauschten Teilschlüsseln berechnen beide Seiten jeweils das gleiche Shared Secret. Im Gegensatz zu einem symmetrischen Verfahren kennt hier niemand das Shared Secret. Der Verschlüssler erzeugt anschliessend intern den Master Key und verschlüsselt ihn mit dem Shared Secret. Auch der Session Key wird vom Verschlüssler erstellt, als Schlüssel für den Schlüsselaustausch dient der Master Key. Die Übertragung der Master- und der Session-Keys von einem Verschlüssler zum andern erfolgt immer in verschlüsselter Form.

Als asymmetrische Verfahren werden primär Diffie-Hellman und RSA eingesetzt. Diffie-Hellman verwendet in der Standardvariante das so genannte „diskrete Logarithmus Problem“. Dieses Verfahren erzeugt aber bei entsprechender Sicherheit sehr lange Teilschlüssel. Gleiches gilt auch für RSA. Moderne Systeme tendieren deshalb zur Verwendung von Diffie-Hellman mit Elliptic Curve Crypto System (ECC). Dies bietet bei wesentlich kürzeren Teilschlüsseln eine höhere Sicherheit und gilt heute als Standard. Nicht alle elliptischen Kurven gelten als gleich sicher. Insbesondere die Sicherheit der NIST-Kurven wird in Fachkreisen als zweifelhaft eingestuft. Einige Anbieter beschränken sich dennoch auf die Unterstützung der NIST-Kurven, während andere dem Kunden die Wahl zwischen NIST-Kurven, Brainpool-Kurven, Safecurves und anderen Kurven lassen. Das Erstellen

elliptischer Kurven ist hochkomplex, vor allem, wenn sie sicher sein müssen. Zwischen den verschiedenen Kurven bestehen Geschwindigkeitsunterschiede, doch sind diese bei statischen Standortvernetzungen vernachlässigbar.

http://en.wikipedia.org/wiki/Diffie-Hellman
http://en.wikipedia.org/wiki/RSA
http://en.wikipedia.org/wiki/Elliptic_Curve_Diffie-Hellman
http://safecurves.cr.yp.to/index.html
http://www.ecc-brainpool.org/links.htm
https://tls.mbed.org/kb/cryptography/elliptic-curve-performance-nist-vs-brainpool

Asymmetrische Verfahren unterschreiben die ausgetauschten Teilschlüssel um sicherzustellen, dass sie auch von der richtigen Gegenstelle stammen. Dies kann entweder durch Zertifikate (X.509) kombiniert mit entsprechenden Verfahren (RSA, DSA oder ECDSA) oder durch Verschlüsselung des Teilschlüssels mit einem Pre-Shared Secret erfolgen.

6.4.3. Austauschfrequenz

Je häufiger der verwendete Session Key geändert wird, desto geringer ist die Wahrscheinlichkeit, dass er geknackt wird oder ein Replay Folgen haben kann. Die Sicherheit des Schlüssels hängt dabei nicht nur von der Vertraulichkeit, sondern auch von den verwendeten Verfahren und den gewählten Parametern ab. So spielen die Länge des Counters und des ICV eine Rolle. Im Counter Mode muss z.B. der Schlüssel gewechselt werden, bevor sich Zählerstand wiederholt. Es ist deshalb wichtig, dass der Session Key vom System automatisch nach einer bestimmten Anzahl Minuten gewechselt wird. Das gleiche gilt für den Key Encryption Key (Master Key), der für die Verschlüsselung des Session Key verwendet wird. Da dieser weniger Daten verschlüsselt, ist die Wechselfrequenz entsprechend tiefer. Auch dieser Schlüssel sollte automatisch ausgewechselt werden können.

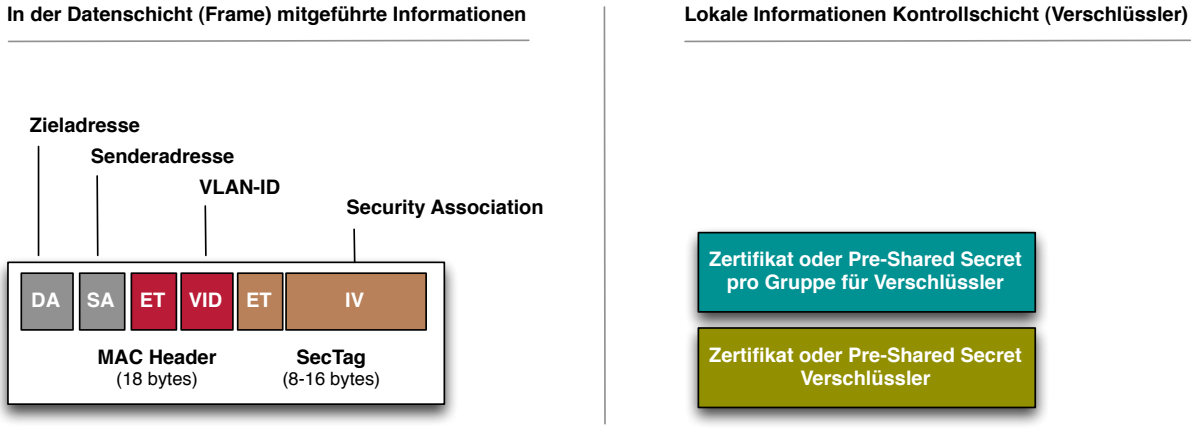
Schlüsseltyp	Wechselfrequenz
Session Key (Data Encryption Key)	alle 1 - 60 Minuten
Master Key (Key Encryption Key)	alle 1 -24 Stunden
Anfangsgeheimnis	alle 12 - 24 Monate

6.5. Schlüsselsystem

Ethernet-Frames gibt es in drei Grundvarianten, welche jeweils durch die Anzahl Zielrechner bestimmt sind:

- Unicast für die Kommunikation von einer mit einer einzelnen anderen MAC-Adresse
- Multicast für die Kommunikation von einer mit mehreren MAC-Adressen
- Broadcast für die Kommunikation von einer mit allen anderen MAC-Adressen

Es stehen unterschiedliche Ansätze zur Verfügung, um sicherzustellen, dass nebst Unicast-Frames auch Multicast- und Broadcast-Frames verschlüsselt werden. Grundlage für das Schlüsselsystem bilden einerseits die im jeweiligen Verschlüssler vorhandenen Anfangsgeheimnisse und andererseits die im Frame mitgeführten Informationen.



Beim Schlüsselsystem kann man grob zwischen zwei unterschiedlichen Lösungsansätzen unterscheiden: Paarweise Schlüssel und Gruppenschlüssel.

Für paarweise Schlüsselsysteme besteht ein Netzwerk aus einer oder mehreren Punkt-zu-Punkt-Verbindungen. Jeder Verschlüssler ist mit jedem anderen Verschlüssler Punkt-zu-Punkt verbunden. Paarweise Schlüsselsysteme verwenden jeweils den gleichen unidirektionalen Schlüssel für die Verbindung zwischen zwei Verschlüsslern.
Gruppenschlüssel orientieren sich hingegen an der Zugehörigkeit zu einer Gruppe und verwenden jeweils einen unterschiedlichen Schlüssel pro Gruppe. Es besteht eine Vielzahl von Möglichkeiten zur Bestimmung einer Gruppe. Eine Gruppe kann beispielweise aus einem VLAN oder mehreren VLANs bestehen. Dann ist sie bidirektional: Jedes Gruppenmitglied verschlüsselt und entschlüsselt mit dem gleichen Schlüssel. Eine Gruppe kann aber auch vom versendenden Verschlüssler so definiert werden, dass alle möglichen Empfänger für ihn eine Gruppe bilden. In diesem Fall ist sie unidirektional: Jeder Verschlüssler verwendet einen anderen Schlüssel zum Verschlüsseln und der Empfänger benutzt jeweils den ihm vom Versender zuvor kommunizierten Schlüssel zum Entschlüsseln. Ein

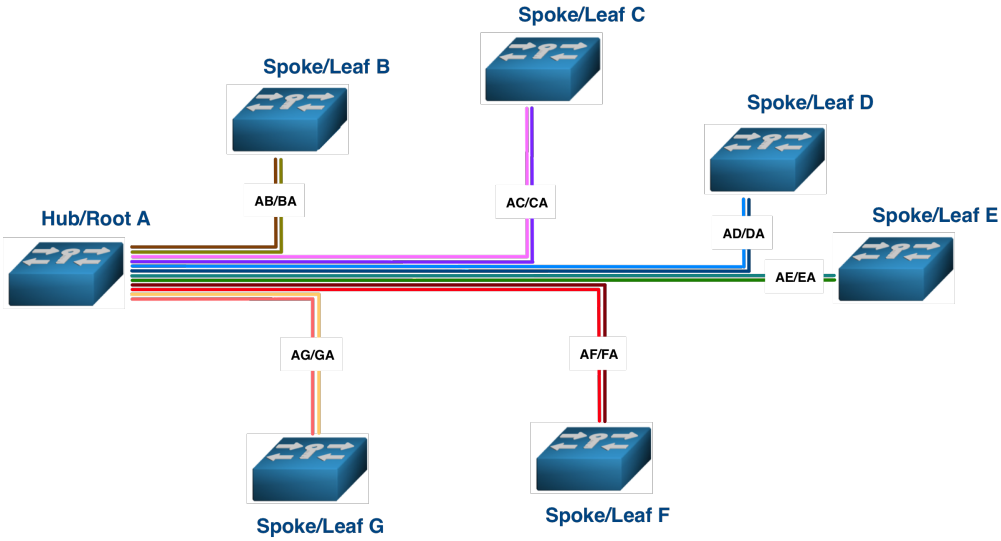
Verschlüssler kann mehrere Gruppen unterstützen. Für jede Gruppe verwendet er einen unterschiedlichen Schlüssel.

Es ist auch möglich, eine Kombination von Gruppe und Paar zu verwenden. So lässt sich organisatorisch ein VLAN als Gruppe betrachten, innerhalb derer paarweise Schlüssel und Gruppenschlüssel verwendet werden. Für jedes VLAN gibt es dann eigene paarweise Schlüssel und Gruppenschlüssel.

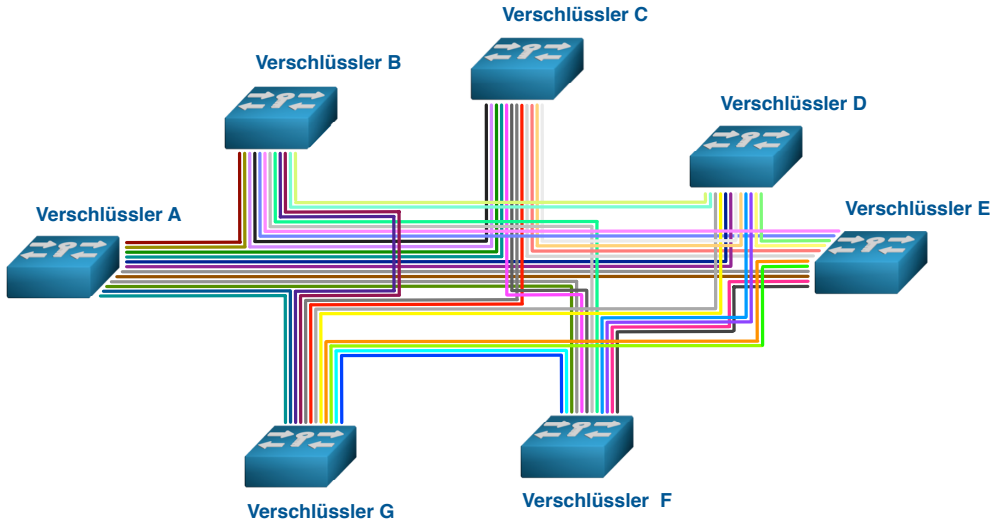
6.5.1. Paarweise Schlüssel

Für ein paarweises Schlüsselsystem entsprechen Punkt-zu-Punkt-Verbindungen einer Leitung, deren Endpunkte durch die beiden Verschlüssler A und B definiert sind.
Für die Verschlüsselung der Daten von A nach B wird der Schlüssel AB verwendet. In der Gegenrichtung, von B nach A, der Schlüssel BA.

Paarweise Schlüsselsysteme sind für Punkt-zu-Punkt-Verbindungen ausgelegt und betrachten deshalb auch Punkt-zu-Multipunkt- und Multipunktnetzwerke als eine Häufung von Punkt-zu-Punkt-Verbindungen. Paarweise Schlüsselsysteme funktionieren deshalb ausschliesslich für Unicast-Frames. Nur diese sind über ihre MAC-Adresse eindeutig zuweisbar. Multicast- und Broadcast-Frames haben mehrere Destinationsadressen, weshalb sie für ein paarweises Schlüsselsystem nicht verschlüsselbar sind. Es gibt z.B. keinen eigenen Schlüssel, mit dem Verschlüssler A ein Multicast-Frame zu zwei Zielverschlüsslern (B und C) verschlüsseln könnte und von beiden Zielverschlüsslern entschlüsselt werden kann.



Bei Multipunkt-zu-Multipunkt-Verbindungen stellt sich das Problem mit den Multicast- und Broadcast-Frames gleich wie bei den Punkt-zu-Multipunkt-Verbindungen.



Für diese Problematik stehen vier unterschiedliche Lösungsansätze zur Verfügung: (1) Multicast- und Broadcast-Frames unverschlüsselt lassen, (2) Die Multicast- und Broadcast-Frames für jede Verbindung replizieren und sie in Unicast-Frames umwandeln, (3) ein zusätzliches, geeignetes Schlüsselsystem für Multicast- und Broadcast-Frames verwenden und (4) ein Schlüsselsystem, das sowohl Unicast-, Multicast- als auch Broadcast-Frames unterstützt.
Die erste Lösung – die Dispensierung der Multicast- und Broadcast-Frames von der Verschlüsselung – ist, zumindest in Bezug auf die Sicherheit von Multicast- und Broadcast-Frames, nicht akzeptabel. Die zweite Lösung - das Replizieren der Multicast- und Broadcast-Frames über alle Verbindungen – führt zu einer erheblichen Mehrbelastung des

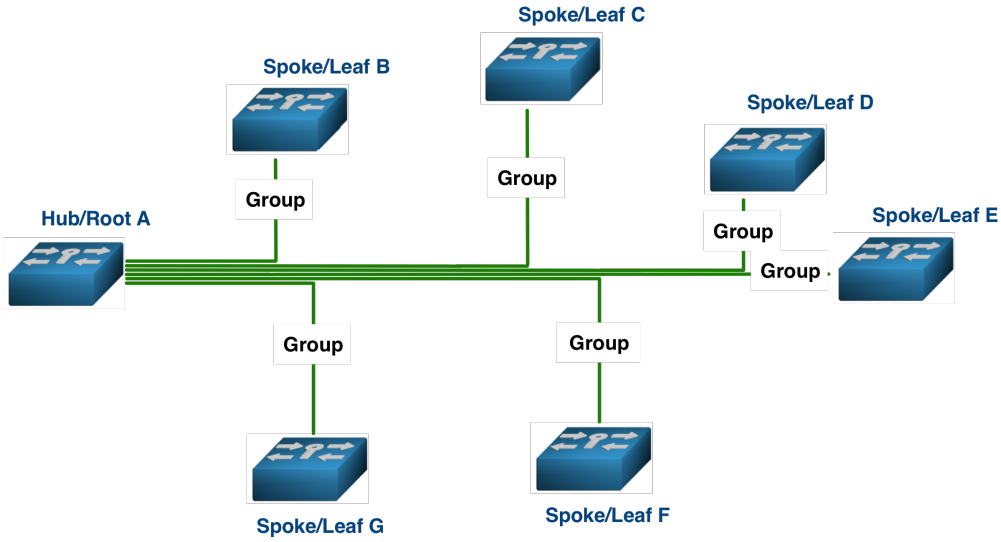
Netzwerks. Dies zieht wiederum höhere Betriebskosten oder eine schlechtere Netzwerkperformance nach sich. Die dritte Lösung – Verwendung eines zweiten Schlüsselsystems – führt zur zwangsweisen Zusammenarbeit zweier unterschiedlicher Schlüsselsysteme, löst aber das Problem der Verschlüsselung von Multicast- und Broadcast-Frames. Je nach Frame-Typ ist dann das eine oder das andere Schlüsselsystem zuständig. Für die Multicast- und Broadcast- Frame-Verschlüsselung werden Gruppenschlüsselsysteme verwendet. Die vierte Lösung ist meist das effizienteste: Ein Schlüsselsystem, das sowohl Unicast-, wie auch Multicast- und Broadcast-Frames unterstützt.

6.5.2. Gruppenschlüssel

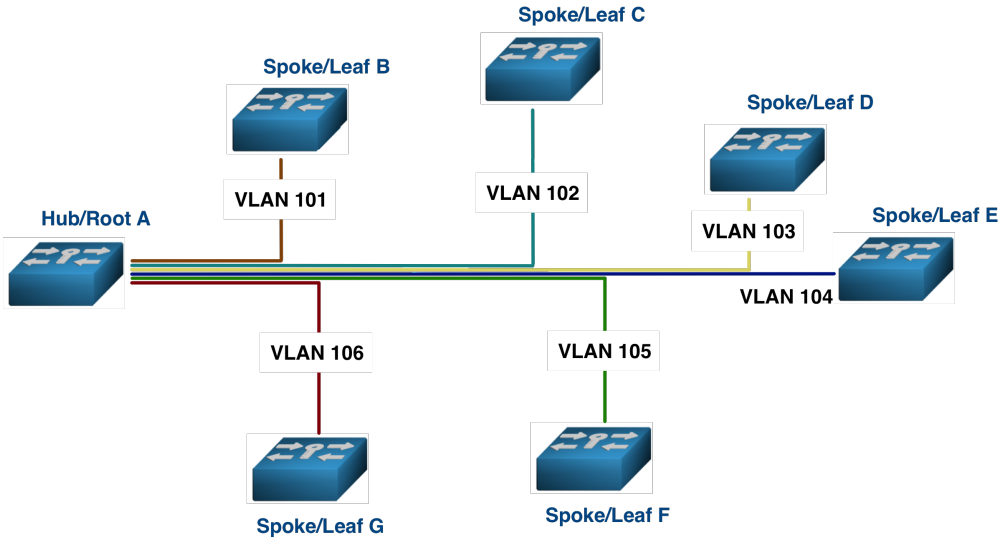
Gruppenschlüsselsysteme basieren auf dem Prinzip, dass für die Kommunikation innerhalb einer definierten Gruppe der gleiche Schlüssel verwendet wird. Die Mitgliedschaft in einer Gruppe schliesst nicht die Mitgliedschaft in weiteren Gruppen aus. Nur wird für die Kommunikation innerhalb der unterschiedlichen Gruppen jeweils ein anderer Schlüssel verwendet. Dies führt zu einer kryptographischen Trennung der Gruppen. Eine Gruppe besteht aus zwei oder mehr Mitgliedern. Für Ethernet werden Gruppen meistens nach VLAN-ID erstellt.

Dies funktioniert für alle drei Grund-Topologien, angefangen mit Punkt-zu-Punkt.

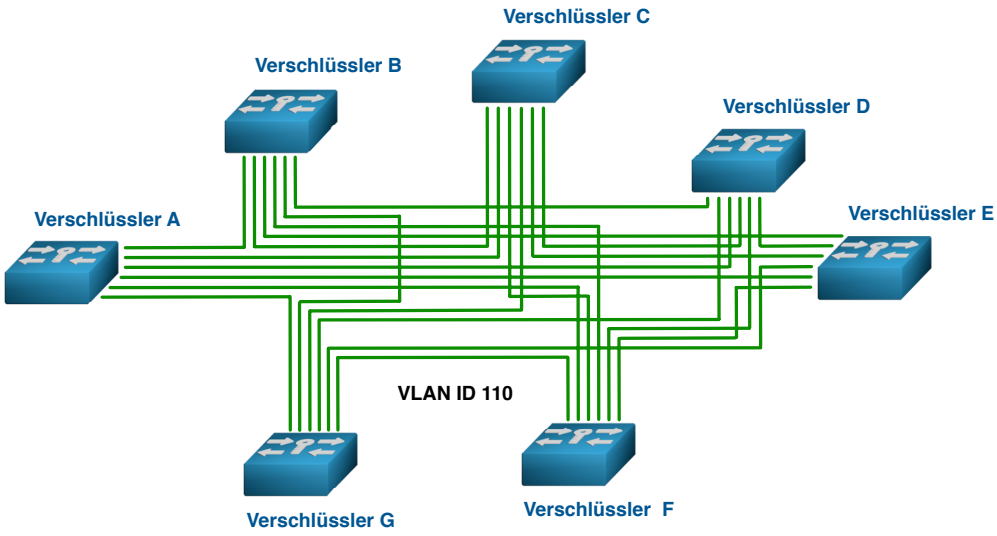
Bei Punkt-zu-Multipunkt bestehen zwei unterschiedliche Möglichkeiten. Das Netzwerk kann entweder als eine einzige Gruppe definiert werden:



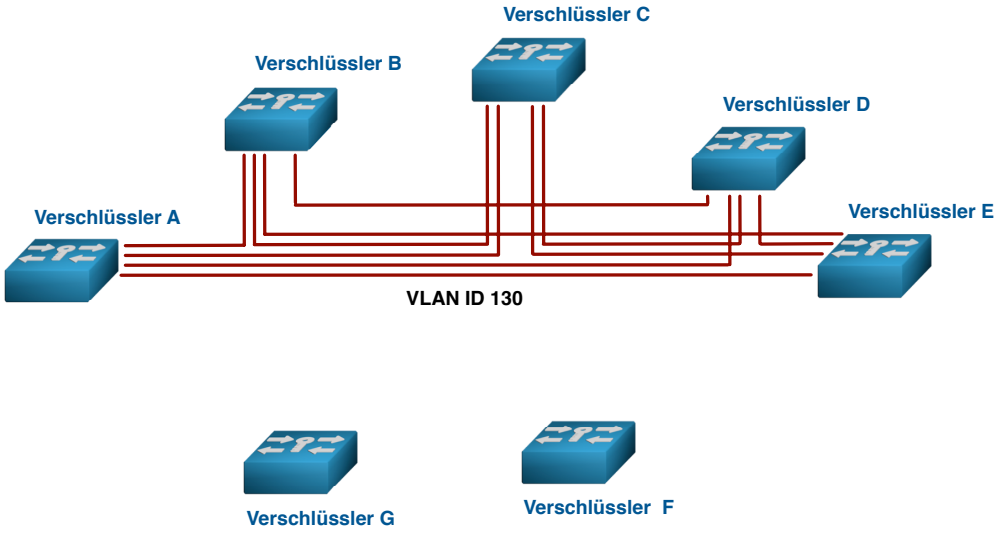
Oder man definiert jede einzelne Verbindung als eigene Gruppe:



Bei Multipunkt-zu-Multipunkt-Netzwerken erlauben Gruppenschlüsselsysteme das Schichten unterschiedlicher Gruppen. So kann beispielsweise eine Gruppe aus den Mitgliedern eines VLANs bestehen. Deckt dieses VLAN alle Standorte ab, so sind auch alle Standorte Gruppenmitglieder, ausser man schliesst einzelne Standorte explizit aus, obwohl sie Mitglieder des VLANs umfassen.



Deckt ein VLAN nur einige der Standorte ab, so sind nur diese Standorte Mitglied dieser Gruppe.



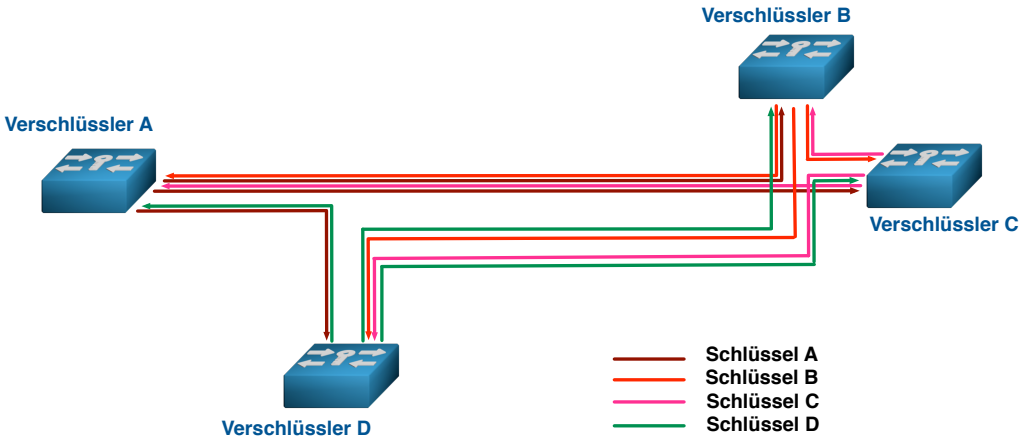
Multipunkt-Verbindungen entsprechen oft Gruppen, die durch Broadcast-Domains verbunden oder getrennt sind. Innerhalb einer Gruppe wird sämtlicher Datenverkehr mit dem gleichen Schlüssel verschlüsselt. Eine Unterscheidung zwischen Unicast-, Multicast- und Broadcast-Frames ist nicht nötig.

Leistungsfähige Gruppenschlüsselsysteme erlauben die Etablierung der Gruppenzugehörigkeit durch Parameter wie VLAN-IDs. Solche Gruppenschlüsselsysteme verwenden in der Regel einen Key Server, der redundant ausgelegt ist. Der Key Server sorgt dafür, dass jeder Verschlüssler die Gruppenschlüssel erhält, welche für die hinter ihm befindlichen Geräte benötigen, um mit den anderen Gruppenmitgliedern an anderen Standorten kommunizieren zu können. Der Key Server muss unter anderem auch sicherstellen, dass bei Änderungen der Gruppenzusammensetzung ein neuer Schlüssel erstellt wird. Mit dem neuen Schlüssel kann der alte Datenverkehr nicht entschlüsselt werden und mit dem alten Schlüssel kann der neue Datenverkehr nicht entschlüsselt werden.

Bei Ethernet drängt es sich auf, die Gruppen nach VLAN-IDs zu organisieren, da in der Regel Firmennetze die Broadcast-Domains durch VLANs eingrenzen und so auch das Netzwerk segmentieren. Bei einer Gruppenverschlüsselung, die nach VLANs organisiert ist, wird diese Segmentierung auch für die Verschlüsselung verwendet und stellt so auch eine kryptographische Trennung der VLANs her.

