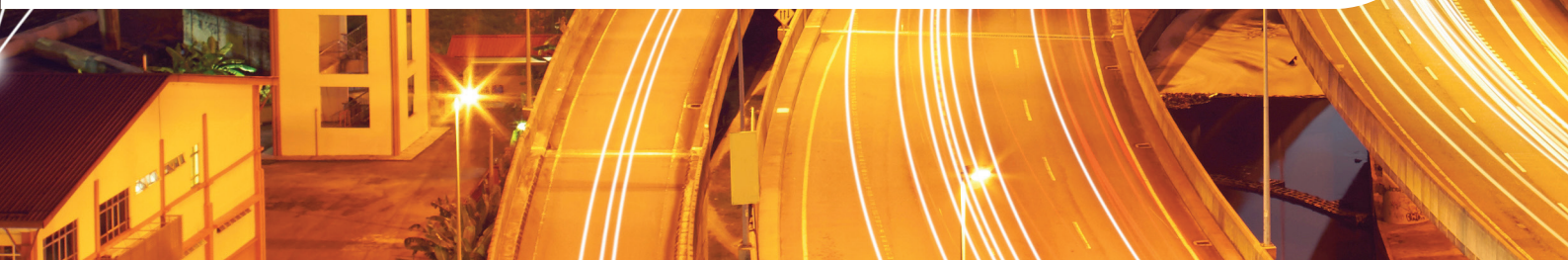
gemalto
security to be free

Securing Your High Speed Ethernet WAN

Important Things You Need To Know

EBOOK



We don't disagree.

High speed Ethernet WANs are the answer to applications and computing technologies that need increasing bandwidth. But did you know that securing your shiny new Ethernet WAN traffic will cost thousands of dollars more every month if you make the wrong choices? Or that security policy management could become your biggest headache and actually cause network outages? Or that encryption overhead could consume half your new bandwidth and astronomically increase network latency?

No? Then we suggest you spend five minutes reading this ebook.

Why you should read this ebook

- You need more bandwidth
- You need to meet compliance demands
- You need to decrease your bandwidth costs
- You need to comply with regulatory requirements
- You're overwhelmed with security administration
- Your network can't handle new application performance needs.

Contents

Diagrams and tables

(video on demand +
online collaboration +
electronic commerce +
IPTV + VoIP +
wireless communications +
cloud computing +
multi-core processing +
virtualization +
networked storage +
I/O convergence)
= need more bandwidth

The Ethernet WAN explosion

Demand for bandwidth is outpacing supply, driven by the convergence of data, voice and video, new computing technologies, and increasing reliance on the Internet. To meet this demand, while reducing costs, organizations are looking not only for larger network pipes but also for finer granularity and more efficient ways to use existing bandwidth.

Ethernet delivers highly scalable granularity – from 1 Mbps to 100 Gbps – while providing lower per-port capital expenditures than traditional WAN technologies. Organizations can pay for bandwidth according to how much they actually use rather than having to make large jumps in bandwidth when they exceed their existing link capacity. As a result, more and more companies now use native Ethernet to carry data over WANs.

Ethernet can connect to either Layer 2 or Layer 3 services to create a networking solution, providing high bandwidth connectivity between locations within a metropolitan area, between two cities, or across a global WAN. Ethernet services help in extending the familiar LAN environment to the WAN, enabling greater application level control compared to traditional deployments. Data center traffic is also rapidly expanding due to a mixture of access, storage requirements and increasing use of virtualization. Data center interconnection speeds between regional hubs are now above 1 Gbps in many leading enterprises.

Data recovery sites that require fast SAN synchronization and the adoption of virtualization that necessitates faster replication also drive network speed requirements. Ethernet WANs offer high speed, low-latency connections for these requirements through an E-LAN or E-Line.

New applications, such as workgroup collaboration and video, are also driving remote/branch office traffic and the need for greater bandwidth. Technologies like IP MPLS can create long delays and are not always ideal for carrying voice and video traffic efficiently. Multi-site organizations are therefore moving to Ethernet WAN for greater scalability, granularity and cost effectiveness.

Real-time transactions processing in brokerage firms and medical imaging for healthcare are among other applications that require high speed networks, and Ethernet offers these speeds at a much lower cost compared to competing technologies.

With the rapid proliferation of carrier-grade Ethernet services, the technology is gaining traction among enterprises that value its ability to provide higher bandwidth in a granular manner. And since the technology is now mature, standards-based, and multi-vendor