Nicht alle Gruppenschlüsselsysteme verschlüsseln jeweils den Datenverkehr bidirektional mit dem gleichen Schlüssel. Es ist auch möglich unidirektionale Schlüssel zu verwenden. Bei solchen Gruppenschlüsselsystemen bestimmt jeweils der absendende Verschlüssler den Schlüssel und verteilt ihn an alle Gruppenmitglieder, die zu seiner Gruppe gehören. Da jedes Gruppenmitglied auch absendender Verschlüssler ist, verteilt jeder Verschlüssler den

Schlüssel, mit dem er die Daten verschlüsselt an die anderen. Jeder Verschlüssler ist dabei Key Server für seine Schlüssel.



Jeder der Plattform-Hersteller verwendet ein unterschiedliches Schlüsselsystem und damit einen anderen Lösungsansatz. Grundsätzlich kann festgehalten werden, dass einige Schlüsselsysteme das Netzwerk hierarchisch als flach behandeln, während andere bestehende Hierarchien und Strukturen im Netz berücksichtigen können. Eine Multi-Mandantenfähigkeit lässt sich nur unter Berücksichtigung von Hierarchien und Strukturen mit Gruppenschlüsseln und verteilten Key Servern erreichen.

8. Netzwerkunterstützung

8.1 Bump-in-the-Wire-Deployment

Können die Verschlüssler ohne Änderung der Netzwerkinfrastruktur einfach in das bestehende Netzwerk eingeschlauft werden, so wird dies als „Bump-in-the-Wire Deployment“ bezeichnet.

8.2 Jumbo-Frames

Die Unterstützung von Jumbo Frames (>1500 bytes) ist eigentlich eine Selbstverständlichkeit, die bei jedem marktgängigen Ethernet-Adapter vorhanden ist.

http://en.wikipedia.org/wiki/Jumbo_frames

8.3. Ethernet Flow Control

Ethernet Flow Control unterstützt verlustfreie Übertragung, indem es den Verkehrsfluss reguliert, damit Frames im Falle von Verstopfungen nicht weggeworfen werden. Dies erfolgt über das Stoppen und Wiederaufnehmen der Übertragung zwischen zwei Geräten bei einem vollduplex Ethernet-Netzwerk. Die Kontrolle des Verkehrsflusses verhindert das Überlaufen der Buffer der beteiligten Geräte, das zu einem Wegwerfen von Frames führen würde. Mit dem PAUSE-Befehl kann die Übermittlung von Daten kurzfristig angehalten und eine Verstopfung verhindert werden.

http://en.wikipedia.org/wiki/Ethernet_flow_control
http://datacenteroverlords.com/2013/02/02/ethernet-congestion-drop-it-or-pause-it/

8.4 Fragmentierung

Fragmentierung/Defragmentierung auf Ethernet-Ebene funktioniert anders als die Fragmentierung von IP-Paketen. Sie wird da gebraucht, wo der Verschlüsselungsmodus die Frame-Grösse ändert und die resultierende Grösse eine MTU von 1500 Bytes, bzw. eine andere, vom Netzwerk vorgegebene MTU, überschreitet. Einen zusätzlichen Overhead von bis zu 32 Bytes vertragen aber in der Regel die meisten Carrier Ethernet-Infrastrukturen klaglos. Zudem können vorgelagerte Traffic Shaper die Frame-Grösse auf das erlaubte Maximum reduzieren. Bei der Kommunikation von IPv6-Geräten erfolgt die Reduktion automatisch.

8.5 Dead Peer Detection

Die Funktion „Dead Peer Detection“ erlaubt es dem Verschlüssler herauszufinden und zu melden, wenn die Gegenstelle ausser Betrieb fällt.

8.6 Optical Loss Pass-Through

Optical Loss-Pass-Through (auch als LLR – Link Loss Return - bezeichnet) dient dem Entdecken von Link-Problemen auf dem Fiberport. Erhält der Empfänger des Fiberports kein gültiges Link-Signal, so sistiert der Sender des Fiberports seine Tätigkeit. Die Funktion ermöglicht so einem Switch oder Router durch den Verschlüssler zu sehen, ob die Verbindung zum Switch oder Router hinter dem Verschlüssler auf der Gegenseite der Verbindung funktioniert.

8.7 Link Loss Carry Forward

Bei Link Loss Carry Forward wird nur ein Link-Signal geschickt, wenn ein Link-Signal empfangen wird. Der Verlust des Links wird so an den Switch weitergereicht, damit der Fehler unmittelbar bekannt wird. So schickt der Ausgangsport des Verschlüsslers nur ein Link-Signal, wenn er auf dem Eingangsport ein Link-Signal erhält und der Eingangsport des Verschlüsslers schickt nur ein Link-Signal wenn er auf dem Ausgangsport ein Link-Signal erhält. Link Loss Carry Forward kann sowohl für fiberoptische als auch für kupferbasierte Netze eingesetzt werden.

9. System Management

Unter dieser Kategorie werden die wichtigsten Funktionalitäten in Bezug auf das System Management aufgeführt.

9.1 Out-of-Band-Zugriff

Die Verschlüssler müssen konfiguriert und überwacht werden können. Für den Out-of-Band-Zugriff stehen dafür ein separater Ethernet-Port und eine serielle Schnittstelle zur Verfügung.

http://en.wikipedia.org/wiki/Out-of-band_management

9.2 In-Band-Zugriff

Für den in-band-Zugriff auf die Verschlüssler über das Netzwerk können unterschiedliche Methoden wie SSH (Secure Shell), TLS, Corba/TLS, SNMP oder proprietäre Protokolle verwendet werden

http://en.wikipedia.org/wiki/Secure_Shell

9.3 Slots und Ports

SD-Card-Slot und USB-Port erlauben Konfigurationsdaten und Updates lokal einzulesen.

9.4 SNMP

Für die Überwachung des Geräts im Netzwerk wird von allen Herstellern SNMP verwendet, wobei SNMP erst ab Version 2c als halbwegs sicher gilt, bzw. die für die Überwachung von High Speed Netzwerkkomponenten notwendigen erweiterten 64 Bit Zähler zur Verfügung stellt. Eine Verschlüsselung ist erst ab Version 3 vorhanden.

http://en.wikipedia.org/wiki/SNMP

Für die Überwachung des Link-Status muss der Verschlüssler laufend seinen Betriebszustand bekannt geben. Diese Daten können von entsprechender Software gelesen und aufgearbeitet werden, so dass der aktuelle Link-Status überwacht werden kann. Dies kann u.a. mittels SNMP Traps für den Uplink und den Downlink erfolgen. Zur Erfüllung dieses Kriteriums muss alle zur Überwachung des Link-Status nötige Software dem Verschlüssler beiliegen. Das reine Zurverfügungstellen der SNMP Traps ist nicht genügend.

9.5 Logs

Im Event Log werden sämtliche Vorfälle abgespeichert. Das Event Log ist bei einem Verschlüssler lokal.

Das Audit Log zeichnet für das Audit relevante Vorgänge auf und ist bei einem Verschlüssler lokal.

Syslog zeichnet Systemvorgänge auf. Für die Übermittlung zwischen Syslog-Server und Verschlüssler wird UDP verwendet, so dass eine Übertragung und Registrierung der Daten nicht garantiert ist. Aus diesem Grund brauchen die Verschlüssler die oben erwähnten lokalen Event und Audit Logs. Syslog-Support erlaubt unter anderem das Einbinden in zentralisierte Log-Management-Umgebungen.

http://en.wikipedia.org/wiki/Computer_data_logging
http://en.wikipedia.org/wiki/Audit_trail
http://en.wikipedia.org/wiki/Syslog

10. Unit

10.1 Rack Unit

Die Höhe der Unit bezieht sich auf den Platz, den sie im 19“-Rack benötigt. Dies hat wiederum einen Einfluss auf die Betriebskosten. Ein 2U-Gehäuse verursacht z.B. höhere Betriebskosten als ein 1U-Gehäuse.

http://en.wikipedia.org/wiki/Rack_unit

10.2 Gerätezugriff

Der Zugriff auf die wichtigsten Anschlüsse sollte bei den Geräten vorne sein. Probleme kann es sonst dort geben, wo ein Display auf der Vorderseite des Gehäuses ist, die Netzwerkanschlüsse aber hinten sind.

10.3 Redundante Netzteile

Verschlüssler sind wichtige Teile der IT-Infrastruktur. Es ist durchaus üblich solche Geräte an zwei unabhängige Stromkreise anzuschliessen, so dass der nahtlose Weiterbetrieb beim Ausfall des einen Stromkreises möglich ist. Redundante Netzteile können an zwei unabhängige Stromkreise angeschlossen werden.
Sind sie „hot-swappable“, so können die Netzteile auch im laufenden Betrieb ausgetauscht werden. Die verwendeten Netzteile haben in der Regel eine MTBF die deutlich über der MTBF der Geräte liegt, so dass der effektive Ausfall eines Netzteils statistisch äusserst unwahrscheinlich ist.

http://en.wikipedia.org/wiki/Uninterruptible_power_supply

10.4 Mean Time between Failures

Die MTBF zeigt die theoretische Dauer zwischen zwei Ausfällen. Je höher der Wert, desto tiefer die Betriebskosten. Dies führt zu inflationären Tendenzen bei den Angaben.

http://en.wikipedia.org/wiki/MTBF

10.5 Geräteschutz

Bei den Gehäusen wird unterschieden zwischen „tamper evident“ und tamper resistent“, wobei „tamper resistent“ deutlich aufwändiger zu bewerkstelligen und entsprechend teurer ist. Für „tamper evident“ kann bereits ein Siegel genügen, das aus einem Kleber besteht, zumindest ist das bei FIPS so.

http://en.wikipedia.org/wiki/Tamper_proof
http://en.wikipedia.org/wiki/Tamper_evident

10.6 Sicherheitsstandards und Sicherheitszulassungen

Es gibt unterschiedliche IT-Sicherheitsrichtlinien, die für Produkte wie Verschlüsslergelten. Einige sind international, einige sind national und andere sind international mit nationalen Kriterien. Einige Länder haben eigene Anforderungen für IT-Sicherheit im Zusammenhang mit Verschlüsslern definiert. In diesen Ländern ist die entsprechende Zertifizierung Voraussetzung für Verkäufe an die Regierung oder die öffentliche Hand. Die meisten dieser Zertifizierungen bringen dem Kunden nur einen beschränkten Nutzen, da oft weder die zu erfüllenden Vorgaben noch der Umfang der Überprüfung eine ausreichende Sicherheit gewährleisten. Es bleibt dem Kunden überlassen, sowohl das Schutzprofil wie auch den Zertifizierungsbericht für ein Produkt im Detail zu lesen und mit seinen eigenen Sicherheitsanforderungen zu vergleichen.

Eine Zertifizierung der Geräte durch eine staatliche Organisation für Regierungsgebrauch ist in der Regel deutlich werthaltiger als die Zertifizierung durch einen unabhängigen kommerziellen Dienstleister, denn die Geräte müssen den Anforderungen von Regierungen für die eigenen klassifizierten Netzwerke genügen. Die absolute Sicherheit garantieren in der Realität aber auch diese Zertifizierungen nicht, doch sind die Geräte in diesem Fall meistens schon bei der Entwicklung von Mathematikern und Kryptographie- und Sicherheitsexperten begleitet und nachher noch einmal bis ins Detail geprüft worden. Die benötigte kombinierte Fachkompetenz ist bei den meisten kommerziellen Dienstleistern meist nicht im nötigen Umfang vorhanden. Das deutsche Bundesamt für Sicherheit in der Informationstechnik gilt für Produkte, die nach den Regeln des IT-Grundschutzes für den Regierungsgebrauch zertifiziert werden, als besonders anspruchsvoll. Entscheidend bleibt für alle Zertifizierungen, wer, was, wo, wie und nach welchen Vorgabengeprüft hat.

Rahmenwerke, Standards und Richtlinien gibt es von unterschiedlichen nationalen und internationalen Organisationen. Es ist in der Regel von Vorteil, wenn ein Gerät nicht nur die nationalen Standards eines einzelnen Landes, sondern eine Mehrzahl an international gebräuchlichen Standards unterstützt.

http://en.wikipedia.org/wiki/Common_Criteria
http://en.wikipedia.org/wiki/Bundesamt_für_Sicherheit_in_der_Informationstechnik
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306
http://en.wikipedia.org/wiki/FIPS_140
http://www.etsi.org/technologies-clusters/clusters/security

10.7 Sicherheitsrelevante Zulassungen

Nebst den eigentlichen Sicherheitszulassungen gibt es auch sicherheitsrelevante Zulassungen. Diese betreffen vorwiegend den Bereich operationeller Sicherheit und Abstrahlung.

http://en.wikipedia.org/wiki/European_standards
http://en.wikipedia.org/wiki/List_of_EN_standards
http://en.wikipedia.org/wiki/FCC

11. Management-Software

Die Verschlüssler werden mit der nötigen Management-Software ausgeliefert. Die Software widerspiegelt die Funktionalität des Verschlüsslers und fällt deshalb je nach Anbieter unterschiedlich aus.

11.1 Management Access

Unterschiedliche Leute, z.B. IT Security und Netzwerkadministration, brauchen Zugriff auf Funktionen des Verschlüsslers. Der Zugriff muss auf autorisierte Benutzer beschränkt sein. Den Benutzern werden Rollen zugewiesen, die definieren, was sie sehen dürfen und auf was sie zugreifen dürfen. Die Rollen können hierarchisch strukturiert sein. Die strikte Trennung der Benutzer ermöglicht, dass mehrere Benutzer gleichzeitig auf das System zugreifen können, ohne dass zusätzliche Sicherheitsrisiken geschaffen werden.

11.2 Device Management

Das Device Management dient der Konfiguration, der Überwachung und der Verwaltung des Verschlüsslers.

11.3 Certificate Authority und Management

Einige der Hersteller kombinieren die Software für Device Management mit einer Certificate Authority, so dass die benötigten X.509-Zertifikate unabhängig von einer vorhandenen CA-Struktur herstellt werden können.
Einige Hersteller verwenden nicht standardkonforme X.509 Zertifikate, so dass eine vorhandene CA-Infrastruktur nicht für die Verschlüsselungsgeräte mitgenutzt werden kann.

http://en.wikipedia.org/wiki/Certificate_authority

11.4 Key Management

Das Key Management dient einerseits der Zuteilung der Anfangsgeheimnisse und andererseits dem Erzeugen und Verwalten der verwendeten Master- und Session Keys.

http://en.wikipedia.org/wiki/Key_management

12. Preis und Garantie

12.1 Preis

Gezeigt werden die Listenpreise. Die Projektpreise sehen je nach Projektgrösse anders aus. Die Preise sind nicht zwangsläufig proportional zur Funktionalität und Qualität eines Geräts. Einige Hersteller kompensieren überhöhte Listenpreise mit entsprechenden Rabatten, während andere mit realistischen Listenpreisen und entsprechend tiefen Rabattstufen arbeiten. Am Schluss ist der bezahlte Preis entscheidend und nicht die Höhe des gewährten Rabattes. Die Preise sind mittlerweile in einer Region angelangt, die eine Kaufentscheidung deutlich vereinfachen. Für 19"-Geräte mit einem vollduplex Durchsatz von 1G liegen sie zwischen €13'000 und €20'000 und für 10G vollduplex zwischen €24'000 und €30'000. Die Preise für 100M-Lösungen liegen bei €6'000. Kompaktgeräte mit externem Netzteil liegen je nach Anbieter zwischen 20-50% unter den Preisen für 19"-Geräte mit redundanter Stromversorgung. Die Grösse des Preisunterschieds hängt dabei auch davon ab, ob sich der Preis des 19"-Geräts am oberen Ende der marktüblichen Preisspanne bewegt. Diese Preise sind für dedizierte Komplettsysteme, inklusive Authentisierung, Schlüsselverwaltung und Echtzeit-Verschlüsselung.

12.2 Betriebskosten

Der zu bezahlende Gerätepreis ist aber ein Teil der Kosten. Bei einer durchschnittlichen Einsatzdauer von 6-7 Jahren sind die Betriebskosten ein substantieller Teil der Gesamtkosten. Die Betriebskosten selbst bestehen einerseits aus den direkten Betriebskosten des Geräts (Garantiedauer, Garantieumfang, Garantieerweiterung, SLA, etc.) und andererseits aus den Leitungskosten. Geräte, welche eine Linienkonsolidierung erlauben, können erheblich tiefere Leitungskosten nach sich ziehen. Werden die Kosten nach betriebswirtschaftlichen Kriterien berechnet, so sind die Leitungskosten ein wichtiger Kostenbestandteil.
Die Betriebskosten sind schwerer zu berechnen als die Gerätekosten, da auch Opportunitätskosten miteinbezogen werden müssen. So z.B. wenn über eine längere Distanz dedizierte Linien verwendet werden müssen, weil der Verschlüssler nicht mit einem kostengünstigeren Transportnetzwerk harmoniert.

12.3 Garantiedauer und Garantieumfang

Auch bei der Garantiedauer und beim Garantieumfang ist die Kostenstruktur je nach Anbieter verschieden. Dies kann zu versteckten Unterschieden von 10%-20% des Preises ausmachen.

Der Dank des Autors gilt den vielen Leuten, die diese Marktübersicht erst möglich gemacht haben:

Michael Braun (atmedia), Mike Churillo (ViaSat), Julian Fay (Senetas), Carsten Fischer (Secunet), Joerg Friedrich (atmedia), Gabi Gerber (Security Interest Group Switzerland/SIGS), Sharon Ginga (Gemalto), Andreas Graubner (Rohde & Schwarz), Harald Herrmann (Rohde & Schwarz), Christoph Hugenschmidt (Inside-IT), Emil Isaakian (ViaSat), Felix Jaggi, Ronald Kuhls (Rohde & Schwarz), Stephan Lehmann, Franjo Majstor, Todd Moore (Gemalto), Ivan Pepelnjak (IPSpace.net), Grégoire Ribordy (IDQuantique), Kelly Richdale (IDQuantique), David Ristow (Secunet), Peter Rost (Rohde & Schwarz), Gilles Trachsel (IDQuantique), Patrick Trinkler (IDQuantique), Joe Warren (Thales), John Weston (Senetas) sowie den unzähligen anderen, die dieses Projekt in der einen oder anderen Form unterstützt haben.

Diese Marktübersicht gibt es sowohl in der vorliegenden Kurz- wie auch in einer Vollversion. In der Kurzversion fehlen mehrere Bereiche, darunter die Sicherheit der Kontrollebene, die Optionen für den Schlüsselaustausch, die detaillierte Beschreibung des Schlüsselaufbaus, des Schlüsselaustausches und der Schlüsselsysteme der drei wichtigsten Plattformen, der bei Traffic Flow Security verwendeten Mechanismen und schliesslich der Positionierungsmöglichkeiten der Verschlüssler im Netzwerk. Die Tabellen der Vollversion werden zudem zur besseren Übersicht als Excel-Datei zur Verfügung gestellt.
Die kostenpflichtige Vollversion steht qualifizierten Personen und Organisationen auf Anfrage zur Verfügung.

Atmedia

	Virtual Appliance	50/100 compact	1G compact	100M	1G	10G	40G	100G
Line Interface/Supported Line Rates								
							Roadmap Q2 2017	Roadmap Q4 2017
10 Mbs	✔	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP			
100 Mps	✔	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+		
1 Gbps	✔	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+	✔/QSFP	
10 Gbps	✔				✔/SFP	✔/SFP+	✔/QSFP	✔/QSFP28
25Gps	✔						✔/QSFP	✔/QSFP28
40 Gbps	✔						✔/QSFP	✔/QSFP28
100 Gbps	✔							✔/QSFP28
Virtual Appliance	✔							
Supported Network Topologies								
Point-to-Point (P2P)	✔	✔	✔	✔	✔	✔	✔	✔
Point-to-Multipoint (P2MP)	✔	✔	✔	✔	✔	✔	✔	✔
Multipoint (MP)	✔	✔	✔	✔	✔	✔	✔	✔
Supported Metro Ethernet Topologies								
Port-based								
Ethernet Private Line (EP-Line)	✔	✔	✔	✔	✔	✔	✔	✔
Ethernet Private Tree (EP-Tree)	✔	✔	✔	✔	✔	✔	✔	✔
Ethernet Private LAN (EP-LAN)	✔	✔	✔	✔	✔	✔	✔	✔
VLAN-based								
Ethernet Virtual Private Line (EVP-Line)	✔	✔	✔	✔	✔	✔	✔	✔
Ethernet Virtual Private Tree (EVP-Tree)	✔	✔	✔	✔	✔	✔	✔	✔
Ethernet Virtual Private LAN (EVP-LAN)	✔	✔	✔	✔	✔	✔	✔	✔
Supported Networks (Encryption)								
Ethernet	✔	✔	✔	✔	✔	✔	✔	✔
MPLS	✔	✔	✔	✔	✔	✔	✔	✔
IP v4/v6	✔	✔	✔	✔	✔	✔	✔	✔
Supported Networks (Transport of Encrypted Frame)								
Ethernet (native)	✔	✔	✔	✔	✔	✔	✔	✔
MPLS (EoMPLS)	✔	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6	✔	✔	✔	✔	✔	✔	✔	✔
TCP	✔	✔	✔	✔	✔	✔	✔	✔
UDP	✔	✔	✔	✔	✔	✔	✔	✔
Supported Usage Scenarios								
Single tenant	✔	✔	✔	✔	✔	✔	✔	✔
Multi-tenant	✔	✔	✔	✔	✔	✔	✔	✔
Self-managed	✔	✔	✔	✔	✔	✔	✔	✔
Managed encryption service	✔	✔	✔	✔	✔	✔	✔	✔
Managed security service	✔	✔	✔	✔	✔	✔	✔	✔
Platform								
Platform used								
Mainboard/Firmware	atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia
Key Management	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia

Atmedia

Data Plane Encryption Standard and Processing

Encryption Standard									
	Block Cipher	AES	AES	AES	AES	AES	AES	AES	AES
	Preferred Mode of Operation	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Alternative Mode of Operation								
	Key Length (in bit)	256	256	256	256	256	256	256	256
Processing Method									
	cut-through	✔	✔	✔	✔	✔	✔	✔	✔
	store&forward	✔	✔	✔	✔	✔	✔	✔	✔
Encryption Hardware									
	FPGA		✔	✔	✔	✔	✔	✔	✔
	ASIC	✔							
	CPU	✔							
Latency									
Latency P2P Mode	cut-through	N/A	<42µs	<8µs	<42µs	<8µs	<4µs	<4µs	<2µs
	store & forward	N/A	<48µs	<9µs	<48µs	<9µs	<4µs	<4µs	<2µs
Latency MP Mode	cut-through	N/A	<42µs	<8µs	<42µs	<8µs	<4µs	<4µs	<2µs
	store & forward	N/A	<48µs	<9µs	<48µs	<9µs	<4µs	<4µs	<2µs

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)		✔	✔	✔	✔	✔	✔	✔	✔
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	Replay protection	✔	✔	✔	✔	✔	✔	✔	✔
	Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s
	Counter length (in bytes)	8	8	8	8	8	8	8	8
	Frame overhead (unauthenticated encryption)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Frame overhead (authenticated encryption)	18/26	18/26	18/26	18/26	18/26	18/26	18/26	18/26
	Ethernet multi-hop support	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Transport (Payload only)		✔	✔	✔	✔	✔	✔	✔	✔
	Max. number of peers	1000	1000	1000	1000	1000	1000	1000	1000
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Max. number of VLAN IDs	unlimited	256	unlimited	256	unlimited	256	unlimited	256
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	Replay protection	✔	✔	✔	✔	✔	✔	✔	✔
	Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s
	Definable encryption offset (fixed)	✔	✔	✔	✔	✔	✔	✔	✔
	Variable encryption offset	✔	✔	✔	✔	✔	✔	✔	✔
	Adaptive encryption offset based on frame content	✔	✔	✔	✔	✔	✔	✔	✔
	Ethertype mutation (unauthenticated encryption only)	✔	✔	✔	✔	✔	✔	✔	✔
	Counter length (in bytes)	8	8	8	8	8	8	8	8
	Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Frame overhead authenticated encryption (AE)	18/26	18/26	18/26	18/26	18/26	18/26	18/26	18/26
	Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	✔
Tunnel (Ethernet over Ethernet)		✔	✔	✔	✔	✔	✔	✔	✔
	Max. number of peers	32	32	32	32	32	32	32	32
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	Replay protection	✔	✔	✔	✔	✔	✔	✔	✔
	Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s
	Counter length (in bytes)	8	8	8	8	8	8	8	8
	Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Frame overhead authenticated encryption (AE)	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*
	Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	✔

*IMIX=100%

Atmedia

Ethernet over IP (EoIP)									
Tunnel (Ethernet over IP)	✔	✔	✔	✔	✔	✔	✔	✔	
Supported transmission protocols (UDP/TCP)	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	
Max. number of peers	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM	
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16	
Replay protection	✔	✔	✔	✔	✔	✔	✔	✔	
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
Counter length (in bytes)	8	8	8	8	8	8	8	8	
Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
Frame overhead authenticated encryption (AE)	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*	*IMIX=100%
Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	✔	
Native IP Encryption									
Supported IP versions									
IPv4	✔	✔	✔	✔	✔	✔	✔	✔	
IPv6	✔	✔	✔	✔	✔	✔	✔	✔	
Supported transmission protocols									
TCP	✔	✔	✔	✔	✔	✔	✔	✔	
UDP	✔	✔	✔	✔	✔	✔	✔	✔	
Transport Tunnel Mode									
Mximum number of peers	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Maximum number of IP addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Maximum number of multicast groups	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM	
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16	
Additional Authenticated Data (header)	✔	✔	✔	✔	✔	✔	✔	✔	
Replay Protection	✔	✔	✔	✔	✔	✔	✔	✔	
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
Counter length (in bytes)	8	8	8	8	8	8	8	8	
Packet overhead authenticated encryption (AE)	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	
Selective Encryption									
Based on MAC Address	✔	✔	✔	✔	✔	✔	✔	✔	
Based on VLAN ID	✔	✔	✔	✔	✔	✔	✔	✔	
Based on Ethertype	✔	✔	✔	✔	✔	✔	✔	✔	
Based on Multicast Group	✔	✔	✔	✔	✔	✔	✔	✔	
Based on Presence of MPLS Tag	✔	✔	✔	✔	✔	✔	✔	✔	
Based on IP Address	✔	✔	✔	✔	✔	✔	✔	✔	
Combination of multiple selection criteria	✔	✔	✔	✔	✔	✔	✔	✔	
Mixed Ethernet, MPLS, EoIP and IP Support									
Based on VLAN ID									
MPLS	✔	✔	✔	✔	✔	✔	✔	✔	
EoIP	✔	✔	✔	✔	✔	✔	✔	✔	
IP	✔	✔	✔	✔	✔	✔	✔	✔	
Based on presence of MPLS tag									
MPLS	✔	✔	✔	✔	✔	✔	✔	✔	
EoIP	✔	✔	✔	✔	✔	✔	✔	✔	
IP	✔	✔	✔	✔	✔	✔	✔	✔	
Based on VLAN ID and presence of MPLS tag									
MPLS	✔	✔	✔	✔	✔	✔	✔	✔	
EoIP	✔	✔	✔	✔	✔	✔	✔	✔	
IP	✔	✔	✔	✔	✔	✔	✔	✔	
Traffic Masking									
Traffic Flow Security	N/A**	✔	✔	✔	✔	✔	✔	✔	

Atmedia

Auto-discovery									
Auto-discovery of network encryptors		✔	✔	✔	✔	✔	✔	✔	✔
Auto-discovery of key servers		✔	✔	✔	✔	✔	✔	✔	✔
Auto-discovery of VLANs		✔	✔	✔	✔	✔	✔	✔	✔
Disabling of auto-discovery		✔	✔	✔	✔	✔	✔	✔	✔
Key Server									
Integrated Key Server		✔	✔	✔	✔	✔	✔	✔	✔
Support for external Key Server		✔	✔	✔	✔	✔	✔	✔	✔
External Key Server									
Support for multiple distributed Key Servers		✔	✔	✔	✔	✔	✔	✔	✔
Support for fail-over to back-up Key Server		✔	✔	✔	✔	✔	✔	✔	✔
Autonomous operation		✔	✔	✔	✔	✔	✔	✔	✔
Key Management									
Key Generation and Storage									
Hardware Random Number Generation		with SC/HSM	✔	✔	✔	✔	✔	✔	✔
Tamper Security Key Storage (tamper-evident or tamper-proof)		with SC/HSM: TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Asymmetric Key Algorithms (Public Key Cryptography)									
RSA									
	Key length	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Elliptic Curve Cryptography (ECC)									
	Key length	512/521	512/521	512/521	512/521	512/521	512/521	512/521	512/521
Supported Curves:									
	NIST	✔	✔	✔	✔	✔	✔	✔	✔
	Brainpool	✔	✔	✔	✔	✔	✔	✔	✔
	Custom Curves	✔	✔	✔	✔	✔	✔	✔	✔
Hash Algorithms									
SHA-2	Key length	512	512	512	512	512	512	512	512
CBC-MAC-GCM	Key length	256	256	256	256	256	256	256	256
Device Authentication									
Symmetric Signature: Pre-shared Key (PSK)		✔	✔	✔	✔	✔	✔	✔	✔
	Maximum number of PSKs per encryptor	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)
	Key length	256	256	256	256	256	256	256	256
Asymmetric Signature: Certificate		optional	optional	optional	optional	optional	optional	optional	optional
	Maximum number of certificates per encryptor	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)
	Key lenght	512	512	512	512	512	512	512	512
Ad-hoc authentication of peers (manual)		✔	✔	✔	✔	✔	✔	✔	✔
Signature key protocol		AES-MAC/ECDSA***	AES-MAC/ECDSA***	AES-MAC/ECDSA***	AES-MAC/ECDSA***	AES-MAC/ECDSA***	AES-MAC/ECDSA***	AES-MAC/ECDSA***	AES-MAC/ECDSA***
Key Agreement and Key Exchange									
Master Key (KEK) Agreement		ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****
Master Key (KEK) Exchange Protocol		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Automatic Change of Master Key		✔	✔	✔	✔	✔	✔	✔	✔
Minimum suggested Time Interval for Master Key Change (min)		60	60	60	60	60	60	60	60
Separate Master Key (KEK) per site		✔	✔	✔	✔	✔	✔	✔	✔
Separate Master Key (KEK) per group		✔	✔	✔	✔	✔	✔	✔	✔
Session Key (DEK) Exchange Agreement		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Session Key (DEK) Exchange Protocol		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Automatic Change of Session Keys		✔	✔	✔	✔	✔	✔	✔	✔
Minimum Time Interval for Session Key Change (min)		1	1	1	1	1	1	1	1

***ECDSA optional for use with optional certificates

*****NIST, Brainpool or custom curves with 256 to 521 bit length

Atmedia

Key System									
Point-to-Point Key System									
Supported key system									
	Pairwise	✔	✔	✔	✔	✔	✔	✔	✔
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:									
	MAC Address	✔	✔	✔	✔	✔	✔	✔	✔
	VLAN ID	✔	✔	✔	✔	✔	✔	✔	✔
	Port	✔	✔	✔	✔	✔	✔	✔	✔
	Group	✔	✔	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔	✔	✔
Point-to-Multipoint Key System									
Supported key systems:									
	Pairwise	✔	✔	✔	✔	✔	✔	✔	✔
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:									
	MAC Address	✔	✔	✔	✔	✔	✔	✔	✔
	VLAN ID	✔	✔	✔	✔	✔	✔	✔	✔
	Port	✔	✔	✔	✔	✔	✔	✔	✔
	Group	✔	✔	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔	✔	✔
Multipoint Key System									
Supported key systems:									
	Pairwise	✔	✔	✔	✔	✔	✔	✔	✔
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
	Mixed (pairwise unicast, group multicast)	✔	✔	✔	✔	✔	✔	✔	✔
Key assignment based on:									
	MAC address (pairwise and mixed)	✔	✔	✔	✔	✔	✔	✔	✔
	Multicast groups (mixed)	✔	✔	✔	✔	✔	✔	✔	✔
	VLAN ID (group)	✔	✔	✔	✔	✔	✔	✔	✔
	Port	✔	✔	✔	✔	✔	✔	✔	✔
	Group (group)	✔	✔	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔	✔	✔
	IP Multicast Group	✔	✔	✔	✔	✔	✔	✔	✔
Individual key per multicast group		✔	✔	✔	✔	✔	✔	✔	✔
Individual key per broadcast group (VLAN ID)		✔	✔	✔	✔	✔	✔	✔	✔
Group Key System Specifics									
Additional separate authentication per group		✔	✔	✔	✔	✔	✔	✔	✔
Group Membership Definition									
	Multicast group membership	✔	✔	✔	✔	✔	✔	✔	✔
	Individual membership	✔	✔	✔	✔	✔	✔	✔	✔
	Network membership	✔	✔	✔	✔	✔	✔	✔	✔
	VLAN membership	✔	✔	✔	✔	✔	✔	✔	✔
	Trunked VLAN membership	✔	✔	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔	✔	✔
Exclusion									
	MAC address	✔	✔	✔	✔	✔	✔	✔	✔
	VLAN ID	✔	✔	✔	✔	✔	✔	✔	✔
	Frames with MPLS tag	✔	✔	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔	✔	✔
	IP Muticast Group	✔	✔	✔	✔	✔	✔	✔	✔
Group Key Distribution									
	Unicast (unique KEK per group member)	✔	✔	✔	✔	✔	✔	✔	✔
	Broadcast (same KEK for all group members)	✔	✔	✔	✔	✔	✔	✔	✔

Atmedia

Network Support									
Bump in the Wire deployment		✔	✔	✔	✔	✔	✔	✔	✔
Jumbo Frame Support		✔	✔	✔	✔	✔	✔	✔	✔
Ethernet Flow Control via PAUSE		✔	✔	✔	✔	✔	✔	✔	✔
Ethernet Fragmentation/Defragmentation		✔	✔	✔	✔	✔	✔	✔	✔
	Point-to-Point	✔	✔	✔	✔	✔	✔	✔	✔
	Point-to-Multipoint	✔	✔	✔	✔	✔	✔	✔	✔
	Multipoint	✔	✔	✔	✔	✔	✔	✔	✔
Dead Peer Detection		✔	✔	✔	✔	✔	✔	✔	✔
Optical Loss Pass-Through		N/A	N/A	N/A	N/A	✔	✔	✔	✔
Link Loss Carry Forward		N/A	✔	✔	✔	✔	✔	N/A	N/A
System Configuration and Management Access									
IPv4		✔	✔	✔	✔	✔	✔	✔	✔
IPv6		✔	✔	✔	✔	✔	✔	✔	✔
Out-of-band Management		✔	✔	✔	✔	✔	✔	✔	✔
	RS-232/V.24	✔	✔	✔	✔	✔	✔	✔	✔
	Separate Ethernet port	✔	✔	✔	✔	✔	✔	✔	✔
Smart Card (Secure Card) Support		✔	✔	✔	✔	✔	✔	✔	✔
USB Port		✔						✔	✔
In-band Management		✔	✔	✔	✔	✔	✔	✔	✔
	SSH	✔	✔	✔	✔	✔	✔	✔	✔
	SNMP (read-only/read-write)	read-only	read-only	read-only	read-only	read-only	read-only	read-only	read-only
	TLS								
	Proprietary	✔	✔	✔	✔	✔	✔	✔	✔
Remote Monitoring (SNMP)		v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3
Logs									
Event Log (local)		✔	✔	✔	✔	✔	✔	✔	✔
Audit Log (local)		✔	✔	✔	✔	✔	✔	✔	✔
Syslog Support (Server)		✔	✔	✔	✔	✔	✔	✔	✔
Unit									
Height in 19" Rack		N/A	1U	1U	1U	1U	1U	1U	1U
Number of external encrypted Ethernet ports		unrestricted	1	1	1	1	1	1-4	1-4
Physical Device Access		N/A	back	back	front	front	front	front	front
Redundant Power Supply		dependent on server			✔	✔	✔	✔	✔
Redundant, hot-swappable power supply		dependent on server			✔	✔	✔	✔	✔
High Availability functionality (two-node cluster)		1:1	1:1	1:1	1:1	1:1	1:1	1:1	1:1
MTBF		N/A	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h
Tamper Security		N/A	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Security Approvals		N/A		BSI VS-NfD, NATO restricted, EU Restrint (including 2nd Evaluation by NL)				*****	*****
Safety Approvals		N/A		EN55032 Class B, FCC Part 15 Class B, ROHS					
Boot Time									
	Cold boot until operational	N/A	25s	25s	25s	25s	25s	25s	25s
	Warm boot until operational	N/A	27s	27s	27s	27s	27s	27s	27s

*****BSI VS-NfD, NATO restricted and EU Restrint planned/in preparation

Atmedia

Management Software									
User Interface									
	Native PC application	✔	✔	✔	✔	✔	✔	✔	✔
	Embedded Webapp								
	CLI	✔	✔	✔	✔	✔	✔	✔	✔
Initial Device Set-up									
	Local (out-of-band)	✔	✔	✔	✔	✔	✔	✔	✔
	Remote (out-of-band)	✔	✔	✔	✔	✔	✔	✔	✔
Device Configuration									
	Local (out-of-band)	✔	✔	✔	✔	✔	✔	✔	✔
	Remote (in-band)	✔	✔	✔	✔	✔	✔	✔	✔
	Remote (out-of-band)	✔	✔	✔	✔	✔	✔	✔	✔
Management Access									
	Role-based access	✔	✔	✔	✔	✔	✔	✔	✔
	Identity-based authentication of user	✔	✔	✔	✔	✔	✔	✔	✔
	Number of hierarchy levels	2	2	2	2	2	2	2	2
	Number of roles	5	5	5	5	5	5	5	5
	Strict internal separation of users	✔	✔	✔	✔	✔	✔	✔	✔
Device Management									
	Device Diagnostics	✔	✔	✔	✔	✔	✔	✔	✔
	Link Monitoring (SNMP)	✔	✔	✔	✔	✔	✔	✔	✔
	Connection Diagnostics	✔	✔	✔	✔	✔	✔	✔	✔
	In-band Network Diagnostics	✔	✔	✔	✔	✔	✔	✔	✔
	Remote Update/Upgrade	✔	✔	✔	✔	✔	✔	✔	✔
Certificate Authority & Management		optional	optional	optional	optional	optional	optional	optional	optional
	Certificate Creation	optional	optional	optional	optional	optional	optional	optional	optional
	Certificate Management	optional	optional	optional	optional	optional	optional	optional	optional
Key Management									
	Group creation	✔	✔	✔	✔	✔	✔	✔	✔
	Group isolation	✔	✔	✔	✔	✔	✔	✔	✔
	Key assignment	✔	✔	✔	✔	✔	✔	✔	✔
	Fail-over configuration	✔	✔	✔	✔	✔	✔	✔	✔
Price									
List Price Encryption Unit (in €)		on request	on request	on request	on request	on request	on request	on request	on request
Per external Key Server (in €); optional, no requirement		on request	on request	on request	on request	on request	on request	on request	on request
Required Management Software									
	2-10 encryptors	included	included	included	included	included	included	included	included
	11-25 encryptors	included	included	included	included	included	included	included	included
	26-50 encryptors	included	included	included	included	included	included	included	included
	51+ encryptors	included	included	included	included	included	included	included	included
Warranty Period (months)		24	24	24	24	24	24	24	24
Warranty Coverage	Parts & Work	✔	✔	✔	✔	✔	✔	✔	✔
	Basic Support (9 to 5, e-mail, phone)	on request	on request	on request	on request	on request	on request	on request	on request
	Software updates and upgrades	on request	on request	on request	on request	on request	on request	on request	on request
Warranty Extension (per year)		on request	on request	on request	on request	on request	on request	on request	on request

Gemalto

	Safenet CN4010	Safenet CN4020	Safenet CN6010	Safenet CN6100	Safenet CN8000	Safenet CN9100	Safenet CN9120
Line Interface/Supported Line Rates							
10 Mbs	✔/RJ45	✔/SFP	✔/RJ45/SFP				
100 Mps	✔/RJ45	✔/SFP	✔/RJ45/SFP				
1 Gbps	✔/RJ45	✔/SFP	✔/RJ45/SFP	✔/SFP	✔/SFP+		
10 Gbps				✔/SFP	✔/SFP+		
25Gps							
40 Gbps					✔/SFP+		
100 Gbps					✔/SFP+	✔/CFP-4	✔/QSFP-28
Virtual Appliance					up to 10 cards at up to 10G each		
Supported Network Topologies							
Point-to-Point (P2P)	✔	✔	✔	✔	✔	✔	✔
Point-to-Multipoint (P2MP)	✔	✔	✔	✔	✔	✔	✔
Multipoint (MP)	✔	✔	✔	✔	✔	✔	✔
Supported Metro Ethernet Topologies							
Port-based							
Ethernet Private Line (EP-Line)	✔	✔	✔	✔	✔	✔	✔
Ethernet Private Tree (EP-Tree)	✔	✔	✔	✔	✔	✔	✔
Ethernet Private LAN (EP-LAN)	✔	✔	✔	✔	✔	✔	✔
VLAN-based							
Ethernet Virtual Private Line (EVP-Line)	✔	✔	✔	✔	✔	✔	✔
Ethernet Virtual Private Tree (EVP-Tree)	✔	✔	✔	✔	✔	✔	✔
Ethernet Virtual Private LAN (EVP-LAN)	✔	✔	✔	✔	✔	✔	✔
Supported Networks (Encryption)							
Ethernet	✔	✔	✔	✔	✔	✔	✔
MPLS (MPLSoE)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6							
Supported Networks (Transport of Encrypted Frame)							
Ethernet (native)	✔	✔	✔	✔	✔	✔	✔
MPLS (EoMPLS)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
TCP	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
UDP	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
Supported Usage Scenarios							
Single tenant	✔	✔	✔	✔	✔	✔	✔
Multi-tenant	*	*	*	*	✔/one tenant per port	*	
Self-managed	✔	✔	✔	✔	✔	✔	✔
Managed encryption service	✔	✔	✔	✔	✔	✔	✔
Managed security service	✔	✔	✔	✔	✔	✔	✔
Platform							
Platform used							
Mainboard/Firmware	Senetas/Senetas	Senetas/Senetas	Senetas/Senetas	Senetas/Senetas	Senetas/IDQuantique	Senetas/Senetas	Senetas/Senetas
Key Management	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas

* IP support only in combination with TRANSEC and limited to P2P. Additional overhead and latency.
* Multi-tenancy support based on certificates. Requires common trust domain of CAs.

Gemalto

Data Plane Encryption Standard and Processing

Encryption Standard								
	Block Cipher	AES	AES	AES	AES	AES	AES	AES
	Preferred Mode of Operation	GCM	GCM	GCM	GCM	GCM	CTR	CTR
	Alternative Mode of Operation	CFB/CTR	CFB/CTR	CFB/CTR	CFB/CTR	CFB/CTR	GCM (Roadmap Q4 2017)	GCM (Roadmap Q4 2017)
	Key Length (in bit)	128/256	128/256	128/256	128/256	128/256	128/256	128/256
Processing Method								
	cut-through	✔	✔	✔	✔	✔		
	store&forward	*	*	*	*	*	✔	✔
Encryption Hardware								
	FPGA	✔	✔	✔	✔	✔	✔	✔
	ASIC							
	CPU							
Latency								
Latency P2P Mode	cut-through	<10µs (@1Gbps)	<10µs (@1Gbps)	<10µs	<5µs	<5µs		
	store & forward	*	*	*	*	*	<2µs	<2µs
Latency MP Mode	cut-through	<10µs (@1Gbps)	<10µs (@1Gbps)	<10µs	<5µs	<5µs		
	store & forward	*	*	*	*	*	<2µs	<2µs

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)		*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM				
	Authentication length (bytes)	16	16	16	16				
	Replay protection	✔	✔	✔	✔				
	Variable replay window (size)	256 frames	256 frames	256 frames	256 frames				
	Counter length (in bytes)	5	5	5	5				
	Frame overhead (unauthenticated encryption)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)				
	Frame overhead (authenticated encryption)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)				
	Ethernet multi-hop support	✔	✔	✔	✔				
Transport (Payload only)		✔	✔	✔	✔	✔	✔	✔	
	Max. number of peers	512	512	512	512	512	512	512	
	Max. number of MAC Addresses	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	limitation only in MAC mod
	Max. number of VLAN IDs	256	256	256	512	512	512	512	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	*GCM (Roadmap Q4 2017)	*GCM (Roadmap Q4 2017)	
	Authentication length (bytes)	16	16	16	16	16	16	16	
	Replay protection	✔	✔	✔	✔	✔	✔	✔	
	Variable replay window (size)	256 frames	256 frames	256 frames	256 frames	256 frames	256 frames	256 frames	
	Definable encryption offset (fixed)	✔	✔	✔	✔	✔	✔	✔	
	Variable encryption offset	✔	✔	✔	✔	✔	✔	✔	
	Adaptive encryption offset based on frame content	✔	✔	✔	✔	✔	✔	✔	
	Ethertype mutation	✔	✔	✔	✔	✔	✔	✔	
	Counter length (in bytes)	5	5	5	5	5	5	5	
	Frame overhead unauthenticated encryption	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	8 (CTR)	8 (CTR)	
	Frame overhead authenticated encryption (AE)	24	24	24	24	24	24*	24*	*GCM (Roadmap Q4 2017)
	Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	
Tunnel (Ethernet over Ethernet)		*	*	*	*	*	* Roadmap Q4 2017	* Roadmap Q4 2017	
	Max. number of peers	2	2	2	2				
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited				
	Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited				
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM				
	Authentication length (bytes)	16	16	16	16				
	Replay protection	✔	✔	✔	✔				
	Variable replay window (size)	256 frames	256 frames	256 frames	256 frames				
	Counter length (in bytes)	5	5	5	5				
	Frame overhead unauthenticated encryption	8 (CTR)	8 (CTR)	8 (CTR)	8 (CTR)				
	Frame overhead authenticated encryption (AE)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)				
	Ethernet multi-hop support	✔	✔	✔	✔				

* except for CN9100/CN9120 store & forward only in combination with TRANSEC and limited to P2P. Frame mode, tunnel mode and EoIP only when using TRANSEC. Frame mode not native. Additional overhead and latency.

Gemalto

Ethernet over IP (EoIP)							
Tunnel (Ethernet over IP)	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
Supported transmission protocols (UDP/TCP)	UDP/TCP	UDP/TCP	UDP/TCP	UDP/TCP			
Max. number of peers	2	2	2	2			
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited			
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited			
Integrity protection (algorithm)	GCM	GCM	GCM	GCM			
Authentication length (bytes)	16	16	16	16			
Replay protection	✔	✔	✔	✔			
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames			
Counter length (in bytes)	5	5	5	5			
Frame overhead unauthenticated encryption	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38			
Frame overhead authenticated encryption (AE)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)			
Ethernet multi-hop support	✔	✔	✔	✔			
Native IP Encryption							
Supported IP versions							
IPv4							
IPv6							
Supported transmission protocols							
TCP							
UDP							
Transport/Tunnel Mode							
Mximum number of peers							
Maximum number of IP addresses							
Maximum number of multicast groups							
Integrity protection (algorithm)							
Authentication length (bytes)							
Additional Authenticated Data (header)							
Replay Protection							
Variable replay window (size)							
Counter length (in bytes)							
Packet overhead authenticated encryption (AE)							
Selective Encryption							
Based on MAC Address	✔	✔	✔	✔	✔	✔	✔
Based on VLAN ID	✔	✔	✔	✔	✔	✔	✔
Based on Ethertype	✔	✔	✔	✔	✔	✔	✔
Based on Multicast Group	✔	✔	✔	✔	✔	✔	✔
Based on Presence of MPLS Tag							
Based on IP Address							
Combination of multiple selection criteria	✔	✔	✔	✔	✔	✔	✔
Mixed Ethernet, MPLS, EoIP and IP Support							
Based on VLAN ID							
MPLS	✔	✔	✔	✔	✔	✔	✔
EoIP							
IP							
Based on presence of MPLS tag							
MPLS							
EoIP							
IP							
Based on VLAN ID and presence of MPLS tag							
MPLS							
EoIP							
IP							
Traffic Masking							
Traffic Flow Security	✔	✔	✔	✔		Roadmap Q4 2017	Roadmap Q4 2017

Gemalto

Auto-discovery							
Auto-discovery of network encryptors	✔	✔	✔	✔	✔	✔	✔
Auto-discovery of key servers	✔	✔	✔	✔	✔	✔	✔
Auto-discovery of VLANs	✔	✔	✔	✔	✔	✔	✔
Disabling of auto-discovery	✔	✔	✔	✔	✔	✔	✔
Key Server							
Integrated Key Server	✔	✔	✔	✔	✔	✔	✔
Support for external Key Server	✔	✔	✔	✔	✔	✔	✔
External Key Server							
Support for multiple distributed Key Servers	✔	✔	✔	✔	✔	✔	✔
Support for fail-over to back-up Key Server	✔	✔	✔	✔	✔	✔	✔
Autonomous operation	✔	✔	✔	✔	✔	✔	✔
Key Management							
Key Generation and Storage							
Hardware Random Number Generation	✔	✔	✔	✔	✔/QRNG	✔QRNG	✔/QRNG
Tamper Security Key Storage (tamper-evident or tamper-proof)	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Asymmetric Key Algorithms (Public Key Cryptography)							
RSA							
Key length	2048	2048	2048	2048	2048	2048	2048
Elliptic Curve Cryptography (ECC)							
Key length	512	512	512	512	512	512	512
Supported Curves:							
NIST	✔	✔	✔	✔	✔	✔	✔
Brainpool	✔	✔	✔	✔	✔	✔	✔
Custom Curves	✔	✔	✔	✔	✔	✔	✔
Hash Algorithms							
SHA-2 Key length	512	512	512	512	512	512	512
Device Authentication							
Symmetric Signature: Pre-shared Key (PSK)							
Maximum number of PSKs per encryptor							
Key length							
Asymmetric Signature: Certificate	x.509	x.509	x.509	x.509	x.509	x.509	x.509
Maximum number of certificates per encryptor	64	64	64	64	64	64	64
Key length	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)
Ad-hoc authentication of peers (manual)							
Signature key protocol	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA
Key Agreement and Key Exchange							
Master Key (KEK) Agreement	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA
Master Key (KEK) Exchange Protocol	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas
Automatic Change of Master Key	✔	✔	✔	✔	✔	✔	✔
Minimum suggested Time Interval for Master Key Change (min)	1440	1440	1440	1440	1440	1440	1440
Separate Master Key (KEK) per site	✔	✔	✔	✔	✔	✔	✔
Separate Master Key (KEK) per group	✔	✔	✔	✔	✔	✔	✔
Session Key (DEK) Exchange Agreement	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications
Session Key (DEK) Exchange Protocol	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A
Automatic Change of Session Keys	✔	✔	✔	✔	✔	✔	✔
Minimum Time Interval for Session Key Change (min)	1	1	1	1	1	1	1

Gemalto

Key System							
Point-to-Point Key System							
Supported key system							
Pairwise	✔	✔	✔	✔	✔	✔	✔
Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:							
MAC Address	✔	✔	✔	✔	✔	✔	✔
VLAN ID	✔	✔	✔	✔	✔	✔	✔
Port	✔	✔	✔	✔	✔	✔	✔
Group	✔	✔	✔	✔	✔	✔	✔
IP Address							
Point-to-Multipoint Key System							
Supported key systems:							
Pairwise	✔	✔	✔	✔	✔	✔	✔
Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:							
MAC Address	✔	✔	✔	✔	✔	✔	✔
VLAN ID	✔	✔	✔	✔	✔	✔	✔
Port	✔	✔	✔	✔	✔	✔	✔
Group	✔	✔	✔	✔	✔	✔	✔
IP Address							
Multipoint Key System							
Supported key systems:							
Pairwise	✔	✔	✔	✔	✔	✔	✔
Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Mixed (pairwise unicast, group multicast)	✔	✔	✔	✔	✔	✔	✔
Key assignment based on:							
MAC address (pairwise and mixed)	✔	✔	✔	✔	✔	✔	✔
Multicast groups (mixed)	✔	✔	✔	✔	✔	✔	✔
VLAN ID (group)	✔	✔	✔	✔	✔	✔	✔
Port	✔	✔	✔	✔	✔	✔	✔
Group (group)	✔	✔	✔	✔	✔	✔	✔
IP Address							
IP Multicast Group							
Individual key per multicast group	✔	✔	✔	✔	✔	✔	✔
Individual key per broadcast group (VLAN ID)	✔	✔	✔	✔	✔	✔	✔
Group Key System Specifics							
Additional separate authentication per group	✔	✔	✔	✔	✔	✔	✔
Group Membership Definition							
Multicast group membership	✔	✔	✔	✔	✔	✔	✔
Individual membership							
Network membership	✔	✔	✔	✔	✔	✔	✔
VLAN membership	✔	✔	✔	✔	✔	✔	✔
Trunked VLAN membership	✔	✔	✔	✔	✔	✔	✔
IP Address							
Exclusion							
MAC address	✔	✔	✔	✔	✔	✔	✔
VLAN ID	✔	✔	✔	✔	✔	✔	✔
Frames with MPLS tag							
IP Address							
IP Muticast Group							
Group Key Distribution							
Unicast (unique KEK per group member)	✔	✔	✔	✔	✔	✔	✔
Broadcast (same KEK for all group members)	✔	✔	✔	✔	✔	✔	✔

Gemalto

Network Support							
Bump in the Wire deployment	✔	✔	✔	✔	✔	✔	✔
Jumbo Frame Support	✔	✔	✔	✔	✔	✔	✔
Ethernet Flow Control via PAUSE							
Ethernet Fragmentation/Defragmentation							
Point-to-Point							
Point-to-Multipoint							
Multipoint							
Dead Peer Detection	✔	✔	✔	✔	✔	✔	✔
Optical Loss Pass-Through		✔	✔	✔	✔	✔	✔
Link Loss Carry Forward	✔	✔	✔	✔	✔	✔	✔
System Configuration and Management Access							
IPv4	✔	✔	✔	✔	✔	✔	✔
IPv6	✔	✔	✔	✔	✔	✔	✔
Out-of-band Management	✔	✔	✔	✔	✔	✔	✔
RS-232/V.24	✔						
Separate Ethernet port	✔	✔	✔	✔	✔	✔	✔
Smart Card (Secure Card) Support							
USB Port	✔	✔	✔	✔	✔	✔	✔
In-band Management	✔	✔	✔	✔	✔	✔	✔
SSH	✔	✔	✔	✔	✔	✔	✔
SNMP (read-only/read-write)	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW
TLS							
Proprietary							
Remote Monitoring (SNMP)	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3
Logs							
Event Log (local)	✔	✔	✔	✔	✔	✔	✔
Audit Log (local)	✔	✔	✔	✔	✔	✔	✔
Syslog Support (Server)	✔	✔	✔	✔	✔	✔	✔
Unit							
Height in 19" Rack	Desktop	Desktop	1U	1U	4U	1U	1U
Number of external encrypted Ethernet ports	1	1	1	1	1-10	1	1
Physical Device Access	back	back	front	front	front	front	front
Redundant Power Supply			✔	✔	✔	✔	✔
Redundant, hot-swappable power supply			✔	✔	✔	✔	✔
High Availability functionality (two-node cluster)	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017
MTBF	> 200.000h	> 200.000h	> 200.000h	> 200.000h	> 100.000h	> 200.000h	> 200.000h
Tamper Security	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Security Approvals	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+	FIPS140-2 L3/ CC EAL2+ in progress	*
Safety Approvals	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000 ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS
Boot Time							
Cold boot until operational (P2P)	65s	65s	65s	65s	65s	65s	65s
Warm boot until operational (P2P)	80s	80s	80s	80s	80s	80s	80s

* For CN 9100 CC EAL2+ in progress, for CN 9120, FIPS 140-2 L3 and CC EAL2+ planned. For both: UC APL and NATO planned

Gemalto

Management Software

User Interface	Native PC application	✔	✔	✔	✔	✔	✔	✔
	Embedded Webapp							
	CLI	✔	✔	✔	✔	✔	✔	✔
Initial Device Set-up								
	Local (out-of-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (out-of-band)	✔	✔	✔	✔	✔	✔	✔
Device Configuration								
	Local (out-of-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (in-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (out-of-band)	✔	✔	✔	✔	✔	✔	✔
Management Access								
	Role-based access	✔	✔	✔	✔	✔	✔	✔
	Identity-based authentication of user	✔	✔	✔	✔	✔	✔	✔
	Number of hierarchy levels	2	2	2	2	2	2	2
	Number of roles	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)
	Strict internal separation of users	✔	✔	✔	✔	✔	✔	✔
Device Management								
	Device Diagnostics	✔	✔	✔	✔	✔	✔	✔
	Link Monitoring (SNMP)	✔	✔	✔	✔	✔	✔	✔
	Connection Diagnostics	✔	✔	✔	✔	✔	✔	✔
	In-band Network Diagnostics	✔	✔	✔	✔	✔	✔	✔
	Remote Update/Upgrade	✔	✔	✔	✔	✔	✔	✔
Certificate Authority & Management								
	Certificate Creation	✔	✔	✔	✔	✔	✔	✔
	Certificate Management	✔	✔	✔	✔	✔	✔	✔
Key Management								
	Group creation	✔	✔	✔	✔	✔	✔	✔
	Group isolation	✔	✔	✔	✔	✔	✔	✔
	Key assignment	✔	✔	✔	✔	✔	✔	✔
	Fail-over configuration	✔	✔	✔	✔	✔	✔	✔

Price

List Price Encryption Unit (in €)		on request	on request	on request	on request	on request	on request	on request
Per external Key Server (in €); optional, no requirement, starting price		on request	on request	on request	on request	on request	on request	on request
Required Management Software		CM7 included	CM7 included	CM7 included	CM7 included	CM7 included	CM7 included	CM7 included
Optional SMC Sofware	1-4 encryptors	free	free	free	free	free	free	free
	5-10 encryptors	on request	on request	on request	on request	on request	on request	on request
	11-20 encryptors	on request	on request	on request	on request	on request	on request	on request
	unlimited	on request	on request	on request	on request	on request	on request	on request
Warranty Period (months)		12	12	12	12	12	12	12
Warranty Coverage	Parts & Work	✔	✔	✔	✔	✔	✔	✔
	Basic Support (9 to 5, e-mail, phone)	✔	✔	✔	✔	✔	✔	✔
	Software updates and upgrades	✔	✔	✔	✔	✔	✔	✔
Warranty Extension (per year)		15%	15%	15%	15%	15%	15%	15%%

* Additionally available: Premium support (24x7 support, Advance RMA) with Plus Maintenance

Idquantique

	Centauris CN4010	Centauris CN4020	Centauris CN6010	Centauris CN6100	Centauris CN8000	Centauris CN9100	Centauris CN9120
Line Interface/Supported Line Rates							
10 Mbs	✔/RJ45	✔/SFP	✔/RJ45/SFP				
100 Mps	✔/RJ45	✔/SFP	✔/RJ45/SFP				
1 Gbps	✔/RJ45	✔/SFP	✔/RJ45/SFP	✔/SFP	✔/SFP+		
10 Gbps				✔/SFP	✔/SFP+		
25Gps							
40 Gbps					✔/SFP+		
100 Gbps					✔/SFP+	✔/CFP-4	✔/QSFP-28
Virtual Appliance					up to 10 cards at up to 10G each		
Supported Network Topologies							
Point-to-Point (P2P)	✔	✔	✔	✔	✔	✔	✔
Point-to-Multipoint (P2MP)	✔	✔	✔	✔	✔	✔	✔
Multipoint (MP)	✔	✔	✔	✔	✔	✔	✔
Supported Metro Ethernet Topologies							
Port-based							
Ethernet Private Line (EP-Line)	✔	✔	✔	✔	✔	✔	✔
Ethernet Private Tree (EP-Tree)	✔	✔	✔	✔	✔	✔	✔
Ethernet Private LAN (EP-LAN)	✔	✔	✔	✔	✔	✔	✔
VLAN-based							
Ethernet Virtual Private Line (EVP-Line)	✔	✔	✔	✔	✔	✔	✔
Ethernet Virtual Private Tree (EVP-Tree)	✔	✔	✔	✔	✔	✔	✔
Ethernet Virtual Private LAN (EVP-LAN)	✔	✔	✔	✔	✔	✔	✔
Supported Networks (Encryption)							
Ethernet	✔	✔	✔	✔	✔	✔	✔
MPLS (MPLSoE)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6							
Supported Networks (Transport of Encrypted Frame)							
Ethernet (native)	✔	✔	✔	✔	✔	✔	✔
MPLS (EoMPLS)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
TCP	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
UDP	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
Supported Usage Scenarios							
Single tenant	✔	✔	✔	✔	✔	✔	✔
Multi-tenant	*	*	*	*	✔/one tenant per port	*	
Self-managed	✔	✔	✔	✔	✔	✔	✔
Managed encryption service	✔	✔	✔	✔	✔	✔	✔
Managed security service	✔	✔	✔	✔	✔	✔	✔
Platform							
Platform used							
Mainboard/Firmware	Senetas/Senetas	Senetas/Senetas	Senetas/Senetas	Senetas/Senetas	Senetas/IDQuantique	Senetas/Senetas	Senetas/Senetas
Key Management	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas

* IP support only in combination with TRANSEC and limited to P2P. Additional overhead and latency.
* Multi-tenancy support based on certificates. Requires common trust domain of multiple CAs or use of a single CA

Idquantique

Data Plane Encryption Standard and Processing

Encryption Standard								
	Block Cipher	AES	AES	AES	AES	AES	AES	AES
	Preferred Mode of Operation	GCM	GCM	GCM	GCM	GCM	CTR	CTR
	Alternative Mode of Operation	CFB/CTR	CFB/CTR	CFB/CTR	CFB/CTR	CFB/CTR	GCM (Roadmap Q4 2017)	GCM (Roadmap Q4 2017)
	Key Length (in bit)	128/256	128/256	128/256	128/256	128/256	128/256	128/256
Processing Method								
	cut-through	✔	✔	✔	✔	✔		
	store&forward	*	*	*	*	*	✔	✔
Encryption Hardware								
	FPGA	✔	✔	✔	✔	✔	✔	✔
	ASIC							
	CPU							
Latency								
Latency P2P Mode	cut-through	<10µs (@1Gbps)	<10µs (@1Gbps)	<10µs	<5µs	<5µs		
	store & forward	*	*	*	*	*	<2µs	<2µs
Latency MP Mode	cut-through	<10µs (@1Gbps)	<10µs (@1Gbps)	<10µs	<5µs	<5µs		
	store & forward	*	*	*	*	*	<2µs	<2µs

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)		*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM				
	Authentication length (bytes)	16	16	16	16				
	Replay protection	✔	✔	✔	✔				
	Variable replay window (size)	256 frames	256 frames	256 frames	256 frames				
	Counter length (in bytes)	5	5	5	5				
	Frame overhead (unauthenticated encryption)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)				
	Frame overhead (authenticated encryption)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)				
	Ethernet multi-hop support	✔	✔	✔	✔				
Transport (Payload only)		✔	✔	✔	✔	✔	✔	✔	
	Max. number of peers	512	512	512	512	512	512	512	
	Max. number of MAC Addresses	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	limitation only in MAC mode
	Max. number of VLAN IDs	256	256	256	512	512	512	512	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	*GCM (Roadmap Q4 2017)	*GCM (Roadmap Q4 2017)	
	Authentication length (bytes)	16	16	16	16	16	16	16	
	Replay protection	✔	✔	✔	✔	✔	✔	✔	
	Variable replay window (size)	256 frames	256 frames	256 frames	256 frames	256 frames	256 frames	256 frames	
	Definable encryption offset (fixed)	✔	✔	✔	✔	✔	✔	✔	
	Variable encryption offset	✔	✔	✔	✔	✔	✔	✔	
	Adaptive encryption offset based on frame content	✔	✔	✔	✔	✔	✔	✔	
	Ethertype mutation	✔	✔	✔	✔	✔	✔	✔	
	Counter length (in bytes)	5	5	5	5	5	5	5	
	Frame overhead unauthenticated encryption	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	8 (CTR)	8 (CTR)	
	Frame overhead authenticated encryption (AE)	24	24	24	24	24	24*	24*	*GCM (Roadmap Q4 2017)
	Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	
Tunnel (Ethernet over Ethernet)		*	*	*	*	*	* Roadmap Q4 2017	* Roadmap Q4 2017	
	Max. number of peers	2	2	2	2				
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited				
	Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited				
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM				
	Authentication length (bytes)	16	16	16	16				
	Replay protection	✔	✔	✔	✔				
	Variable replay window (size)	256 frames	256 frames	256 frames	256 frames				
	Counter length (in bytes)	5	5	5	5				
	Frame overhead unauthenticated encryption	8 (CTR)	8 (CTR)	8 (CTR)	8 (CTR)				
	Frame overhead authenticated encryption (AE)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)				
	Ethernet multi-hop support	✔	✔	✔	✔				

* except for CN9100/CN9120 store & forward only in combination with TRANSEC and limited to P2P. Frame mode, tunnel mode and EoIP only when using TRANSEC. Frame mode not native. Additional overhead and latency.

Idquantique

Ethernet over IP (EoIP)							
Tunnel (Ethernet over IP)	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
Supported transmission protocols (UDP/TCP)	UDP/TCP	UDP/TCP	UDP/TCP	UDP/TCP			
Max. number of peers	2	2	2	2			
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited			
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited			
Integrity protection (algorithm)	GCM	GCM	GCM	GCM			
Authentication length (bytes)	16	16	16	16			
Replay protection	✔	✔	✔	✔			
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames			
Counter length (in bytes)	5	5	5	5			
Frame overhead unauthenticated encryption	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38			
Frame overhead authenticated encryption (AE)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)			
Ethernet multi-hop support	✔	✔	✔	✔			
Native IP Encryption							
Supported IP versions							
IPv4							
IPv6							
Supported transmission protocols							
TCP							
UDP							
Transport/Tunnel Mode							
Mximum number of peers							
Maximum number of IP addresses							
Maximum number of multicast groups							
Integrity protection (algorithm)							
Authentication length (bytes)							
Additional Authenticated Data (header)							
Replay Protection							
Variable replay window (size)							
Counter length (in bytes)							
Packet overhead authenticated encryption (AE)							
Selective Encryption							
Based on MAC Address	✔	✔	✔	✔	✔	✔	✔
Based on VLAN ID	✔	✔	✔	✔	✔	✔	✔
Based on Ethertype	✔	✔	✔	✔	✔	✔	✔
Based on Multicast Group	✔	✔	✔	✔	✔	✔	✔
Based on Presence of MPLS Tag							
Based on IP Address							
Combination of multiple selection criteria	✔	✔	✔	✔	✔	✔	✔
Mixed Ethernet, MPLS, EoIP and IP Support							
Based on VLAN ID							
MPLS	✔	✔	✔	✔	✔	✔	✔
EoIP							
IP							
Based on presence of MPLS tag							
MPLS							
EoIP							
IP							
Based on VLAN ID and presence of MPLS tag							
MPLS							
EoIP							
IP							
Traffic Masking							
Traffic Flow Security	✔	✔	✔	✔		Roadmap Q4 2017	Roadmap Q4 2017

* EoIP only when using TRANSEC. Limited to P2P. Additional overhead and latency.

Idquantique

Auto-discovery							
Auto-discovery of network encryptors	✔	✔	✔	✔	✔	✔	✔
Auto-discovery of key servers	✔	✔	✔	✔	✔	✔	✔
Auto-discovery of VLANs	✔	✔	✔	✔	✔	✔	✔
Disabling of auto-discovery	✔	✔	✔	✔	✔	✔	✔
Key Server							
Integrated Key Server	✔	✔	✔	✔	✔	✔	✔
Support for external Key Server	✔	✔	✔	✔	✔	✔	✔
External Key Server							
Support for multiple distributed Key Servers	✔	✔	✔	✔	✔	✔	✔
Support for fail-over to back-up Key Server	✔	✔	✔	✔	✔	✔	✔
Autonomous operation	✔	✔	✔	✔	✔	✔	✔
Key Management							
Key Generation and Storage							
Hardware Random Number Generation	✔	✔	✔	✔	✔/QRNG	✔QRNG	✔/QRNG
Tamper Security Key Storage (tamper-evident or tamper-proof)	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Asymmetric Key Algorithms (Public Key Cryptography)							
RSA							
Key length	2048	2048	2048	2048	2048	2048	2048
Elliptic Curve Cryptography (ECC)							
Key length	512	512	512	512	512	512	512
Supported Curves:							
NIST	✔	✔	✔	✔	✔	✔	✔
Brainpool	✔	✔	✔	✔	✔	✔	✔
Custom Curves	✔	✔	✔	✔	✔	✔	✔
Hash Algorithms							
SHA-2 Key length	512	512	512	512	512	512	512
Device Authentication							
Symmetric Signature: Pre-shared Key (PSK)							
Maximum number of PSKs per encryptor							
Key length							
Asymmetric Signature: Certificate	x.509	x.509	x.509	x.509	x.509	x.509	x.509
Maximum number of certificates per encryptor	64	64	64	64	64	64	64
Key length	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)
Ad-hoc authentication of peers (manual)							
Signature key protocol	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA
Key Agreement and Key Exchange							
Master Key (KEK) Agreement	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA
Master Key (KEK) Exchange Protocol	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas
Automatic Change of Master Key	✔	✔	✔	✔	✔	✔	✔
Minimum suggested Time Interval for Master Key Change (min)	1440	1440	1440	1440	1440	1440	1440
Separate Master Key (KEK) per site	✔	✔	✔	✔	✔	✔	✔
Separate Master Key (KEK) per group	✔	✔	✔	✔	✔	✔	✔
Session Key (DEK) Exchange Agreement	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications
Session Key (DEK) Exchange Protocol	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A
Automatic Change of Session Keys	✔	✔	✔	✔	✔	✔	✔
Minimum Time Interval for Session Key Change (min)	1	1	1	1	1	1	1

Idquantique

Key System							
Point-to-Point Key System							
Supported key system							
Pairwise	✔	✔	✔	✔	✔	✔	✔
Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:							
MAC Address	✔	✔	✔	✔	✔	✔	✔
VLAN ID	✔	✔	✔	✔	✔	✔	✔
Port	✔	✔	✔	✔	✔	✔	✔
Group	✔	✔	✔	✔	✔	✔	✔
IP Address							
Point-to-Multipoint Key System							
Supported key systems:							
Pairwise	✔	✔	✔	✔	✔	✔	✔
Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:							
MAC Address	✔	✔	✔	✔	✔	✔	✔
VLAN ID	✔	✔	✔	✔	✔	✔	✔
Port	✔	✔	✔	✔	✔	✔	✔
Group	✔	✔	✔	✔	✔	✔	✔
IP Address							
Multipoint Key System							
Supported key systems:							
Pairwise	✔	✔	✔	✔	✔	✔	✔
Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Mixed (pairwise unicast, group multicast)	✔	✔	✔	✔	✔	✔	✔
Key assignment based on:							
MAC address (pairwise and mixed)	✔	✔	✔	✔	✔	✔	✔
Multicast groups (mixed)	✔	✔	✔	✔	✔	✔	✔
VLAN ID (group)	✔	✔	✔	✔	✔	✔	✔
Port	✔	✔	✔	✔	✔	✔	✔
Group (group)	✔	✔	✔	✔	✔	✔	✔
IP Address							
IP Multicast Group							
Individual key per multicast group	✔	✔	✔	✔	✔	✔	✔
Individual key per broadcast group (VLAN ID)	✔	✔	✔	✔	✔	✔	✔
Group Key System Specifics							
Additional separate authentication per group	✔	✔	✔	✔	✔	✔	✔
Group Membership Definition							
Multicast group membership	✔	✔	✔	✔	✔	✔	✔
Individual membership							
Network membership	✔	✔	✔	✔	✔	✔	✔
VLAN membership	✔	✔	✔	✔	✔	✔	✔
Trunked VLAN membership	✔	✔	✔	✔	✔	✔	✔
IP Address							
Exclusion							
MAC address	✔	✔	✔	✔	✔	✔	✔
VLAN ID	✔	✔	✔	✔	✔	✔	✔
Frames with MPLS tag							
IP Address							
IP Muticast Group							
Group Key Distribution							
Unicast (unique KEK per group member)	✔	✔	✔	✔	✔	✔	✔
Broadcast (same KEK for all group members)	✔	✔	✔	✔	✔	✔	✔

Idquantique

Network Support							
Bump in the Wire deployment	✔	✔	✔	✔	✔	✔	✔
Jumbo Frame Support	✔	✔	✔	✔	✔	✔	✔
Ethernet Flow Control via PAUSE							
Ethernet Fragmentation/Defragmentation							
Point-to-Point							
Point-to-Multipoint							
Multipoint							
Dead Peer Detection	✔	✔	✔	✔	✔	✔	✔
Optical Loss Pass-Through		✔	✔	✔	✔	✔	✔
Link Loss Carry Forward	✔	✔	✔	✔	✔	✔	✔
System Configuration and Management Access							
IPv4	✔	✔	✔	✔	✔	✔	✔
IPv6	✔	✔	✔	✔	✔	✔	✔
Out-of-band Management	✔	✔	✔	✔	✔	✔	✔
RS-232/V.24	✔						
Separate Ethernet port	✔	✔	✔	✔	✔	✔	✔
Smart Card (Secure Card) Support							
USB Port	✔	✔	✔	✔	✔	✔	✔
In-band Management	✔	✔	✔	✔	✔	✔	✔
SSH	✔	✔	✔	✔	✔	✔	✔
SNMP (read-only/read-write)	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW
TLS							
Proprietary							
Remote Monitoring (SNMP)	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3
Logs							
Event Log (local)	✔	✔	✔	✔	✔	✔	✔
Audit Log (local)	✔	✔	✔	✔	✔	✔	✔
Syslog Support (Server)	✔	✔	✔	✔	✔	✔	✔
Unit							
Height in 19" Rack	Desktop	Desktop	1U	1U	4U	1U	1U
Number of external encrypted Ethernet ports	1	1	1	1	1-10	1	1
Physical Device Access	back	back	front	front	front	front	front
Redundant Power Supply			✔	✔	✔	✔	✔
Redundant, hot-swappable power supply			✔	✔	✔	✔	✔
High Availability functionality (two-node cluster)	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017
MTBF	> 200.000h	> 200.000h	> 200.000h	> 200.000h	> 100.000h	> 200.000h	> 200.000h
Tamper Security	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Security Approvals	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+	FIPS140-2 L3/ CC EAL2+ in progress	*
Safety Approvals	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000 ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS
Boot Time							
Cold boot until operational (P2P)	65s	65s	65s	65s	65s	65s	65s
Warm boot until operational (P2P)	80s	80s	80s	80s	80s	80s	80s

* For CN 9100 CC EAL2+ in progress, for CN 9120, FIPS 140-2 L3 and CC EAL2+ planned. For both: UC APL and NATO planned

Idquantique

Management Software								
User Interface	Native PC application	✔	✔	✔	✔	✔	✔	✔
	Embedded Webapp							
	CLI	✔	✔	✔	✔	✔	✔	✔
Initial Device Set-up								
	Local (out-of-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (out-of-band)	✔	✔	✔	✔	✔	✔	✔
Device Configuration								
	Local (out-of-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (in-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (out-of-band)	✔	✔	✔	✔	✔	✔	✔
Management Access								
	Role-based access	✔	✔	✔	✔	✔	✔	✔
	Identity-based authentication of user	✔	✔	✔	✔	✔	✔	✔
	Number of hierarchy levels	2	2	2	2	2	2	2
	Number of roles	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)
	Strict internal separation of users	✔	✔	✔	✔	✔	✔	✔
Device Management								
	Device Diagnostics	✔	✔	✔	✔	✔	✔	✔
	Link Monitoring (SNMP)	✔	✔	✔	✔	✔	✔	✔
	Connection Diagnostics	✔	✔	✔	✔	✔	✔	✔
	In-band Network Diagnostics	✔	✔	✔	✔	✔	✔	✔
	Remote Update/Upgrade	✔	✔	✔	✔	✔	✔	✔
Certificate Authority & Management								
	Certificate Creation	✔	✔	✔	✔	✔	✔	✔
	Certificate Management	✔	✔	✔	✔	✔	✔	✔
Key Management								
	Group creation	✔	✔	✔	✔	✔	✔	✔
	Group isolation	✔	✔	✔	✔	✔	✔	✔
	Key assignment	✔	✔	✔	✔	✔	✔	✔
	Fail-over configuration	✔	✔	✔	✔	✔	✔	✔

Price								
List Price Encryption Unit (in €)		on request	on request	on request	on request	on request	on request	on request
Per external Key Server (in €); optional, no requirement, starting price		on request	on request	on request	on request	on request	on request	on request
Required Management Software		CM7 included	CM7 included	CM7 included	CM7 included	CM7 included	CM7 included	CM7 included
Optional SMC Sofware	1-4 encryptors	free	free	free	free	free	free	free
	5-10 encryptors	on request	on request	on request	on request	on request	on request	on request
	11-20 encryptors	on request	on request	on request	on request	on request	on request	on request
	unlimited	on request	on request	on request	on request	on request	on request	on request
Warranty Period (months)		12	12	12	12	12	12	12
Warranty Coverage	Parts & Work	✔	✔	✔	✔	✔	✔	✔
	Basic Support (9 to 5, e-mail, phone)	✔	✔	✔	✔	✔	✔	✔
	Software updates and upgrades	✔	✔	✔	✔	✔	✔	✔
Warranty Extension (per year)		10%	10%	10%	10%	10%	10%	10%

* Additionally available: Premium support (24x7 support, Advance RMA) with Plus Maintenance

Rohde & Schwarz Cybersecurity

	SITLine ETH50	SITLine ETH4G	SITLine ETH10G	SITLine ETH40G	
Line Interface/Supported Line Rates					
10 Mbs	✔/RJ45	✔/4xRJ45/4xSFP	✔/4xRJ45/4xSFP+		
100 Mps	✔/RJ45	✔/4xRJ45/4xSFP	✔/4xRJ45/4xSFP+		
1 Gbps		✔/4xRJ45/4xSFP	✔/4xRJ45/4xSFP+		
10 Gbps		✔/(license upgrade)	✔/4xRJ45/4xSFP+	✔/4xRJ45/4xSFP+	
25Gps					
40 Gbps				✔/QSFP	on request
100 Gbps					
Virtual Appliance					
Supported Network Topologies					
Point-to-Point (P2P)	✔	✔	✔	✔	
Point-to-Multipoint (P2MP)	✔	✔	✔	✔	
Multipoint (MP)	✔	✔	✔	✔	
Supported Metro Ethernet Topologies					
Port-based					
Ethernet Private Line (EP-Line)	✔	✔	✔	✔	
Ethernet Private Tree (EP-Tree)	✔	✔	✔	✔	
Ethernet Private LAN (EP-LAN)	✔	✔	✔	✔	
VLAN-based					
Ethernet Virtual Private Line (EVP-Line)	✔	✔	✔	✔	
Ethernet Virtual Private Tree (EVP-Tree)	✔	✔	✔	✔	
Ethernet Virtual Private LAN (EVP-LAN)	✔	✔	✔	✔	
Supported Networks (Encryption)					
Ethernet	✔	✔	✔	✔	
MPLS					supported by SITline IP Roadmap Q3 2017
IPv4/IPv6					supported by SITline IP Roadmap Q3 2017
Supported Networks (Transport of Encrypted Frame)					
Ethernet (native)	✔	✔	✔	✔	
MPLS (EoMPLS)	✔	✔	✔	✔	
IPv4/IPv6					supported by SITline IP Roadmap Q3 2017
TCP					supported by SITline IP Roadmap Q3 2017
UDP					supported by SITline IP Roadmap Q3 2017
Supported Usage Scenarios					
Single tenant	✔	✔	✔	✔	
Multi-tenant					
Self-managed	✔	✔	✔	✔	
Managed encryption service	✔	✔	✔	✔	
Managed security service	✔	✔	✔	✔	separate network and security management (NMS, SMS)
Platform					
Platform used					
Mainboard/Firmware	Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	
Key Management	Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	

Rohde & Schwarz Cybersecurity

Data Plane Encryption Standard and Processing

Encryption Standard						
	Block Cipher	AES	AES	AES	AES	
	Preferred Mode of Operation	GCM	GCM	GCM	GCM	
	Alternative Mode of Operation	CFB	CFB	CFB	CFB	
	Key Length (in bit)	256	256	256	256	
Processing Method						
	cut-through		✔	✔	✔	
	store&forward	✔	✔	✔	✔	
Encryption Hardware						
	FPGA	✔	✔	✔	✔	
	ASIC					
	CPU					
Latency						
Latency P2P Mode	cut-through	N/A	5µs	<3µs	<3µs	
	store & forward	*	*	*	*	* dependent on packet size/bandwidth
Latency MP Mode	cut-through	N/A	5µs	<3µs	<3µs	
	store & forward	*	*	*	*	

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)			✔	✔	✔	
	Integrity protection (algorithm)		GCM	GCM	GCM	
	Authentication length (bytes)		8-16	8-16	8-16	
	Replay protection		✔	✔	✔	
	Variable replay window (size)		3 frames per priority	3 frames per priority	3 frames per priority	
	Counter length (in bytes)		5	5	5	
	Frame overhead (unauthenticated encryption)		0 (CFB), 5 (CTR)	0 (CFB), 5 (CTR)	0 (CFB), 5 (CTR)	
	Frame overhead (authenticated encryption)		13-21	13-21	13-21	
Transport (Payload only)		✔	✔	✔	✔	
	Max. number of peers	250	4000	4000	4000	
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	
	Max. number of VLAN IDs	250	4000	4000	4000	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	
	Authentication length (bytes)	8-16	8-16	8-16	8-16	
	Replay protection	✔	✔	✔	✔	
	Variable replay window (size)	3 frames per priority	3 frames per priority	3 frames per priority	3 frames per priority	
	Definable encryption offset (fixed)					
	Variable encryption offset	✔	✔	✔	✔	
	Adaptive encryption offset based on frame content	✔	✔	✔	✔	
	Ethertype mutation (unauthenticated encryption only)	✔	✔	✔	✔	
	Counter length (in bytes)	5	5	5	5	
	Frame overhead unauthenticated encryption	5 (PP)/ 10 (MP)	5 (PP)/ 10 (MP)	5 (PP)/ 10 (MP)	5 (PP)/ 10 (MP)	
	Frame overhead authenticated encryption (AE)	13-21 (PP), 18-26 (MP)	13-21 (PP), 18-26 (MP)	13-21 (PP), 18-26 (MP)	13-21 (PP), 18-26 (MP)	
	Ethernet multi-hop support	✔	✔	✔	✔	
Tunnel (Ethernet over Ethernet)		✔	✔	✔	✔	tunnel in multipoint mode only replaces destination address
	Max. number of peers	250	4000	4000	4000	
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	
	Max. number of VLAN IDs	250	4000	4000	4000	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	
	Authentication length (bytes)	8-16	8-16	8-16	8-16	
	Replay protection	✔	✔	✔	✔	
	Variable replay window (size)	3 frames per priority	3 frames per priority	3 frames per priority	3 frames per priority	
	Counter length (in bytes)	5	5	5	5	
	Frame overhead unauthenticated encryption	20	20	20	20	
	Frame overhead authenticated encryption (AE)	18-26 (P2P), 28-36 (MP)	18-26 (P2P), 28-36 (MP)	18-26 P2P 28-36 (MP)	18-26 (P2P), 28-36 (MP)	
	Ethernet multi-hop support	✔	✔	✔	✔	

Rohde & Schwarz Cybersecurity

Ethernet over IP (EoIP)					
Tunnel (Ethernet over IP)					
Supported transmission protocols (UDP/TCP)					
Max. number of peers					
Max. number of MAC Addresses					
Max. number of VLAN IDs					
Integrity protection (algorithm)					
Authentication length (bytes)					
Replay protection					
Variable replay window (size)					
Counter length (in bytes)					
Frame overhead unauthenticated encryption					
Frame overhead authenticated encryption (AE)					
Ethernet multi-hop support					
Native IP Encryption					
Supported IP versions					
IPv4					supported by SITline IP Roadmap Q3 2017
IPv6					supported by SITline IP Roadmap Q3 2017
Supported transmission protocols					
TCP					supported by SITline IP Roadmap Q3 2017
UDP					supported by SITline IP Roadmap Q3 2017
Transport/Tunnel Mode					supported by SITline IP Roadmap Q3 2017
Mximum number of peers					
Maximum number of IP addresses					
Maximum number of multicast groups					
Integrity protection (algorithm)					
Authentication length (bytes)					
Additional Authenticated Data (header)					
Replay Protection					
Variable replay window (size)					
Counter length (in bytes)					
Packet overhead authenticated encryption (AE)					
Selective Encryption					
Based on MAC Address	✔	✔	✔	✔	
Based on VLAN ID	✔	✔	✔	✔	
Based on Ethertype	✔	✔	✔	✔	
Based on Multicast Group	✔	✔	✔	✔	
Based on Presence of MPLS Tag					
Based on IP Address					
Combination of multiple selection criteria	✔	✔	✔	✔	
Mixed Ethernet, MPLS, EoIP and IP Support					
Based on VLAN ID					
MPLS					
EoIP					
IP					
Based on presence of MPLS tag					
MPLS					
EoIP					
IP					
Based on VLAN ID and presence of MPLS tag					
MPLS					
EoIP					
IP					
Traffic Masking					
Traffic Flow Security					

Rohde & Schwarz Cybersecurity

Auto-discovery						
Auto-discovery of network encryptors		✔	✔	✔	✔	
Auto-discovery of key servers		✔	✔	✔	✔	
Auto-discovery of VLANs		✔	✔	✔	✔	Automatische Partnersuche über VLANs
Disabling of auto-discovery		✔	✔	✔	✔	
Key Server						
Integrated Key Server		✔	✔	✔	✔	
Support for external Key Server						
External Key Server						
Support for multiple distributed Key Servers		✔	✔	✔	✔	
Support for fail-over to back-up Key Server		N/A	N/A	N/A	N/A	
Autonomous operation		✔	✔	✔	✔	
Key Management						
Key Generation and Storage						
Hardware Random Number Generation		✔ (PTG-3)	✔ (PTG-3)	✔ (PTG-3)	✔ (PTG-3)	
Tamper Security Key Storage (tamper-evident or tamper-proof)		TE/TP	TE/TP	TE/TP	TE/TP	
Asymmetric Key Algorithms (Public Key Cryptography)						
RSA						
	Key length	2048	2048	2048	2048	
Elliptic Curve Cryptography (ECC)						
	Key length	257	257	257	257	
Supported Curves:						
	NIST					
	Brainpool					
	Custom Curves	✔	✔	✔	✔	
Hash Algorithms						
SHA-2	Key length	256	256	256	256	
Device Authentication						
Symmetric Signature: Pre-shared Key (PSK)						
	Maximum number of PSKs per encryptor					
	Key length					
Asymmetric Signature: Certificate		x.509	x.509	x.509	x.509	
	Maximum number of certificates per encryptor	1	1	1	1	
	Key lenght	257	257	257	257	
Ad-hoc authentication of peers (manual)		✔	✔	✔	✔	
Signature key protocol		ECDSA	ECDSA	ECDSA	ECDSA	
Key Agreement and Key Exchange						
Master Key (KEK) Agreement		DH-ECKAS	DH-ECKAS	DH-ECKAS	DH-ECKAS	
Master Key (KEK) Exchange Protocol		ECDH	ECDH	ECDH	ECDH	
Automatic Change of Master Key		✔	✔	✔	✔	
Minimum suggested Time Interval for Master Key Change (min)		360	360	360	360	
Separate Master Key (KEK) per site		✔	✔	✔	✔	
Separate Master Key (KEK) per group						
Session Key (DEK) Exchange Agreement		Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	
Session Key (DEK) Exchange Protocol		Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	
Automatic Change of Session Keys		✔	✔	✔	✔	
Minimum Time Interval for Session Key Change (min)		1	1	1	1	

Rohde & Schwarz Cybersecurity

Key System					
Point-to-Point Key System					
Supported key system					
	Pairwise	✔	✔	✔	✔
	Group				
Key assignment based on:					
	MAC Address				
	VLAN ID	✔	✔	✔	✔
	Port	✔	✔	✔	✔
	Group				
	IP Address				
Point-to-Multipoint Key System					
Supported key systems:					
	Pairwise	✔	✔	✔	✔
	Group				
Key assignment based on:					
	MAC Address				
	VLAN ID	✔	✔	✔	✔
	Port				
	Group				
	IP Address				
Multipoint Key System					
Supported key systems:					
	Pairwise	✔	✔	✔	✔
	Group	Unidirectional Group	Unidirectional Group	Unidirectional Group	Unidirectional Group
	Mixed (pairwise unicast, group multicast)	✔	✔	✔	✔
Key assignment based on:					
	MAC address (pairwise and mixed)				
	Multicast groups (mixed)				
	VLAN ID (group)	✔	✔	✔	✔
	Port	✔	✔	✔	✔
	Group (group)	✔	✔	✔	✔
	IP Address				
	IP Multicast Group				
Individual key per multicast group		✔	✔	✔	✔
Individual key per broadcast group (VLAN ID)		✔	✔	✔	✔
Group Key System Specifics					
Additional separate authentication per group		✔	✔	✔	✔
Group Membership Definition					
	Multicast group membership				
	Individual membership	✔	✔	✔	✔
	Network membership	✔	✔	✔	✔
	VLAN membership	✔	✔	✔	✔
	Trunked VLAN membership	✔	✔	✔	✔
	IP Address				
Exclusion					
	MAC address	✔	✔	✔	✔
	VLAN ID	✔	✔	✔	✔
	Frames with MPLS tag				
	IP Address				
	IP Muticast Group				
Group Key Distribution					
	Unicast (unique KEK per group member)	✔	✔	✔	✔
	Broadcast (same KEK for all group members)				

Rohde & Schwarz Cybersecurity

Network Support						
Bump in the Wire deployment		✔	✔	✔	✔	
Jumbo Frame Support		✔	✔	✔	✔	bis 16000 Bytes
Ethernet Flow Control via PAUSE		✔	✔	✔	✔	
Ethernet Fragmentation/Defragmentation						
	Point-to-Point					
	Point-to-Multipoint					
	Multipoint					
Dead Peer Detection		✔	✔	✔	✔	
Optical Loss Pass-Through		✔	✔	✔	✔	
Link Loss Carry Forward		✔	✔	✔	✔	
System Configuration and Management Access						
IPv4		✔	✔	✔	✔	
IPv6						
Out-of-band Management		✔	✔	✔	✔	
	RS-232/V.24					
	Separate Ethernet port		✔	✔	✔	
Smart Card (Secure Card) Support		✔	✔	✔	✔	
USB Port		✔				
In-band Management		✔	✔	✔	✔	
	SSH		✔	✔	✔	
	SNMP (read-only/read-write)	✔	✔	✔	✔	
	TLS	✔	✔	✔	✔	
	Proprietary	✔	✔	✔	✔	
Remote Monitoring (SNMP)		v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	
Logs						
Event Log (local)		✔	✔	✔	✔	
Audit Log (local)		✔	✔	✔	✔	
Syslog Support (Server)		✔	✔	✔	✔	
Unit						
Height in 19" Rack		1U (1/2 19" width)	1	1	1	
Number of external encrypted Ethernet ports		1	1 or 4	1 or 4	1 or 4	
Physical Device Access		front	front	front	front	
Redundant Power Supply		✔	✔	✔	✔	
Redundant, hot-swappable power supply		✔	✔	✔	✔	
High Availability functionality (two-node cluster)		1-1	1-1	1-1	1-1	
MTBF		350000h	170000h	170000h	170000h	
Tamper Security		TE/TP	TE/TP	TE/TP	TE/TP	
Security Approvals		BSI VS-NfD, EU restreint	BSI VS-NfD, EU restreint	BSI VS-NfD, EU restreint, **CC EAL4+	BSI VS-NfD, EU restreint, **CC EAL4+	CC EAL 4+ pending
Safety Approvals		CE, ROHS	CE, ROHS	CE, ROHS	CE, ROHS	
Boot Time						
	Cold boot until operational (P2P)	60s	40s	40s	40s	
	Warm boot until operational (P2P)	60s	40s	40s	40s	

Rohde & Schwarz Cybersecurity

Management Software						
User Interface	Native PC application	✔	✔	✔	✔	
	Embedded Webapp					
	CLI	✔	✔	✔	✔	
Initial Device Set-up						
	Local (out-of-band)	✔	✔	✔	✔	
	Remote (out-of-band)					
Device Configuration						
	Local (out-of-band)	✔	✔	✔	✔	
	Remote (in-band)	✔	✔	✔	✔	
	Remote (out-of-band)	✔	✔	✔	✔	
Management Access						
	Role-based access	✔	✔	✔	✔	
	Identity-based authentication of user	✔	✔	✔	✔	
	Number of hierarchy levels	2	2	2	2	
	Number of roles	8	8	8	8	customizable roles
	Strict internal separation of users	✔	✔	✔	✔	
Device Management						
	Device Diagnostics	✔	✔	✔	✔	
	Link Monitoring (SNMP)	✔	✔	✔	✔	
	Connection Diagnostics	✔	✔	✔	✔	
	In-band Network Diagnostics	✔	✔	✔	✔	
	Remote Update/Upgrade	✔	✔	✔	✔	
Certificate Authority & Management						
	Certificate Creation	✔	✔	✔	✔	
	Certificate Management	✔	✔	✔	✔	
Key Management						
	Group creation	✔	✔	✔	✔	
	Group isolation	✔	✔	✔	✔	via key management
	Key assignment	✔	✔	✔	✔	
	Fail-over configuration	✔	✔	✔	✔	

Price					
List Price Encryption Unit (in €)		on request	on request	on request	on request
Per extermal Key Server (in €)					
Required Management Software		on request	on request	on request	on request
	2-10 encryptors	on request	on request	on request	on request
	11-25 encryptors	on request	on request	on request	on request
	26-50 encryptors	on request	on request	on request	on request
	51+ encryptors	on request	on request	on request	on request
Warranty Period (months)		12	12	12	12
Warranty Coverage	Parts & Work	✔	✔	✔	✔
	Basic Support (9 to 5, e-mail, phone)	3%	3%	3%	3%
	Software updates and upgrades	3%	3%	3%	3%
Warranty Extension (per year)		5%	5%	5%	5%

Secunet

	50M compact	100M	1G	10G	40G	100G
Line Interface/Supported Line Rates						
					Roadmap Q2 2017	Roadmap Q4 2017
10 Mbs	✔/RJ45	✔/RJ45	✔/SFP			
100 Mps	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+		
1 Gbps	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+	✔/QSFP	
10 Gbps			✔/SFP	✔/SFP+	✔/QSFP	✔/QSFP28
25Gps					✔/QSFP	✔/QSFP28
40 Gbps					✔/QSFP	✔/QSFP28
100 Gbps						✔/QSFP28
Virtual Appliance						
Supported Network Topologies						
Point-to-Point (P2P)	✔	✔	✔	✔	✔	✔
Point-to-Multipoint (P2MP)	✔	✔	✔	✔	✔	✔
Multipoint (MP)	✔	✔	✔	✔	✔	✔
Supported Metro Ethernet Topologies						
Port-based						
Ethernet Private Line (EP-Line)	✔	✔	✔	✔	✔	✔
Ethernet Private Tree (EP-Tree)	✔	✔	✔	✔	✔	✔
Ethernet Private LAN (EP-LAN)	✔	✔	✔	✔	✔	✔
VLAN-based						
Ethernet Virtual Private Line (EVP-Line)	✔	✔	✔	✔	✔	✔
Ethernet Virtual Private Tree (EVP-Tree)	✔	✔	✔	✔	✔	✔
Ethernet Virtual Private LAN (EVP-LAN)	✔	✔	✔	✔	✔	✔
Supported Networks (Encryption)						
Ethernet	✔	✔	✔	✔	✔	✔
MPLS	✔	✔	✔	✔	✔	✔
IP v4/v6	✔	✔	✔	✔	✔	✔
Supported Networks (Transport of Encrypted Frame)						
Ethernet (native)	✔	✔	✔	✔	✔	✔
MPLS (EoMPLS)	✔	✔	✔	✔	✔	✔
IPv4/IPv6	✔	✔	✔	✔	✔	✔
TCP	✔	✔	✔	✔	✔	✔
UDP	✔	✔	✔	✔	✔	✔
Supported Usage Scenarios						
Single tenant	✔	✔	✔	✔	✔	✔
Multi-tenant	✔	✔	✔	✔	✔	✔
Self-managed	✔	✔	✔	✔	✔	✔
Managed encryption service	✔	✔	✔	✔	✔	✔
Managed security service	✔	✔	✔	✔	✔	✔
Platform						
Platform used						
Mainboard/Firmware	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia
Key Management	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia

Secunet

Data Plane Encryption Standard and Processing

Encryption Standard								
	Block Cipher	AES	AES	AES	AES	AES	AES	
	Preferred Mode of Operation	GCM	GCM	GCM	GCM	GCM	GCM	
	Alternative Mode of Operation							
	Key Length (in bit)	256	256	256	256	256	256	
Processing Method								
	cut-through	✔	✔	✔	✔	✔	✔	
	store&forward	✔	✔	✔	✔	✔	✔	
Encryption Hardware								
	FPGA	✔	✔	✔	✔	✔	✔	
	ASIC							
	CPU							
Latency								
Latency P2P Mode	cut-through	<42µs	<42µs	<8µs	<4µs	<4µs	<2µs	
	store & forward	<48µs	<48µs	<9µs	<4µs	<4µs	<2µs	
Latency MP Mode	cut-through	<42µs	<42µs	<8µs	<4µs	<4µs	<2µs	
	store & forward	<48µs	<48µs	<9µs	<4µs	<4µs	<2µs	

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)		✔	✔	✔	✔	✔	✔	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	
	Replay protection	✔	✔	✔	✔	✔	✔	
	Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
	Counter length (in bytes)	8	8	8	8	8	8	
	Frame overhead (unauthenticated encryption)	N/A	N/A	N/A	N/A	N/A	N/A	
	Frame overhead (authenticated encryption)	18/26	18/26	18/26	18/26	18/26	18/26	
	Ethernet multi-hop support	N/A	N/A	N/A	N/A	N/A	N/A	
Transport (Payload only)		✔	✔	✔	✔	✔	✔	
	Max. number of peers	1000	1000	1000	1000	1000	1000	
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
	Max. number of VLAN IDs	256	256	unlimited	256	unlimited	256	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	
	Replay protection	✔	✔	✔	✔	✔	✔	
	Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
	Definable encryption offset (fixed)	✔	✔	✔	✔	✔	✔	
	Variable encryption offset	✔	✔	✔	✔	✔	✔	
	Adaptive encryption offset based on frame content	✔	✔	✔	✔	✔	✔	
	Ethertype mutation (unauthenticated encryption only)	✔	✔	✔	✔	✔	✔	
	Counter length (in bytes)	8	8	8	8	8	8	
	Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	
	Frame overhead authenticated encryption (AE)	18/26	18/26	18/26	18/26	18/26	18/26	
	Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	
Tunnel (Ethernet over Ethernet)		✔	✔	✔	✔	✔	✔	
	Max. number of peers	32	32	32	32	32	32	
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
	Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	
	Replay protection	✔	✔	✔	✔	✔	✔	
	Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
	Counter length (in bytes)	8	8	8	8	8	8	
	Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	
	Frame overhead authenticated encryption (AE)	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*	*IMIX=100%
	Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	

Secunet

Ethernet over IP (EoIP)							
Tunnel (Ethernet over IP)	✔	✔	✔	✔	✔	✔	
Supported transmission protocols (UDP/TCP)	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	
Max. number of peers	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	
Replay protection	✔	✔	✔	✔	✔	✔	
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
Registered Ethertype	✔	✔	✔	✔	✔	✔	
Counter length (in bytes)	8	8	8	8	8	8	
Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	
Frame overhead authenticated encryption (AE)	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*	*IMIX=100%
Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	
Native IP Encryption							
Supported IP versions							
IPv4	✔	✔	✔	✔	✔	✔	
IPv6	✔	✔	✔	✔	✔	✔	
Supported transmission protocols							
TCP	✔	✔	✔	✔	✔	✔	
UDP	✔	✔	✔	✔	✔	✔	
Transport Tunnel Mode							
Mximum number of peers	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Maximum number of IP addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Maximum number of multicast groups	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	
Additional Authenticated Data (header)	✔	✔	✔	✔	✔	✔	
Replay Protection	✔	✔	✔	✔	✔	✔	
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
Counter length (in bytes)	8	8	8	8	8	8	
Packet overhead authenticated encryption (AE)	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	
Selective Encryption							
Based on MAC Address	✔	✔	✔	✔	✔	✔	
Based on VLAN ID	✔	✔	✔	✔	✔	✔	
Based on Ethertype	✔	✔	✔	✔	✔	✔	
Based on Multicast Group	✔	✔	✔	✔	✔	✔	
Based on Presence of MPLS Tag	✔	✔	✔	✔	✔	✔	
Based on IP Address	✔	✔	✔	✔	✔	✔	
Combination of multiple selection criteria	✔	✔	✔	✔	✔	✔	
Mixed Ethernet, MPLS, EoIP and IP Support							
Based on VLAN ID							
MPLS	✔	✔	✔	✔	✔	✔	
EoIP	✔	✔	✔	✔	✔	✔	
IP	✔	✔	✔	✔	✔	✔	
Based on presence of MPLS tag							
MPLS	✔	✔	✔	✔	✔	✔	
EoIP	✔	✔	✔	✔	✔	✔	
IP	✔	✔	✔	✔	✔	✔	
Based on VLAN ID and presence of MPLS tag							
MPLS	✔	✔	✔	✔	✔	✔	
EoIP	✔	✔	✔	✔	✔	✔	
IP	✔	✔	✔	✔	✔	✔	
Traffic Masking							
Traffic Flow Security	✔	✔	✔	✔	✔	✔	

**TFS mode only secure based on ASIC or FPGA

Secunet

Auto-discovery							
Auto-discovery of network encryptors		✔	✔	✔	✔	✔	✔
Auto-discovery of key servers		✔	✔	✔	✔	✔	✔
Auto-discovery of VLANs		✔	✔	✔	✔	✔	✔
Disabling of auto-discovery		✔	✔	✔	✔	✔	✔
Key Server							
Integrated Key Server		✔	✔	✔	✔	✔	✔
Support for external Key Server		✔	✔	✔	✔	✔	✔
External Key Server							
Support for multiple distributed Key Servers		✔	✔	✔	✔	✔	✔
Support for fail-over to back-up Key Server		✔	✔	✔	✔	✔	✔
Autonomous operation		✔	✔	✔	✔	✔	✔
Key Management							
Key Generation and Storage							
Hardware Random Number Generation		✔	✔	✔	✔	✔	✔
Tamper Security Key Storage (tamper-evident or tamper-proof)		TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Asymmetric Key Algorithms (Public Key Cryptography)							
RSA							
	Key length	N/A	N/A	N/A	N/A	N/A	N/A
Elliptic Curve Cryptography (ECC)							
	Key length	512/521	512/521	512/521	512/521	512/521	512/521
Supported Curves:							
	NIST	✔	✔	✔	✔	✔	✔
	Brainpool	✔	✔	✔	✔	✔	✔
	Custom Curves	✔	✔	✔	✔	✔	✔
Hash Algorithms							
SHA-2	Key length	512	512	512	512	512	512
CBC-MAC-GCM	Key length	256	256	256	256	256	256
Device Authentication							
Symmetric Signature: Pre-shared Key (PSK)		✔	✔	✔	✔	✔	✔
	Maximum number of PSKs per encryptor	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)
	Key length	256	256	256	256	256	256
Asymmetric Signature: Certificate		optional	optional	optional	optional	optional	optional
	Maximum number of certificates per encryptor	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)
	Key lenght	512	512	512	512	512	512
Ad-hoc authentication of peers (manual)		✔	✔	✔	✔	✔	✔
Signature key protocol		AES-MAC/ECDSA***	AES-MAC/ECDSA***	AES-MAC/ECDSA***	AES-MAC/ECDSA***	AES-MAC/ECDSA***	AES-MAC/ECDSA***
Key Agreement and Key Exchange							
Master Key (KEK) Agreement		ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****
Master Key (KEK) Exchange Protocol		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Automatic Change of Master Key		✔	✔	✔	✔	✔	✔
Minimum suggested Time Interval for Master Key Change (min)		60	60	60	60	60	60
Separate Master Key (KEK) per site		✔	✔	✔	✔	✔	✔
Separate Master Key (KEK) per group		✔	✔	✔	✔	✔	✔
Session Key (DEK) Exchange Agreement		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Session Key (DEK) Exchange Protocol		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Automatic Change of Session Keys		✔	✔	✔	✔	✔	✔
Minimum Time Interval for Session Key Change (min)		1	1	1	1	1	1

***ECDSA optional for use with optional certificates

*****NIST, Brainpool or custom curves with 256 to 521 bit length

Secunet

Key System

Point-to-Point Key System

Supported key system						
	Pairwise	✔	✔	✔	✔	✔	✔
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:						
	MAC Address	✔	✔	✔	✔	✔	✔
	VLAN ID	✔	✔	✔	✔	✔	✔
	Port	✔	✔	✔	✔	✔	✔
	Group	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔

Point-to-Multipoint Key System

Supported key systems:						
	Pairwise	✔	✔	✔	✔	✔	✔
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:						
	MAC Address	✔	✔	✔	✔	✔	✔
	VLAN ID	✔	✔	✔	✔	✔	✔
	Port	✔	✔	✔	✔	✔	✔
	Group	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔

Multipoint Key System

Supported key systems:						
	Pairwise	✔	✔	✔	✔	✔	✔
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
	Mixed (pairwise unicast, group multicast)	✔	✔	✔	✔	✔	✔
Key assignment based on:						
	MAC address (pairwise and mixed)	✔	✔	✔	✔	✔	✔
	Multicast groups (mixed)	✔	✔	✔	✔	✔	✔
	VLAN ID (group)	✔	✔	✔	✔	✔	✔
	Port	✔	✔	✔	✔	✔	✔
	Group (group)	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔
	IP Multicast Group	✔	✔	✔	✔	✔	✔
Individual key per multicast group		✔	✔	✔	✔	✔	✔
Individual key per broadcast group (VLAN ID)		✔	✔	✔	✔	✔	✔

Group Key System Specifics

Additional separate authentication per group		✔	✔	✔	✔	✔	✔
Group Membership Definition						
	Multicast group membership	✔	✔	✔	✔	✔	✔
	Individual membership	✔	✔	✔	✔	✔	✔
	Network membership	✔	✔	✔	✔	✔	✔
	VLAN membership	✔	✔	✔	✔	✔	✔
	Trunked VLAN membership	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔
Exclusion						
	MAC address	✔	✔	✔	✔	✔	✔
	VLAN ID	✔	✔	✔	✔	✔	✔
	Frames with MPLS tag	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔
	IP Muticast Group	✔	✔	✔	✔	✔	✔
Group Key Distribution						
	Unicast (unique KEK per group member)	✔	✔	✔	✔	✔	✔
	Broadcast (same KEK for all group members)	✔	✔	✔	✔	✔	✔

Secunet

Network Support							
Bump in the Wire deployment		✔	✔	✔	✔	✔	✔
Jumbo Frame Support		✔	✔	✔	✔	✔	✔
Ethernet Flow Control via PAUSE		✔	✔	✔	✔	✔	✔
Ethernet Fragmentation/Defragmentation		✔	✔	✔	✔	✔	✔
	Point-to-Point	✔	✔	✔	✔	✔	✔
	Point-to-Multipoint	✔	✔	✔	✔	✔	✔
	Multipoint	✔	✔	✔	✔	✔	✔
Dead Peer Detection		✔	✔	✔	✔	✔	✔
Optical Loss Pass-Through		N/A	N/A	✔	✔	✔	✔
Link Loss Carry Forward		✔	✔	✔	✔	N/A	N/A
System Configuration and Management Access							
IPv4		✔	✔	✔	✔	✔	✔
IPv6		✔	✔	✔	✔	✔	✔
Out-of-band Management		✔	✔	✔	✔	✔	✔
	RS-232/V.24	✔	✔	✔	✔	✔	✔
	Separate Ethernet port	✔	✔	✔	✔	✔	✔
Smart Card (Secure Card) Support		✔	✔	✔	✔	✔	✔
USB Port						✔	✔
In-band Management		✔	✔	✔	✔	✔	✔
	SSH	✔	✔	✔	✔	✔	✔
	SNMP (read-only/read-write)	read-only	read-only	read-only	read-only	read-only	read-only
	TLS						
	Proprietary	✔	✔	✔	✔	✔	✔
Remote Monitoring (SNMP)		v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3
Logs							
Event Log (local)		✔	✔	✔	✔	✔	✔
Audit Log (local)		✔	✔	✔	✔	✔	✔
Syslog Support (Server)		✔	✔	✔	✔	✔	✔
Unit							
Height in 19" Rack		1U	1U	1U	1U	1U	1U
Number of external encrypted Ethernet ports		1	1	1	1	1-4	1-4
Physical Device Access		back	front	front	front	front	front
Redundant Power Supply			✔	✔	✔	✔	✔
Redundant, hot-swappable power supply			✔	✔	✔	✔	✔
High Availability functionality (two-node cluster)		1:1	1:1	1:1	1:1	1:1	1:1
MTBF		> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h
Tamper Security		TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Security Approvals			BSI VS-NfD, NATO restricted, EU Restrint (including 2nd Evaluation by NL)			*****	*****
Safety Approvals			EN55032 Class B, FCC Part 15 Class B, ROHS				
Boot Time							
	Cold boot until operational	25s	25s	25s	25s	25s	25s
	Warm boot until operational	27s	27s	27s	27s	27s	27s

*****BSI VS-NfD, NATO restricted and EU Restrint planned/in preparation

Secunet

Management Software

User Interface	Native PC application	✔	✔	✔	✔	✔	✔
	Embedded Webapp						
	CLI	✔	✔	✔	✔	✔	✔
Initial Device Set-up							
	Local (out-of-band)	✔	✔	✔	✔	✔	✔
	Remote (out-of-band)	✔	✔	✔	✔	✔	✔
Device Configuration							
	Local (out-of-band)	✔	✔	✔	✔	✔	✔
	Remote (in-band)	✔	✔	✔	✔	✔	✔
	Remote (out-of-band)	✔	✔	✔	✔	✔	✔
Management Access							
	Role-based access	✔	✔	✔	✔	✔	✔
	Identity-based authentication of user	✔	✔	✔	✔	✔	✔
	Number of hierarchy levels	2	2	2	2	2	2
	Number of roles	5	5	5	5	5	5
	Strict internal separation of users	✔	✔	✔	✔	✔	✔
Device Management							
	Device Diagnostics	✔	✔	✔	✔	✔	✔
	Link Monitoring (SNMP)	✔	✔	✔	✔	✔	✔
	Connection Diagnostics	✔	✔	✔	✔	✔	✔
	In-band Network Diagnostics	✔	✔	✔	✔	✔	✔
	Remote Update/Upgrade	✔	✔	✔	✔	✔	✔
Certificate Authority & Management		optional	optional	optional	optional	optional	optional
	Certificate Creation	optional	optional	optional	optional	optional	optional
	Certificate Management	optional	optional	optional	optional	optional	optional
Key Management							
	Group creation	✔	✔	✔	✔	✔	✔
	Group isolation	✔	✔	✔	✔	✔	✔
	Key assignment	✔	✔	✔	✔	✔	✔
	Fail-over configuration	✔	✔	✔	✔	✔	✔

Price

List Price Encryption Unit (in €)		on request	on request	on request	on request	on request	on request
Per extermal Key Server (in €); optional, no requirement		on request	on request	on request	on request	on request	on request
Required Management Software (SINA Software optional)							
	2-10 encryptors	included	included	included	included	included	included
	11-25 encryptors	included	included	included	included	included	included
	26-50 encryptors	included	included	included	included	included	included
	51+ encryptors	included	included	included	included	included	included
Warranty Period (months)		36	36	36	36	36	36
Warranty Coverage	Parts & Work	✔	✔	✔	✔	✔	✔
	Basic Support (9 to 5, e-mail, phone)	✔	✔	✔	✔	✔	✔
	Software updates and upgrades	✔	✔	✔	✔	✔	✔
Warranty Extension (per year)		on request	on request	on request	on request	on request	on request

Securosys

	Centurion 50/100 compact	Centurion 1G compact	Centurion 100M	Centurion 1G	Centurion 10G	Centurion 40G	Centurion 100G
Line Interface/Supported Line Rates							
						Roadmap Q2 2017	Roadmap Q4 2017
10 Mbs	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP			
100 Mps	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+		
1 Gbps	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+	✔/QSFP	
10 Gbps				✔/SFP	✔/SFP+	✔/QSFP	✔/QSFP28
25Gps						✔/QSFP	✔/QSFP28
40 Gbps						✔/QSFP	✔/QSFP28
100 Gbps							✔/QSFP28
Virtual Appliance							
Supported Network Topologies							
Point-to-Point (P2P)	✔	✔	✔	✔	✔	✔	✔
Point-to-Multipoint (P2MP)	✔	✔	✔	✔	✔	✔	✔
Multipoint (MP)	✔	✔	✔	✔	✔	✔	✔
Supported Metro Ethernet Topologies							
Port-based							
Ethernet Private Line (EP-Line)	✔	✔	✔	✔	✔	✔	✔
Ethernet Private Tree (EP-Tree)	✔	✔	✔	✔	✔	✔	✔
Ethernet Private LAN (EP-LAN)	✔	✔	✔	✔	✔	✔	✔
VLAN-based							
Ethernet Virtual Private Line (EVP-Line)	✔	✔	✔	✔	✔	✔	✔
Ethernet Virtual Private Tree (EVP-Tree)	✔	✔	✔	✔	✔	✔	✔
Ethernet Virtual Private LAN (EVP-LAN)	✔	✔	✔	✔	✔	✔	✔
Supported Networks (Encryption)							
Ethernet	✔	✔	✔	✔	✔	✔	✔
MPLS	✔	✔	✔	✔	✔	✔	✔
IP v4/v6	✔	✔	✔	✔	✔	✔	✔
Supported Networks (Transport of Encrypted Frame)							
Ethernet (native)	✔	✔	✔	✔	✔	✔	✔
MPLS (EoMPLS)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6	✔	✔	✔	✔	✔	✔	✔
TCP	✔	✔	✔	✔	✔	✔	✔
UDP	✔	✔	✔	✔	✔	✔	✔
Supported Usage Scenarios							
Single tenant	✔	✔	✔	✔	✔	✔	✔
Multi-tenant	✔	✔	✔	✔	✔	✔	✔
Self-managed	✔	✔	✔	✔	✔	✔	✔
Managed encryption service	✔	✔	✔	✔	✔	✔	✔
Managed security service	✔	✔	✔	✔	✔	✔	✔
Platform							
Platform used							
Mainboard/Firmware	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia
Key Management	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia

Securosys

Data Plane Encryption Standard and Processing

Encryption Standard									
	Block Cipher	AES	AES	AES	AES	AES	AES	AES	
	Preferred Mode of Operation	GCM	GCM	GCM	GCM	GCM	GCM	GCM	
	Alternative Mode of Operation								
	Key Length (in bit)	256	256	256	256	256	256	256	
Processing Method									
	cut-through	✔	✔	✔	✔	✔	✔	✔	
	store&forward	✔	✔	✔	✔	✔	✔	✔	
Encryption Hardware									
	FPGA	✔	✔	✔	✔	✔	✔	✔	
	ASIC								
	CPU								
Latency									
Latency P2P Mode	cut-through	<42µs	<8µs	<42µs	<8µs	<4µs	<4µs	<2µs	
	store & forward	<48µs	<9µs	<48µs	<9µs	<4µs	<4µs	<2µs	
Latency MP Mode	cut-through	<42µs	<8µs	<42µs	<8µs	<4µs	<4µs	<2µs	
	store & forward	<48µs	<9µs	<48µs	<9µs	<4µs	<4µs	<2µs	

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)		✔	✔	✔	✔	✔	✔	✔	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	
	Replay protection	✔	✔	✔	✔	✔	✔	✔	
	Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
	Counter length (in bytes)	8	8	8	8	8	8	8	
	Frame overhead (unauthenticated encryption)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
	Frame overhead (authenticated encryption)	18/26	18/26	18/26	18/26	18/26	18/26	18/26	
	Ethernet multi-hop support	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
Transport (Payload only)		✔	✔	✔	✔	✔	✔	✔	
	Max. number of peers	1000	1000	1000	1000	1000	1000	1000	
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
	Max. number of VLAN IDs	256	unlimited	256	unlimited	256	unlimited	256	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	
	Replay protection	✔	✔	✔	✔	✔	✔	✔	
	Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
	Definable encryption offset (fixed)	✔	✔	✔	✔	✔	✔	✔	
	Variable encryption offset	✔	✔	✔	✔	✔	✔	✔	
	Adaptive encryption offset based on frame content	✔	✔	✔	✔	✔	✔	✔	
	Ethertype mutation (unauthenticated encryption only)	✔	✔	✔	✔	✔	✔	✔	
	Counter length (in bytes)	8	8	8	8	8	8	8	
	Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
	Frame overhead authenticated encryption (AE)	18/26	18/26	18/26	18/26	18/26	18/26	18/26	
	Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	
Tunnel (Ethernet over Ethernet)		✔	✔	✔	✔	✔	✔	✔	
	Max. number of peers	32	32	32	32	32	32	32	
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
	Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	
	Replay protection	✔	✔	✔	✔	✔	✔	✔	
	Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
	Counter length (in bytes)	8	8	8	8	8	8	8	
	Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
	Frame overhead authenticated encryption (AE)	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*	*IMIX=100%
	Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	

Securosys

Ethernet over IP (EoIP)								
Tunnel (Ethernet over IP)	✔	✔	✔	✔	✔	✔	✔	
Supported transmission protocols (UDP/TCP)	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	
Max. number of peers	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	
AAD (additional authenticated data)	✔	✔	✔	✔	✔	✔	✔	
Replay protection	✔	✔	✔	✔	✔	✔	✔	
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
Registered Ethertype	✔	✔	✔	✔	✔	✔	✔	
Counter length (in bytes)	8	8	8	8	8	8	8	
Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
Frame overhead authenticated encryption (AE)	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*	*IMIX=100%
Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	
Native IP Encryption								
Supported IP versions								
IPv4	✔	✔	✔	✔	✔	✔	✔	
IPv6	✔	✔	✔	✔	✔	✔	✔	
Supported transmission protocols								
TCP	✔	✔	✔	✔	✔	✔	✔	
UDP	✔	✔	✔	✔	✔	✔	✔	
Transport Tunnel Mode								
Maximum number of peers	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Maximum number of IP addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Maximum number of multicast groups	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	
Additional Authenticated Data (header)	✔	✔	✔	✔	✔	✔	✔	
Replay Protection	✔	✔	✔	✔	✔	✔	✔	
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
Counter length (in bytes)	8	8	8	8	8	8	8	
Packet overhead authenticated encryption (AE)	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	
Selective Encryption								
Based on MAC Address	✔	✔	✔	✔	✔	✔	✔	
Based on VLAN ID	✔	✔	✔	✔	✔	✔	✔	
Based on Ethertype	✔	✔	✔	✔	✔	✔	✔	
Based on Multicast Group	✔	✔	✔	✔	✔	✔	✔	
Based on Presence of MPLS Tag	✔	✔	✔	✔	✔	✔	✔	
Based on IP Address	✔	✔	✔	✔	✔	✔	✔	
Combination of multiple selection criteria	✔	✔	✔	✔	✔	✔	✔	
Mixed Ethernet, MPLS, EoIP and IP Support								
Based on VLAN ID								
MPLS	✔	✔	✔	✔	✔	✔	✔	
EoIP	✔	✔	✔	✔	✔	✔	✔	
IP	✔	✔	✔	✔	✔	✔	✔	
Based on presence of MPLS tag								
MPLS	✔	✔	✔	✔	✔	✔	✔	
EoIP	✔	✔	✔	✔	✔	✔	✔	
IP	✔	✔	✔	✔	✔	✔	✔	
Based on VLAN ID and presence of MPLS tag								
MPLS	✔	✔	✔	✔	✔	✔	✔	
EoIP	✔	✔	✔	✔	✔	✔	✔	
IP	✔	✔	✔	✔	✔	✔	✔	
Traffic Masking								
Traffic Flow Security	✔	✔	✔	✔	✔	✔	✔	**TFS mode only secure based on ASIC or FPGA

Securosys

Auto-discovery								
Auto-discovery of network encryptors		✔	✔	✔	✔	✔	✔	✔
Auto-discovery of key servers		✔	✔	✔	✔	✔	✔	✔
Auto-discovery of VLANs		✔	✔	✔	✔	✔	✔	✔
Disabling of auto-discovery		✔	✔	✔	✔	✔	✔	✔
Key Server								
Integrated Key Server		✔	✔	✔	✔	✔	✔	✔
Support for external Key Server		✔	✔	✔	✔	✔	✔	✔
External Key Server								
Support for multiple distributed Key Servers		✔	✔	✔	✔	✔	✔	✔
Support for fail-over to back-up Key Server		✔	✔	✔	✔	✔	✔	✔
Autonomous operation		✔	✔	✔	✔	✔	✔	✔
Key Management								
Key Generation and Storage								
Hardware Random Number Generation		✔	✔	✔	✔	✔	✔	✔
Tamper Security Key Storage (tamper-evident or tamper-proof)		TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Asymmetric Key Algorithms (Public Key Cryptography)								
RSA								
	Key length	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Elliptic Curve Cryptography (ECC)								
	Key length	512/521	512/521	512/521	512/521	512/521	512/521	512/521
Supported Curves:								
	NIST	✔	✔	✔	✔	✔	✔	✔
	Brainpool	✔	✔	✔	✔	✔	✔	✔
	Custom Curves	✔	✔	✔	✔	✔	✔	✔
Hash Algorithms								
SHA-2	Key length	512	512	512	512	512	512	512
CBC-MAC-GCM	Key length	256	256	256	256	256	256	256
Device Authentication								
Symmetric Signature: Pre-shared Key (PSK)		✔	✔	✔	✔	✔	✔	✔
	Maximum number of PSKs per encryptor	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)
	Key length	256	256	256	256	256	256	256
Asymmetric Signature: Certificate		optional	optional	optional	optional	optional	optional	optional
	Maximum number of certificates per encryptor	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)
	Key lenght	512	512	512	512	512	512	512
Ad-hoc authentication of peers (manual)		✔	✔	✔	✔	✔	✔	✔
Signature key protocol		AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****
Key Agreement and Key Exchange								
Master Key (KEK) Agreement		ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****
Master Key (KEK) Exchange Protocol		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Automatic Change of Master Key		✔	✔	✔	✔	✔	✔	✔
Minimum suggested Time Interval for Master Key Change (min)		60	60	60	60	60	60	60
Separate Master Key (KEK) per site		✔	✔	✔	✔	✔	✔	✔
Separate Master Key (KEK) per group		✔	✔	✔	✔	✔	✔	✔
Session Key (DEK) Exchange Agreement		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Session Key (DEK) Exchange Protocol		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Automatic Change of Session Keys		✔	✔	✔	✔	✔	✔	✔
Minimum Time Interval for Session Key Change (min)		1	1	1	1	1	1	1

***ECDSA optional for use with optional certificates

*****NIST, Brainpool or custom curves with 256 to 521 bit length

Securosys

Key System								
Point-to-Point Key System								
Supported key system								
	Pairwise	✔	✔	✔	✔	✔	✔	✔
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:								
	MAC Address	✔	✔	✔	✔	✔	✔	✔
	VLAN ID	✔	✔	✔	✔	✔	✔	✔
	Port	✔	✔	✔	✔	✔	✔	✔
	Group	✔	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔	✔
Point-to-Multipoint Key System								
Supported key systems:								
	Pairwise	✔	✔	✔	✔	✔	✔	✔
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:								
	MAC Address	✔	✔	✔	✔	✔	✔	✔
	VLAN ID	✔	✔	✔	✔	✔	✔	✔
	Port	✔	✔	✔	✔	✔	✔	✔
	Group	✔	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔	✔
Multipoint Key System								
Supported key systems:								
	Pairwise	✔	✔	✔	✔	✔	✔	✔
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
	Mixed (pairwise unicast, group multicast)	✔	✔	✔	✔	✔	✔	✔
Key assignment based on:								
	MAC address (pairwise and mixed)	✔	✔	✔	✔	✔	✔	✔
	Multicast groups (mixed)	✔	✔	✔	✔	✔	✔	✔
	VLAN ID (group)	✔	✔	✔	✔	✔	✔	✔
	Port	✔	✔	✔	✔	✔	✔	✔
	Group (group)	✔	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔	✔
	IP Multicast Group	✔	✔	✔	✔	✔	✔	✔
Individual key per multicast group		✔	✔	✔	✔	✔	✔	✔
Individual key per broadcast group (VLAN ID)		✔	✔	✔	✔	✔	✔	✔
Group Key System Specifics								
Additional separate authentication per group		✔	✔	✔	✔	✔	✔	✔
Group Membership Definition								
	Multicast group membership	✔	✔	✔	✔	✔	✔	✔
	Individual membership	✔	✔	✔	✔	✔	✔	✔
	Network membership	✔	✔	✔	✔	✔	✔	✔
	VLAN membership	✔	✔	✔	✔	✔	✔	✔
	Trunked VLAN membership	✔	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔	✔
Exclusion								
	MAC address	✔	✔	✔	✔	✔	✔	✔
	VLAN ID	✔	✔	✔	✔	✔	✔	✔
	Frames with MPLS tag	✔	✔	✔	✔	✔	✔	✔
	IP Address	✔	✔	✔	✔	✔	✔	✔
	IP Muticast Group	✔	✔	✔	✔	✔	✔	✔
Group Key Distribution								
	Unicast (unique KEK per group member)	✔	✔	✔	✔	✔	✔	✔
	Broadcast (same KEK for all group members)	✔	✔	✔	✔	✔	✔	✔

Securosys

Network Support								
	Bump in the Wire deployment	✔	✔	✔	✔	✔	✔	✔
	Jumbo Frame Support	✔	✔	✔	✔	✔	✔	✔
	Ethernet Flow Control via PAUSE	✔	✔	✔	✔	✔	✔	✔
	Ethernet Fragmentation/Defragmentation	✔	✔	✔	✔	✔	✔	✔
	Point-to-Point	✔	✔	✔	✔	✔	✔	✔
	Point-to-Multipoint	✔	✔	✔	✔	✔	✔	✔
	Multipoint	✔	✔	✔	✔	✔	✔	✔
	Dead Peer Detection	✔	✔	✔	✔	✔	✔	✔
	Optical Loss Pass-Through	N/A	N/A	N/A	✔	✔	✔	✔
	Link Loss Carry Forward	✔	✔	✔	✔	✔	N/A	N/A
System Configuration and Management Access								
	IPv4	✔	✔	✔	✔	✔	✔	✔
	IPv6	✔	✔	✔	✔	✔	✔	✔
	Out-of-band Management	✔	✔	✔	✔	✔	✔	✔
	RS-232/V.24	✔	✔	✔	✔	✔	✔	✔
	Separate Ethernet port	✔	✔	✔	✔	✔	✔	✔
	Smart Card (Secure Card) Support	✔	✔	✔	✔	✔	✔	✔
	USB Port						✔	✔
	In-band Management	✔	✔	✔	✔	✔	✔	✔
	SSH	✔	✔	✔	✔	✔	✔	✔
	SNMP (read-only/read-write)	read-only	read-only	read-only	read-only	read-only	read-only	read-only
	TLS							
	Proprietary	✔	✔	✔	✔	✔	✔	✔
	Remote Monitoring (SNMP)	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3
Logs								
	Event Log (local)	✔	✔	✔	✔	✔	✔	✔
	Audit Log (local)	✔	✔	✔	✔	✔	✔	✔
	Syslog Support (Server)	✔	✔	✔	✔	✔	✔	✔
Unit								
	Height in 19" Rack	1U	1U	1U	1U	1U	1U	1U
	Number of external encrypted Ethernet ports	1	1	1	1	1	1-4	1-4
	Physical Device Access	back	back	front	front	front	front	front
	Redundant Power Supply			✔	✔	✔	✔	✔
	Redundant, hot-swappable power supply			✔	✔	✔	✔	✔
	High Availability functionality (two-node cluster)	1:1	1:1	1:1	1:1	1:1	1:1	1:1
	MTBF	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h
	Tamper Security	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
	Security Approvals		*****	*****	*****	*****	*****	*****
	Safety Approvals	EN55032 Class B, FCC Part 15 Class B, ROHS						
	Boot Time							
	Cold boot until operational	25s	25s	25s	25s	25s	25s	25s
	Warm boot until operational	27s	27s	27s	27s	27s	27s	27s

***** Products using the same platform have BSI VS-NfD, NATO restricted, EU Restrint (including 2nd Evaluation by NL) approval

Securosys

Management Software								
User Interface								
	Native PC application	✔	✔	✔	✔	✔	✔	✔
	Embedded Webapp							
	CLI	✔	✔	✔	✔	✔	✔	✔
Initial Device Set-up								
	Local (out-of-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (out-of-band)	✔	✔	✔	✔	✔	✔	✔
Device Configuration								
	Local (out-of-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (in-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (out-of-band)	✔	✔	✔	✔	✔	✔	✔
Management Access								
	Role-based access	✔	✔	✔	✔	✔	✔	✔
	Identity-based authentication of user	✔	✔	✔	✔	✔	✔	✔
	Number of hierarchy levels	2	2	2	2	2	2	2
	Number of roles	5	5	5	5	5	5	5
	Strict internal separation of users	✔	✔	✔	✔	✔	✔	✔
Device Management								
	Device Diagnostics	✔	✔	✔	✔	✔	✔	✔
	Link Monitoring (SNMP)	✔	✔	✔	✔	✔	✔	✔
	Connection Diagnostics	✔	✔	✔	✔	✔	✔	✔
	In-band Network Diagnostics	✔	✔	✔	✔	✔	✔	✔
	Remote Update/Upgrade	✔	✔	✔	✔	✔	✔	✔
Certificate Authority & Management		optional	optional	optional	optional	optional	optional	optional
	Certificate Creation	optional	optional	optional	optional	optional	optional	optional
	Certificate Management	optional	optional	optional	optional	optional	optional	optional
Key Management								
	Group creation	✔	✔	✔	✔	✔	✔	✔
	Group isolation	✔	✔	✔	✔	✔	✔	✔
	Key assignment	✔	✔	✔	✔	✔	✔	✔
	Fail-over configuration	✔	✔	✔	✔	✔	✔	✔

Price								
List Price Encryption Unit (in €)		on request	on request	on request	on request	on request	on request	on request
Per external Key Server (in €); optional, no requirement		on request	on request	on request	on request	on request	on request	on request
Required Management Software								
	2-10 encryptors	included	included	included	included	included	included	included
	11-25 encryptors	included	included	included	included	included	included	included
	26-50 encryptors	included	included	included	included	included	included	included
	51+ encryptors	included	included	included	included	included	included	included
Warranty Period (months)		24	24	24	24	24	24	24
Warranty Coverage	Parts & Work	✔	✔	✔	✔	✔	✔	✔
	Basic Support (9 to 5, e-mail, phone)	on request	on request	on request	on request	on request	on request	on request
	Software updates and upgrades	on request	on request	on request	on request	on request	on request	on request
Warranty Extension (per year)		on request	on request	on request	on request	on request	on request	on request

Senetas

	CN4010	CN4020	CN6010	CN6100	CN8000	CN9100	CN9120
Line Interface/Supported Line Rates							
10 Mbs	✔/RJ45	✔/SFP	✔/RJ45/SFP				
100 Mps	✔/RJ45	✔/SFP	✔/RJ45/SFP				
1 Gbps	✔/RJ45	✔/SFP	✔/RJ45/SFP	✔/SFP	✔/SFP+		
10 Gbps				✔/SFP	✔/SFP+		
25Gps							
40 Gbps					✔/SFP+		
100 Gbps					✔/SFP+	✔/CFP-4	✔/QSFP-28
					up to 10 cards at up to 10G each		
Virtual Appliance							
Supported Network Topologies							
Point-to-Point (P2P)	✔	✔	✔	✔	✔	✔	✔
Point-to-Multipoint (P2MP)	✔	✔	✔	✔	✔	✔	✔
Multipoint (MP)	✔	✔	✔	✔	✔	✔	✔
Supported Metro Ethernet Topologies							
Port-based							
Ethernet Private Line (EP-Line)	✔	✔	✔	✔	✔	✔	✔
Ethernet Private Tree (EP-Tree)	✔	✔	✔	✔	✔	✔	✔
Ethernet Private LAN (EP-LAN)	✔	✔	✔	✔	✔	✔	✔
VLAN-based							
Ethernet Virtual Private Line (EVP-Line)	✔	✔	✔	✔	✔	✔	✔
Ethernet Virtual Private Tree (EVP-Tree)	✔	✔	✔	✔	✔	✔	✔
Ethernet Virtual Private LAN (EVP-LAN)	✔	✔	✔	✔	✔	✔	✔
Supported Networks (Encryption)							
Ethernet	✔	✔	✔	✔	✔	✔	✔
MPLS (MPLSoE)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6							
Supported Networks (Transport of Encrypted Frame)							
Ethernet (native)	✔	✔	✔	✔	✔	✔	✔
MPLS (EoMPLS)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
TCP	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
UDP	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
Supported Usage Scenarios							
Single tenant	✔	✔	✔	✔	✔	✔	✔
Multi-tenant	*	*	*	*	✔/one tenant per port	*	
Self-managed	✔	✔	✔	✔	✔	✔	✔
Managed encryption service	✔	✔	✔	✔	✔	✔	✔
Managed security service	✔	✔	✔	✔	✔	✔	✔
Platform							
Platform used							
Mainboard/Firmware	Senetas/Senetas	Senetas/Senetas	Senetas/Senetas	Senetas/Senetas	Senetas/IDQuantique	Senetas/Senetas	Senetas/Senetas
Key Management	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas

* IP support only in combination with TRANSEC and limited to P2P. Additional overhead and latency.
* Multi-tenancy support based on certificates. Requires common trust domain of multiple CAs or use of a single CA

Senetas

Data Plane Encryption Standard and Processing

Encryption Standard								
	Block Cipher	AES	AES	AES	AES	AES	AES	AES
	Preferred Mode of Operation	GCM	GCM	GCM	GCM	GCM	CTR	CTR
	Alternative Mode of Operation	CFB/CTR	CFB/CTR	CFB/CTR	CFB/CTR	CFB/CTR	GCM (Roadmap Q4 2017)	GCM (Roadmap Q4 2017)
	Key Length (in bit)	128/256	128/256	128/256	128/256	128/256	128/256	128/256
Processing Method								
	cut-through	✔	✔	✔	✔	✔		
	store&forward	*	*	*	*	*	✔	✔
Encryption Hardware								
	FPGA	✔	✔	✔	✔	✔	✔	✔
	ASIC							
	CPU							
Latency								
Latency P2P Mode	cut-through	<10µs (@1Gbps)	<10µs (@1Gbps)	<10µs	<5µs	<5µs		
	store & forward	*	*	*	*	*	<2µs	<2µs
Latency MP Mode	cut-through	<10µs (@1Gbps)	<10µs (@1Gbps)	<10µs	<5µs	<5µs		
	store & forward	*	*	*	*	*	<2µs	<2µs

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)		*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM			
	Authentication length (bytes)	16	16	16	16			
	Replay protection	✔	✔	✔	✔			
	Variable replay window (size)	256 frames	256 frames	256 frames	256 frames			
	Counter length (in bytes)	5	5	5	5			
	Frame overhead (unauthenticated encryption)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)			
	Frame overhead (authenticated encryption)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)			
	Ethernet multi-hop support	✔	✔	✔	✔			
Transport (Payload only)		✔	✔	✔	✔	✔	✔	✔	
	Max. number of peers	512	512	512	512	512	512	512	
	Max. number of MAC Addresses	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	limitation only in MAC mode
	Max. number of VLAN IDs	256	256	256	512	512	512	512	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	*GCM (Roadmap Q4 2017)	*GCM (Roadmap Q4 2017)	
	Authentication length (bytes)	16	16	16	16	16	16	16	
	Replay protection	✔	✔	✔	✔	✔	✔	✔	
	Variable replay window (size)	256 frames	256 frames	256 frames	256 frames	256 frames	256 frames	256 frames	
	Definable encryption offset (fixed)	✔	✔	✔	✔	✔	✔	✔	
	Variable encryption offset	✔	✔	✔	✔	✔	✔	✔	
	Adaptive encryption offset based on frame content	✔	✔	✔	✔	✔	✔	✔	
	Ethertype mutation	✔	✔	✔	✔	✔	✔	✔	
	Counter length (in bytes)	5	5	5	5	5	5	5	
	Frame overhead unauthenticated encryption	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	8 (CTR)	8 (CTR)	
	Frame overhead authenticated encryption (AE)	24	24	24	24	24	24*	24*	*GCM (Roadmap Q4 2017)
	Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	
Tunnel (Ethernet over Ethernet)		*	*	*	*	*	* Roadmap Q4 2017	* Roadmap Q4 2017	
	Max. number of peers	2	2	2	2				
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited				
	Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited				
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM				
	Authentication length (bytes)	16	16	16	16				
	Replay protection	✔	✔	✔	✔				
	Variable replay window (size)	256 frames	256 frames	256 frames	256 frames				
	Counter length (in bytes)	5	5	5	5				
	Frame overhead unauthenticated encryption	8 (CTR)	8 (CTR)	8 (CTR)	8 (CTR)				
	Frame overhead authenticated encryption (AE)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)				
	Ethernet multi-hop support	✔	✔	✔	✔				

Senetas

Ethernet over IP (EoIP)							
Tunnel (Ethernet over IP)	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
Supported transmission protocols (UDP/TCP)	UDP/TCP	UDP/TCP	UDP/TCP	UDP/TCP			
Max. number of peers	2	2	2	2			
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited			
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited			
Integrity protection (algorithm)	GCM	GCM	GCM	GCM			
Authentication length (bytes)	16	16	16	16			
Replay protection	✔	✔	✔	✔			
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames			
Counter length (in bytes)	5	5	5	5			
Frame overhead unauthenticated encryption	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38 bytes)			
Frame overhead authenticated encryption (AE)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)			
Ethernet multi-hop support	✔	✔	✔	✔			
Native IP Encryption							
Supported IP versions							
IPv4							
IPv6							
Supported transmission protocols							
TCP							
UDP							
Transport/Tunnel Mode							
Mximum number of peers							
Maximum number of IP addresses							
Maximum number of multicast groups							
Integrity protection (algorithm)							
Authentication length (bytes)							
Additional Authenticated Data (header)							
Replay Protection							
Variable replay window (size)							
Counter length (in bytes)							
Packet overhead authenticated encryption (AE)							
Selective Encryption							
Based on MAC Address	✔	✔	✔	✔	✔	✔	✔
Based on VLAN ID	✔	✔	✔	✔	✔	✔	✔
Based on Ethertype	✔	✔	✔	✔	✔	✔	✔
Based on Multicast Group	✔	✔	✔	✔	✔	✔	✔
Based on Presence of MPLS Tag							
Based on IP Address							
Combination of multiple selection criteria	✔	✔	✔	✔	✔	✔	✔
Mixed Ethernet, MPLS, EoIP and IP Support							
Based on VLAN ID							
MPLS	✔	✔	✔	✔	✔	✔	✔
EoIP							
IP							
Based on presence of MPLS tag							
MPLS							
EoIP							
IP							
Based on VLAN ID and presence of MPLS tag							
MPLS							
EoIP							
IP							
Traffic Masking							
Traffic Flow Security	✔	✔	✔	✔		Roadmap Q4 2017	Roadmap Q4 2017

Senetas

Auto-discovery							
Auto-discovery of network encryptors	✔	✔	✔	✔	✔	✔	✔
Auto-discovery of key servers	✔	✔	✔	✔	✔	✔	✔
Auto-discovery of VLANs	✔	✔	✔	✔	✔	✔	✔
Disabling of auto-discovery	✔	✔	✔	✔	✔	✔	✔
Key Server							
Integrated Key Server	✔	✔	✔	✔	✔	✔	✔
Support for external Key Server	✔	✔	✔	✔	✔	✔	✔
External Key Server							
Support for multiple distributed Key Servers	✔	✔	✔	✔	✔	✔	✔
Support for fail-over to back-up Key Server	✔	✔	✔	✔	✔	✔	✔
Autonomous operation	✔	✔	✔	✔	✔	✔	✔
Key Management							
Key Generation and Storage							
Hardware Random Number Generation	✔	✔	✔	✔	✔/QRNG	✔QRNG	✔/QRNG
Tamper Security Key Storage (tamper-evident or tamper-proof)	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Asymmetric Key Algorithms (Public Key Cryptography)							
RSA							
Key length	2048	2048	2048	2048	2048	2048	2048
Elliptic Curve Cryptography (ECC)							
Key length	512	512	512	512	512	512	512
Supported Curves:							
NIST	✔	✔	✔	✔	✔	✔	✔
Brainpool	✔	✔	✔	✔	✔	✔	✔
Custom Curves	✔	✔	✔	✔	✔	✔	✔
Hash Algorithms							
SHA-2 Key length	512	512	512	512	512	512	512
Device Authentication							
Symmetric Signature: Pre-shared Key (PSK)							
Maximum number of PSKs per encryptor							
Key length							
Asymmetric Signature: Certificate	x.509	x.509	x.509	x.509	x.509	x.509	x.509
Maximum number of certificates per encryptor	64	64	64	64	64	64	64
Key length	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)
Ad-hoc authentication of peers (manual)							
Signature key protocol	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA
Key Agreement and Key Exchange							
Master Key (KEK) Agreement	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA
Master Key (KEK) Exchange Protocol	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas
Automatic Change of Master Key	✔	✔	✔	✔	✔	✔	✔
Minimum suggested Time Interval for Master Key Change (min)	1440	1440	1440	1440	1440	1440	1440
Separate Master Key (KEK) per site	✔	✔	✔	✔	✔	✔	✔
Separate Master Key (KEK) per group	✔	✔	✔	✔	✔	✔	✔
Session Key (DEK) Exchange Agreement	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications
Session Key (DEK) Exchange Protocol	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A
Automatic Change of Session Keys	✔	✔	✔	✔	✔	✔	✔
Minimum Time Interval for Session Key Change (min)	1	1	1	1	1	1	1

Senetas

Key System							
Point-to-Point Key System							
Supported key system							
Pairwise	✔	✔	✔	✔	✔	✔	✔
Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:							
MAC Address	✔	✔	✔	✔	✔	✔	✔
VLAN ID	✔	✔	✔	✔	✔	✔	✔
Port	✔	✔	✔	✔	✔	✔	✔
Group	✔	✔	✔	✔	✔	✔	✔
IP Address							
Point-to-Multipoint Key System							
Supported key systems:							
Pairwise	✔	✔	✔	✔	✔	✔	✔
Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:							
MAC Address	✔	✔	✔	✔	✔	✔	✔
VLAN ID	✔	✔	✔	✔	✔	✔	✔
Port	✔	✔	✔	✔	✔	✔	✔
Group	✔	✔	✔	✔	✔	✔	✔
IP Address							
Multipoint Key System							
Supported key systems:							
Pairwise	✔	✔	✔	✔	✔	✔	✔
Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Mixed (pairwise unicast, group multicast)	✔	✔	✔	✔	✔	✔	✔
Key assignment based on:							
MAC address (pairwise and mixed)	✔	✔	✔	✔	✔	✔	✔
Multicast groups (mixed)	✔	✔	✔	✔	✔	✔	✔
VLAN ID (group)	✔	✔	✔	✔	✔	✔	✔
Port	✔	✔	✔	✔	✔	✔	✔
Group (group)	✔	✔	✔	✔	✔	✔	✔
IP Address							
IP Multicast Group							
Individual key per multicast group	✔	✔	✔	✔	✔	✔	✔
Individual key per broadcast group (VLAN ID)	✔	✔	✔	✔	✔	✔	✔
Group Key System Specifics							
Additional separate authentication per group	✔	✔	✔	✔	✔	✔	✔
Group Membership Definition							
Multicast group membership	✔	✔	✔	✔	✔	✔	✔
Individual membership							
Network membership	✔	✔	✔	✔	✔	✔	✔
VLAN membership	✔	✔	✔	✔	✔	✔	✔
Trunked VLAN membership	✔	✔	✔	✔	✔	✔	✔
IP Address							
Exclusion							
MAC address	✔	✔	✔	✔	✔	✔	✔
VLAN ID	✔	✔	✔	✔	✔	✔	✔
Frames with MPLS tag							
IP Address							
IP Muticast Group							
Group Key Distribution							
Unicast (unique KEK per group member)	✔	✔	✔	✔	✔	✔	✔
Broadcast (same KEK for all group members)	✔	✔	✔	✔	✔	✔	✔

Senetas

Network Support							
Bump in the Wire deployment	✔	✔	✔	✔	✔	✔	✔
Jumbo Frame Support	✔	✔	✔	✔	✔	✔	✔
Ethernet Flow Control via PAUSE							
Ethernet Fragmentation/Defragmentation							
Point-to-Point							
Point-to-Multipoint							
Multipoint							
Dead Peer Detection	✔	✔	✔	✔	✔	✔	✔
Optical Loss Pass-Through		✔	✔	✔	✔	✔	✔
Link Loss Carry Forward	✔	✔	✔	✔	✔	✔	✔
System Configuration and Management Access							
IPv4	✔	✔	✔	✔	✔	✔	✔
IPv6	✔	✔	✔	✔	✔	✔	✔
Out-of-band Management	✔	✔	✔	✔	✔	✔	✔
RS-232/V.24	✔						
Separate Ethernet port	✔	✔	✔	✔	✔	✔	✔
Smart Card (Secure Card) Support							
USB Port	✔	✔	✔	✔	✔	✔	✔
In-band Management	✔	✔	✔	✔	✔	✔	✔
SSH	✔	✔	✔	✔	✔	✔	✔
SNMP (read-only/read-write)	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW
TLS							
Proprietary							
Remote Monitoring (SNMP)	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3
Logs							
Event Log (local)	✔	✔	✔	✔	✔	✔	✔
Audit Log (local)	✔	✔	✔	✔	✔	✔	✔
Syslog Support (Server)	✔	✔	✔	✔	✔	✔	✔
Unit							
Height in 19" Rack	Desktop	Desktop	1U	1U	4U	1U	1U
Number of external encrypted Ethernet ports	1	1	1	1	1-10	1	1
Physical Device Access	back	back	front	front	front	front	front
Redundant Power Supply			✔	✔	✔	✔	✔
Redundant, hot-swappable power supply			✔	✔	✔	✔	✔
High Availability functionality (two-node cluster)	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017
MTBF	> 200.000h	> 200.000h	> 200.000h	> 200.000h	> 100.000h	> 200.000h	> 200.000h
Tamper Security	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Security Approvals	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+	FIPS140-2 L3/CC EAL2+ in progress	*
Safety Approvals	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000 ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS
Boot Time							
Cold boot until operational (P2P)	65s	65s	65s	65s	65s	65s	65s
Warm boot until operational (P2P)	80s	80s	80s	80s	80s	80s	80s

CC EAL2+, FIPS 140-2 L3, UC APL/CPA in progress/planned

* For CN 9100 CC EAL2+ in progress, for CN 9120, FIPS 140-2 L3 and CC EAL2+ planned. For both: UC APL and NATO planned

Senetas

Management Software								
User Interface	Native PC application	✔	✔	✔	✔	✔	✔	✔
	Embedded Webapp							
	CLI	✔	✔	✔	✔	✔	✔	✔
Initial Device Set-up								
	Local (out-of-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (out-of-band)	✔	✔	✔	✔	✔	✔	✔
Device Configuration								
	Local (out-of-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (in-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (out-of-band)	✔	✔	✔	✔	✔	✔	✔
Management Access								
	Role-based access	✔	✔	✔	✔	✔	✔	✔
	Identity-based authentication of user	✔	✔	✔	✔	✔	✔	✔
	Number of hierarchy levels	2	2	2	2	2	2	2
	Number of roles	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)
	Strict internal separation of users	✔	✔	✔	✔	✔	✔	✔
Device Management								
	Device Diagnostics	✔	✔	✔	✔	✔	✔	✔
	Link Monitoring (SNMP)	✔	✔	✔	✔	✔	✔	✔
	Connection Diagnostics	✔	✔	✔	✔	✔	✔	✔
	In-band Network Diagnostics	✔	✔	✔	✔	✔	✔	✔
	Remote Update/Upgrade	✔	✔	✔	✔	✔	✔	✔
Certificate Authority & Management								
	Certificate Creation	✔	✔	✔	✔	✔	✔	✔
	Certificate Management	✔	✔	✔	✔	✔	✔	✔
Key Management								
	Group creation	✔	✔	✔	✔	✔	✔	✔
	Group isolation	✔	✔	✔	✔	✔	✔	✔
	Key assignment	✔	✔	✔	✔	✔	✔	✔
	Fail-over configuration	✔	✔	✔	✔	✔	✔	✔
Price								
List Price Encryption Unit (in €)		on request	on request	on request	on request	on request	on request	on request
Per external Key Server (in €); optional, no requirement, starting price		on request	on request	on request	on request	on request	on request	on request
Required Management Software		CM7 included	CM7 included	CM7 included	CM7 included	CM7 included	CM7 included	CM7 included
Optional SMC Sofware	1-4 encryptors	free	free	free	free	free	free	free
	5-10 encryptors	on request	on request	on request	on request	on request	on request	on request
	11-20 encryptors	on request	on request	on request	on request	on request	on request	on request
	unlimited	on request	on request	on request	on request	on request	on request	on request
Warranty Period (months)		12	12	12	12	12	12	12
Warranty Coverage	Parts & Work	✔	✔	✔	✔	✔	✔	✔
	Basic Support (9 to 5, e-mail, phone)	✔	✔	✔	✔	✔	✔	✔
	Software updates and upgrades	✔	✔	✔	✔	✔	✔	✔
Warranty Extension (per year)		15%	15%	15%	15%	15%	15%	15%%

* Additionally available: Premium support (24x7 support, Advance RMA) with Plus Maintenance

Thales E-Security

	Datacryptor 5100	Datacryptor 5100	Datacryptor 5200	Datacryptor 5300	Datacryptor 5400	40G	100G
Line Interface/Supported Line Rates							
						Roadmap Q2 2017	Roadmap Q4 2017
10 Mbs	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP			
100 Mps	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+		
1 Gbps	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+	✔/QSFP	
10 Gbps				✔/SFP	✔/SFP+	✔/QSFP	✔/QSFP28
25Gps						✔/QSFP	✔/QSFP28
40 Gbps						✔/QSFP	✔/QSFP28
100 Gbps							✔/QSFP28
Virtual Appliance							
Supported Network Topologies							
Point-to-Point (P2P)	✔	✔	✔	✔	✔	✔	✔
Point-to-Multipoint (P2MP)	✔	✔	✔	✔	✔	✔	✔
Multipoint (MP)	✔	✔	✔	✔	✔	✔	✔
Supported Metro Ethernet Topologies							
Port-based							
Ethernet Private Line (EP-Line)	✔	✔	✔	✔	✔	✔	✔
Ethernet Private Tree (EP-Tree)	✔	✔	✔	✔	✔	✔	✔
Ethernet Private LAN (EP-LAN)	✔	✔	✔	✔	✔	✔	✔
VLAN-based							
Ethernet Virtual Private Line (EVP-Line)	✔	✔	✔	✔	✔	✔	✔
Ethernet Virtual Private Tree (EVP-Tree)	✔	✔	✔	✔	✔	✔	✔
Ethernet Virtual Private LAN (EVP-LAN)	✔	✔	✔	✔	✔	✔	✔
Supported Networks (Encryption)							
Ethernet	✔	✔	✔	✔	✔	✔	✔
MPLS	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6	✔	✔	✔	✔	✔	✔	✔
Supported Networks (Transport of Encrypted Frame)							
Ethernet (native)	✔	✔	✔	✔	✔	✔	✔
MPLS (EoMPLS)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6	✔	✔	✔	✔	✔	✔	✔
TCP	✔	✔	✔	✔	✔	✔	✔
UDP	✔	✔	✔	✔	✔	✔	✔
Supported Usage Scenarios							
Single tenant	✔	✔	✔	✔	✔	✔	✔
Multi-tenant	✔	✔	✔	✔	✔	✔	✔
Self-managed	✔	✔	✔	✔	✔	✔	✔
Managed encryption service	✔	✔	✔	✔	✔	✔	✔
Managed security service	✔	✔	✔	✔	✔	✔	✔
Platform							
Platform used							
Mainboard/Firmware	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia
Key Management	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia

Thales E-Security

Data Plane Encryption Standard and Processing

Encryption Standard									
	Block Cipher	AES	AES	AES	AES	AES	AES	AES	
	Preferred Mode of Operation	GCM	GCM	GCM	GCM	GCM	GCM	GCM	
	Alternative Mode of Operation								
	Key Length (in bit)	256	256	256	256	256	256	256	
Processing Method									
	cut-through	✔	✔	✔	✔	✔	✔	✔	
	store&forward	✔	✔	✔	✔	✔	✔	✔	
Encryption Hardware									
	FPGA	✔	✔	✔	✔	✔	✔	✔	
	ASIC								
	CPU								
Latency									
Latency P2P Mode	cut-through	<42µs	<8µs	<42µs	<8µs	<4µs	<4µs	<2µs	
	store & forward	<48µs	<9µs	<48µs	<9µs	<4µs	<4µs	<2µs	
Latency MP Mode	cut-through	<42µs	<8µs	<42µs	<8µs	<4µs	<4µs	<2µs	
	store & forward	<48µs	<9µs	<48µs	<9µs	<4µs	<4µs	<2µs	

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)		✔	✔	✔	✔	✔	✔	✔	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	
	Replay protection	✔	✔	✔	✔	✔	✔	✔	
	Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
	Counter length (in bytes)	8	8	8	8	8	8	8	
	Frame overhead (unauthenticated encryption)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
	Frame overhead (authenticated encryption)	18/26	18/26	18/26	18/26	18/26	18/26	18/26	
Transport (Payload only)		✔	✔	✔	✔	✔	✔	✔	
	Max. number of peers	1000	1000	1000	1000	1000	1000	1000	
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
	Max. number of VLAN IDs	256	unlimited	256	unlimited	256	unlimited	256	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	
	Replay protection	✔	✔	✔	✔	✔	✔	✔	
	Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
	Definable encryption offset (fixed)	✔	✔	✔	✔	✔	✔	✔	
	Variable encryption offset	✔	✔	✔	✔	✔	✔	✔	
	Adaptive encryption offset based on frame content	✔	✔	✔	✔	✔	✔	✔	
	Ethertype mutation (unauthenticated encryption only)	✔	✔	✔	✔	✔	✔	✔	
	Counter length (in bytes)	8	8	8	8	8	8	8	
	Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
	Frame overhead authenticated encryption (AE)	18/26	18/26	18/26	18/26	18/26	18/26	18/26	
	Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	
Tunnel (Ethernet over Ethernet)		✔	✔	✔	✔	✔	✔	✔	
	Max. number of peers	32	32	32	32	32	32	32	
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
	Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	
	Replay protection	✔	✔	✔	✔	✔	✔	✔	
	Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
	Counter length (in bytes)	8	8	8	8	8	8	8	
	Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
	Frame overhead authenticated encryption (AE)	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*	*IMIX=100%
	Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	

Thales E-Security

Ethernet over IP (EoIP)								
Tunnel (Ethernet over IP)	✔	✔	✔	✔	✔	✔	✔	
Supported transmission protocols (UDP/TCP)	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	
Max. number of peers	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	
Replay protection	✔	✔	✔	✔	✔	✔	✔	
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
Counter length (in bytes)	8	8	8	8	8	8	8	
Frame overhead authenticated encryption (AE)	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*	*IMIX=100%
Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	
Native IP Encryption								
Supported IP versions								
IPv4	✔	✔	✔	✔	✔	✔	✔	
IPv6	✔	✔	✔	✔	✔	✔	✔	
Supported transmission protocols								
TCP	✔	✔	✔	✔	✔	✔	✔	
UDP	✔	✔	✔	✔	✔	✔	✔	
Transport Tunnel Mode								
Maximum number of peers	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Maximum number of IP addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Maximum number of multicast groups	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	
Additional Authenticated Data (header)	✔	✔	✔	✔	✔	✔	✔	
Replay Protection	✔	✔	✔	✔	✔	✔	✔	
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	
Counter length (in bytes)	8	8	8	8	8	8	8	
Packet overhead authenticated encryption (AE)	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	
Selective Encryption								
Based on MAC Address	✔	✔	✔	✔	✔	✔	✔	
Based on VLAN ID	✔	✔	✔	✔	✔	✔	✔	
Based on Ethertype	✔	✔	✔	✔	✔	✔	✔	
Based on Multicast Group	✔	✔	✔	✔	✔	✔	✔	
Based on Presence of MPLS Tag	✔	✔	✔	✔	✔	✔	✔	
Based on IP Address	✔	✔	✔	✔	✔	✔	✔	
Combination of multiple selection criteria	✔	✔	✔	✔	✔	✔	✔	
Mixed Ethernet, MPLS, EoIP and IP Support								
Based on VLAN ID								
MPLS	✔	✔	✔	✔	✔	✔	✔	
EoIP	✔	✔	✔	✔	✔	✔	✔	
IP	✔	✔	✔	✔	✔	✔	✔	
Based on presence of MPLS tag								
MPLS	✔	✔	✔	✔	✔	✔	✔	
EoIP	✔	✔	✔	✔	✔	✔	✔	
IP	✔	✔	✔	✔	✔	✔	✔	
Based on VLAN ID and presence of MPLS tag								
MPLS	✔	✔	✔	✔	✔	✔	✔	
EoIP	✔	✔	✔	✔	✔	✔	✔	
IP	✔	✔	✔	✔	✔	✔	✔	
Traffic Masking								
Traffic Flow Security	✔	✔	✔	✔	✔	✔	✔	

**TFS mode only secure based on ASIC or FPGA

Thales E-Security

Auto-discovery							
Auto-discovery of network encryptors	✔	✔	✔	✔	✔	✔	✔
Auto-discovery of key servers	✔	✔	✔	✔	✔	✔	✔
Auto-discovery of VLANs	✔	✔	✔	✔	✔	✔	✔
Disabling of auto-discovery	✔	✔	✔	✔	✔	✔	✔
Key Server							
Integrated Key Server	✔	✔	✔	✔	✔	✔	✔
Support for external Key Server	✔	✔	✔	✔	✔	✔	✔
External Key Server							
Support for multiple distributed Key Servers	✔	✔	✔	✔	✔	✔	✔
Support for fail-over to back-up Key Server	✔	✔	✔	✔	✔	✔	✔
Autonomous operation	✔	✔	✔	✔	✔	✔	✔
Key Management							
Key Generation and Storage							
Hardware Random Number Generation	✔	✔	✔	✔	✔	✔	✔
Tamper Security Key Storage (tamper-evident or tamper-proof)	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Asymmetric Key Algorithms (Public Key Cryptography)							
RSA							
Key length	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Elliptic Curve Cryptography (ECC)							
Key length	512/521	512/521	512/521	512/521	512/521	512/521	512/521
Supported Curves:							
NIST	✔	✔	✔	✔	✔	✔	✔
Brainpool	✔	✔	✔	✔	✔	✔	✔
Custom Curves	✔	✔	✔	✔	✔	✔	✔
Hash Algorithms							
SHA-2 Key length	512	512	512	512	512	512	512
CBC-MAC-GCM Key length	256	256	256	256	256	256	256
Device Authentication							
Symmetric Signature: Pre-shared Key (PSK)	✔	✔	✔	✔	✔	✔	✔
Maximum number of PSKs per encryptor	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)
Key length	256	256	256	256	256	256	256
Asymmetric Signature: Certificate	optional	optional	optional	optional	optional	optional	optional
Maximum number of certificates per encryptor	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)
Key lenght	512	512	512	512	512	512	512
Ad-hoc authentication of peers (manual)	✔	✔	✔	✔	✔	✔	✔
Signature key protocol	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****
Key Agreement and Key Exchange							
Master Key (KEK) Agreement	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****
Master Key (KEK) Exchange Protocol	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Automatic Change of Master Key	✔	✔	✔	✔	✔	✔	✔
Minimum suggested Time Interval for Master Key Change (min)	60	60	60	60	60	60	60
Separate Master Key (KEK) per site	✔	✔	✔	✔	✔	✔	✔
Separate Master Key (KEK) per group	✔	✔	✔	✔	✔	✔	✔
Session Key (DEK) Exchange Agreement	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Session Key (DEK) Exchange Protocol	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Automatic Change of Session Keys	✔	✔	✔	✔	✔	✔	✔
Minimum Time Interval for Session Key Change (min)	1	1	1	1	1	1	1

***ECDSA optional for use with optional certificates
*****NIST, Brainpool or custom curves with 256 to 521 bit length

Thales E-Security

Key System							
Point-to-Point Key System							
Supported key system							
Pairwise	✔	✔	✔	✔	✔	✔	✔
Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:							
MAC Address	✔	✔	✔	✔	✔	✔	✔
VLAN ID	✔	✔	✔	✔	✔	✔	✔
Port	✔	✔	✔	✔	✔	✔	✔
Group	✔	✔	✔	✔	✔	✔	✔
IP Address	✔	✔	✔	✔	✔	✔	✔
Point-to-Multipoint Key System							
Supported key systems:							
Pairwise	✔	✔	✔	✔	✔	✔	✔
Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:							
MAC Address	✔	✔	✔	✔	✔	✔	✔
VLAN ID	✔	✔	✔	✔	✔	✔	✔
Port	✔	✔	✔	✔	✔	✔	✔
Group	✔	✔	✔	✔	✔	✔	✔
IP Address	✔	✔	✔	✔	✔	✔	✔
Multipoint Key System							
Supported key systems:							
Pairwise	✔	✔	✔	✔	✔	✔	✔
Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Mixed (pairwise unicast, group multicast)	✔	✔	✔	✔	✔	✔	✔
Key assignment based on:							
MAC address (pairwise and mixed)	✔	✔	✔	✔	✔	✔	✔
Multicast groups (mixed)	✔	✔	✔	✔	✔	✔	✔
VLAN ID (group)	✔	✔	✔	✔	✔	✔	✔
Port	✔	✔	✔	✔	✔	✔	✔
Group (group)	✔	✔	✔	✔	✔	✔	✔
IP Address	✔	✔	✔	✔	✔	✔	✔
IP Multicast Group	✔	✔	✔	✔	✔	✔	✔
Individual key per multicast group	✔	✔	✔	✔	✔	✔	✔
Individual key per broadcast group (VLAN ID)	✔	✔	✔	✔	✔	✔	✔
Group Key System Specifics							
Additional separate authentication per group	✔	✔	✔	✔	✔	✔	✔
Group Membership Definition							
Multicast group membership	✔	✔	✔	✔	✔	✔	✔
Individual membership	✔	✔	✔	✔	✔	✔	✔
Network membership	✔	✔	✔	✔	✔	✔	✔
VLAN membership	✔	✔	✔	✔	✔	✔	✔
Trunked VLAN membership	✔	✔	✔	✔	✔	✔	✔
IP Address	✔	✔	✔	✔	✔	✔	✔
Exclusion							
MAC address	✔	✔	✔	✔	✔	✔	✔
VLAN ID	✔	✔	✔	✔	✔	✔	✔
Frames with MPLS tag	✔	✔	✔	✔	✔	✔	✔
IP Address	✔	✔	✔	✔	✔	✔	✔
IP Muticast Group	✔	✔	✔	✔	✔	✔	✔
Group Key Distribution							
Unicast (unique KEK per group member)	✔	✔	✔	✔	✔	✔	✔
Broadcast (same KEK for all group members)	✔	✔	✔	✔	✔	✔	✔

Thales E-Security

Network Support								
Bump in the Wire deployment		✔	✔	✔	✔	✔	✔	✔
Jumbo Frame Support		✔	✔	✔	✔	✔	✔	✔
Ethernet Flow Control via PAUSE		✔	✔	✔	✔	✔	✔	✔
Ethernet Fragmentation/Defragmentation		✔	✔	✔	✔	✔	✔	✔
	Point-to-Point	✔	✔	✔	✔	✔	✔	✔
	Point-to-Multipoint	✔	✔	✔	✔	✔	✔	✔
	Multipoint	✔	✔	✔	✔	✔	✔	✔
Dead Peer Detection		✔	✔	✔	✔	✔	✔	✔
Optical Loss Pass-Through		N/A	N/A	N/A	✔	✔	✔	✔
Link Loss Carry Forward		✔	✔	✔	✔	✔	N/A	N/A
System Configuration and Management Access								
IPv4		✔	✔	✔	✔	✔	✔	✔
IPv6		✔	✔	✔	✔	✔	✔	✔
Out-of-band Management		✔	✔	✔	✔	✔	✔	✔
	RS-232/V.24	✔	✔	✔	✔	✔	✔	✔
	Separate Ethernet port	✔	✔	✔	✔	✔	✔	✔
Smart Card (Secure Card) Support		✔	✔	✔	✔	✔	✔	✔
USB Port							✔	✔
In-band Management		✔	✔	✔	✔	✔	✔	✔
	SSH	✔	✔	✔	✔	✔	✔	✔
	SNMP (read-only/read-write)	read-only	read-only	read-only	read-only	read-only	read-only	read-only
	TLS							
	Proprietary	✔	✔	✔	✔	✔	✔	✔
Remote Monitoring (SNMP)		v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3
Logs								
Event Log (local)		✔	✔	✔	✔	✔	✔	✔
Audit Log (local)		✔	✔	✔	✔	✔	✔	✔
Syslog Support (Server)		✔	✔	✔	✔	✔	✔	✔
Unit								
Height in 19" Rack		1U	1U	1U	1U	1U	1U	1U
Number of external encrypted Ethernet ports		1	1	1	1	1	1-4	1-4
Physical Device Access		back	back	front	front	front	front	front
Redundant Power Supply				✔	✔	✔	✔	✔
Redundant, hot-swappable power supply				✔	✔	✔	✔	✔
High Availability functionality (two-node cluster)		1:1	1:1	1:1	1:1	1:1	1:1	1:1
MTBF		> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h
Tamper Security		TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Security Approvals *		FIPS 140-2 L3 in progress	FIPS 140-2 L3 in progress	FIPS 140-2 L3 in progress	FIPS 140-2 L3 in progress	FIPS 140-2 L3 in progress	FIPS 140-2 L3 iplanned	FIPS 140-2 L3 planned
Safety Approvals		EN55032 Class B, FCC Part 15 Class B, ROHS						
Boot Time								
	Cold boot until operational	25s	25s	25s	25s	25s	25s	25s
	Warm boot until operational	27s	27s	27s	27s	27s	27s	27s

* Products using the platform have BSI VS-NfD, NATO restricted, EU Restrint (including 2nd Evaluation by NL) approvals

Thales E-Seccurity

Management Software								
User Interface								✔
	Native PC application	✔	✔	✔	✔	✔	✔	✔
	Embedded Webapp							
	CLI	✔	✔	✔	✔	✔	✔	✔
Initial Device Set-up								
	Local (out-of-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (out-of-band)	✔	✔	✔	✔	✔	✔	✔
Device Configuration								
	Local (out-of-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (in-band)	✔	✔	✔	✔	✔	✔	✔
	Remote (out-of-band)	✔	✔	✔	✔	✔	✔	✔
Management Access								
	Role-based access	✔	✔	✔	✔	✔	✔	✔
	Identity-based authentication of user	✔	✔	✔	✔	✔	✔	✔
	Number of hierarchy levels	2	2	2	2	2	2	2
	Number of roles	5	5	5	5	5	5	5
	Strict internal separation of users	✔	✔	✔	✔	✔	✔	✔
Device Management								
	Device Diagnostics	✔	✔	✔	✔	✔	✔	✔
	Link Monitoring (SNMP)	✔	✔	✔	✔	✔	✔	✔
	Connection Diagnostics	✔	✔	✔	✔	✔	✔	✔
	In-band Network Diagnostics	✔	✔	✔	✔	✔	✔	✔
	Remote Update/Upgrade	✔	✔	✔	✔	✔	✔	✔
Certificate Authority & Management		optional	optional	optional	optional	optional	optional	optional
	Certificate Creation	optional	optional	optional	optional	optional	optional	optional
	Certificate Management	optional	optional	optional	optional	optional	optional	optional
Key Management								
	Group creation	✔	✔	✔	✔	✔	✔	✔
	Group isolation	✔	✔	✔	✔	✔	✔	✔
	Key assignment	✔	✔	✔	✔	✔	✔	✔
	Fail-over configuration	✔	✔	✔	✔	✔	✔	✔

Price								
List Price Encryption Unit (in €)		on request	on request	on request	on request	on request	on request	on request
Per external Key Server (in €); optional, no requirement		on request	on request	on request	on request	on request	on request	on request
Required Management Software								
	2-10 encryptors	included	included	included	included	included	included	included
	11-25 encryptors	included	included	included	included	included	included	included
	26-50 encryptors	included	included	included	included	included	included	included
	51+ encryptors	included	included	included	included	included	included	included
Warranty Period (months)		24	24	24	24	24	24	24
Warranty Coverage	Parts & Work	✔	✔	✔	✔	✔	✔	✔
	Basic Support (9 to 5, e-mail, phone)	on request	on request	on request	on request	on request	on request	on request
	Software updates and upgrades	on request	on request	on request	on request	on request	on request	on request
Warranty Extension (per year)		on request	on request	on request	on request	on request	on request	on request

Viasat

	SEC-1140V	SEC-1170	
Line Interface/Supported Line Rates			
10 Mbs	✔		
100 Mps	✔		
1 Gbps	✔		
10 Gbps		✔/SFP+	
25Gps		✔/SFP28	
40 Gbps		✔/QSFP	
100 Gbps		✔/QSFP28	
Virtual Appliance	✔		
Supported Network Topologies			
Point-to-Point (P2P)	✔	✔	
Point-to-Multipoint (P2MP)	✔	✔	
Multipoint (MP)	✔	✔	
Supported Metro Ethernet Topologies			
Port-based			
Ethernet Private Line (EP-Line)	✔	✔	
Ethernet Private Tree (EP-Tree)	✔	✔	
Ethernet Private LAN (EP-LAN)	✔	✔	
VLAN-based			
Ethernet Virtual Private Line (EVP-Line)	✔	✔	
Ethernet Virtual Private Tree (EVP-Tree)	✔	✔	
Ethernet Virtual Private LAN (EVP-LAN)	✔	✔	
Supported Networks (Encryption)			
Ethernet	✔	✔	
MPLS	✔	✔	
IPv4/IPv6			
Supported Networks (Transport of Encrypted Frame)			
Ethernet (native)	✔	✔	
MPLS (EoMPLS)	✔	✔	
IPv4/IPv6			
TCP	Roadmap Q4 CY 2017	Roadmap Q4 CY 2017	EoIP only
UDP	Roadmap Q4 CY 2017	Roadmap Q4 CY 2017	EoIP only
Supported Usage Scenarios			
Single tenant	✔	✔	
Multi-tenant			
Self-managed	✔	✔	
Managed encryption service	Roadmap Q4 CY 2017	Roadmap Q4 CY 2017	
Managed security service	Roadmap Q4 CY 2017	Roadmap Q4 CY 2017	
Platform			
Platform used			
Mainboard/Firmware	ViaSat/ViaSat	ViaSat/ViaSat	
Key Management	MKA/EAPOL-TLS	MKA/EAPOL-TLS	

Viasat

Data Plane Encryption Standard and Processing			
Encryption Standard			
	Block Cipher	AES	AES
	Preferred Mode of Operation	GCM	GCM
	Alternative Mode of Operation		
	Key Length (in bit)	256	256
Processing Method			
	cut-through		
	store&forward	✔	✔
Encryption Hardware			
	FPGA		✔
	ASIC		
	CPU	✔	
Latency			
Latency P2P Mode	cut-through		
	store & forward	N/A	<3µs
Latency MP Mode	cut-through		
	store & forward	N/A	<3µs
Encryption Modes			
Native Ethernet Encryption			
Frame Encryption (Bulk - P2P only)			
	Integrity protection (algorithm)		
	Authentication length (bytes)		
	Replay protection		
	Variable replay window (size)		
	Counter length (in bytes)		
	Frame overhead (unauthenticated encryption)		
	Frame overhead (authenticated encryption)		
	Ethernet multi-hop support		
Transport (Payload only)		✔	✔
	Max. number of peers	32 - Expandable to 256	32 - Expandable to 256
	Max. number of MAC Addresses	unlimited	unlimited
	Max. number of VLAN IDs	unlimited	unlimited
	Integrity protection (algorithm)	GCM	GCM
	Authentication length (bytes)	16	16
	Replay protection	✔	✔
	Variable replay window (size)	≤ 2^31-1 frames/time	≤ 2^31-1 frames/time
	Definable encryption offset (fixed)	✔	✔
	Variable encryption offset	✔	✔
	Adaptive encryption offset based on frame content	✔	✔
	Ethertype mutation (unauthenticated encryption only)		
	Counter length (in bytes)	8	8
	Frame overhead unauthenticated encryption		
	Frame overhead authenticated encryption (AE)	32	32
	Ethernet multi-hop support	✔	✔
Tunnel (Ethernet over Ethernet)			
	Max. number of peers		
	Max. number of MAC Addresses		
	Max. number of VLAN IDs		
	Integrity protection (algorithm)		
	Authentication length (bytes)		
	Replay protection		
	Variable replay window (size)		
	Counter length (in bytes)		
	Frame overhead unauthenticated encryption		
	Frame overhead authenticated encryption (AE)		
	Ethernet multi-hop support		

Viasat

Ethernet over IP (EoIP)		
Tunnel (Ethernet over IP)	Roadmap Q4 CY2017	Roadmap Q4 CY2017
Supported transmission protocols (UDP/TCP)		
Max. number of peers		
Max. number of MAC Addresses		
Max. number of VLAN IDs		
Integrity protection (algorithm)		
Authentication length (bytes)		
Replay protection		
Variable replay window (size)		
Counter length (in bytes)		
Frame overhead unauthenticated encryption		
Frame overhead authenticated encryption (AE)		
Ethernet multi-hop support		
Native IP Encryption		
Supported IP versions		
IPv4		
IPv6		
Supported transmission protocols		
TCP		
UDP		
Transport/Tunnel Mode		
Mximum number of peers		
Maximum number of IP addresses		
Maximum number of multicast groups		
Integrity protection (algorithm)		
Authentication length (bytes)		
Additional Authenticated Data (header)		
Replay Protection		
Variable replay window (size)		
Counter length (in bytes)		
Packet overhead authenticated encryption (AE)		
Selective Encryption		
Based on MAC Address		
Based on VLAN ID		
Based on Ethertype		
Based on Multicast Group		
Based on Presence of MPLS Tag		
Based on IP Address		
Combination of multiple selection criteria		
Mixed Ethernet, MPLS, EoIP and IP Support		
Based on VLAN ID		
MPLS	✔ Roadmap Q4 CY2017	✔ Roadmap Q4 CY2017
EoIP		
IP		
Based on presence of MPLS tag		
MPLS	✔ Roadmap Q4 CY2017	✔ Roadmap Q4 CY2017
EoIP		
IP		
Based on VLAN ID and presence of MPLS tag		
MPLS	✔ Roadmap Q4 CY2017	✔ Roadmap Q4 CY2017
EoIP		
IP		
Traffic Masking		
Traffic Flow Security	Roadmap Q4 CY2017	Roadmap Q4 CY2017

Viasat

Auto-discovery				
Auto-discovery of network encryptors		✔	✔	
Auto-discovery of key servers		✔	✔	
Auto-discovery of VLANs				
Disabling of auto-discovery		✔	✔	
Key Server				
Integrated Key Server		✔	✔	
Support for external Key Server		Roadmap Q4 CY2017	Roadmap Q4 CY2017	
External Key Server		Roadmap Q4 CY2017	Roadmap Q4 CY2017	
Support for multiple distributed Key Servers		✔	✔	
Support for fail-over to back-up Key Server		✔	✔	
Autonomous operation		✔	✔	
Key Management				
Key Generation and Storage				
Hardware Random Number Generation		✔ (dependent on CPU)	✔	VNF requires Intel RDRAND (Hardware TRNG) built into all Xeons
Tamper Security Key Storage (tamper-evident or tamper-proof)		N/A	TE/TP	
Asymmetric Key Algorithms (Public Key Cryptography)				
RSA				
	Key length			
Elliptic Curve Cryptography (ECC)				
	Key length	384	384	
Supported Curves:				
	NIST	✔	✔	
	Brainpool			
	Custom Curves			
Hash Algorithms				
SHA-2	Key length	512	512	
Device Authentication				
Symmetric Signature: Pre-shared Key (PSK)		✔	✔	Connectivity Association Key (CA), also used for Key derivation to get SAKs and KEKs
	Maximum number of PSKs per encryptor	512	512	
	Key length	256	256	256-bit CAKs and a 128-bit CAK-Name (CKN) which is cryptographically derived from the CAK.
Asymmetric Signature: Certificate		x.509	x.509	Certificates used for asymmetric exchange and key derivation exchange
	Maximum number of certificates per encryptor	1	1	Only 1 certificate currently supported - due to market re-analyzing when multi-tenant support will be added.
	Key lenght			
Ad-hoc authentication of peers (manual)		✔	✔	
Signature key protocol		ECDSA w/SHA384	ECDSA w/SHA384	
Key Agreement and Key Exchange				
Master Key (KEK) Agreement		TLS 1.2	TLS 1.2	
Master Key (KEK) Exchange Protocol		EAP	EAP	
Automatic Change of Master Key		✔	✔	
Minimum suggested Time Interval for Master Key Change (min)		60	60	
Separate Master Key (KEK) per site		✔	✔	
Separate Master Key (KEK) per group		✔	✔	
Session Key (DEK) Exchange Agreement		MKA	MKA	
Session Key (DEK) Exchange Protocol		EAP	EAP	
Automatic Change of Session Keys		✔	✔	
Minimum Time Interval for Session Key Change (min)		5	5	

Certificates have to be provisioned onto units via management port. at our factory with a unique cert per unit.
Currently units are shipped with a ViaSat default Certificate per unit, and are then pre-provisioned

Viasat

Key System		
Point-to-Point Key System		
Supported key system		
Pairwise	✔	✔
Group	Unidirectional Group	Unidirectional Group
Key assignment based on:		
MAC Address	✔	✔
VLAN ID	✔	✔
Port		✔
Group	✔	✔
IP Address		
Point-to-Multipoint Key System		
Supported key systems:		
Pairwise	✔	✔
Group	Unidirectional Group	Unidirectional Group
Key assignment based on:		
MAC Address	✔	✔
VLAN ID	✔	✔
Port		✔
Group	✔	✔
IP Address		
Multipoint Key System		
Supported key systems:		
Pairwise	✔	✔
Group	Unidirectional Group	Unidirectional Group
Mixed (pairwise unicast, group multicast)	✔	✔
Key assignment based on:		
MAC address (pairwise and mixed)	✔	✔
Multicast groups (mixed)	✔	✔
VLAN ID (group)	✔	✔
Port		✔
Group (group)	✔	✔
IP Address		
IP Multicast Group		
Individual key per multicast group	✔	✔
Individual key per broadcast group (VLAN ID)	✔	✔
Group Key System Specifics		
Additional separate authentication per group	✔	✔
Group Membership Definition		
Multicast group membership	✔	✔
Individual membership		
Network membership	✔	✔
VLAN membership	✔	✔
Trunked VLAN membership	✔	✔
IP Address		
Exclusion		
MAC address	✔	✔
VLAN ID	✔	✔
Frames with MPLS tag	Roadmap Q2 2017	Roadmap Q2 2017
IP Address		
IP Muticast Group		
Group Key Distribution		
Unicast (unique KEK per group member)	✔	✔
Broadcast (same KEK for all group members)	✔	✔

Viasat

Network Support				
Bump in the Wire deployment		✔	✔	
Jumbo Frame Support		✔	✔	
Ethernet Flow Control via PAUSE		✔	✔	
Ethernet Fragmentation/Defragmentation				
	Point-to-Point			
	Point-to-Multipoint			
	Multipoint			
Dead Peer Detection		✔	✔	
Optical Loss Pass-Through				
Link Loss Carry Forward				
System Configuration and Management Access				
IPv4		✔	✔	
IPv6				
Out-of-band Management		✔	✔	
	RS-232/V.24			
	Separate Ethernet port	✔	✔	
Smart Card (Secure Card) Support				
USB Port				
In-band Management		✔	✔	
	SSH	Roadmap Q3 CY2017	Roadmap Q3 CY2017	
	SNMP (read-only/read-write)			
	TLS			
	Proprietary			
Remote Monitoring (SNMP)		v3	v3	
Logs				
Event Log (local)		✔	✔	
Audit Log (local)		✔	✔	
Syslog Support (Server)		✔	✔	
Unit				
Height in 19" Rack		N/A	1	
Number of external encrypted Ethernet ports		unrestricted	up to 4	
Physical Device Access		N/A	front	
Redundant Power Supply				
Redundant, hot-swappable power supply			✔	
High Availability functionality (two-node cluster)		1-1	1-1	
MTBF				
Tamper Security		N/A	TE/TP	
Security Approvals			FIPS-140-2 Level 3 CY2017, NIAP/CC EAL-4	All planned; FIPS is in process.
Safety Approvals			EN55022 class B - FCC Part 15 Class B	
Boot Time				
	Cold boot until operational (P2P)	560s	120s	
	Warm boot until operational (P2P)	560s	120s	

Viasat

Management Software			
User Interface	Native PC application		
	Embedded Webapp	✔	✔
	CLI	✔	✔
Initial Device Set-up			
	Local (out-of-band)	✔	✔
	Remote (out-of-band)	✔	✔
Device Configuration			
	Local (out-of-band)	✔	✔
	Remote (in-band)		
	Remote (out-of-band)		
Management Access			
	Role-based access	✔	✔
	Identity-based authentication of user	✔	✔
	Number of hierarchy levels	3	3
	Number of roles	2	2
	Strict internal separation of users	✔	✔
Device Management			
	Device Diagnostics	✔	✔
	Link Monitoring (SNMP)	✔	✔
	Connection Diagnostics	✔	✔
	In-band Network Diagnostics	✔	✔
	Remote Update/Upgrade	✔	✔
Certificate Authority & Management			
	Certificate Creation	Roadmap Q2 CY2017	Roadmap Q2 CY2017
	Certificate Management	Roadmap Q2 CY2017	Roadmap Q2 CY2017
Key Management			
	Group creation	✔	✔
	Group isolation	✔	✔
	Key assignment	✔	✔
	Fail-over configuration	✔	✔

Price			
List Price Encryption Unit (in €)	1G VNF, or 10G SEC-1170	on request	on request
List Price Encryption Unit (in €)	4x10G, 4x25G		on request
List Price Encryption Unit (in €)	100G		on request
Per external Key Server (in €)			
Required Management Software			
	2-10 encryptors		
	11-25 encryptors		
	26-50 encryptors		
	51+ encryptors		
Warranty Period (months)		12	12
Warranty Coverage	Parts & Work		
	Basic Support (9 to 5, e-mail, phone)		
	Software updates and upgrades		
Warranty Extension (per year)		✔	✔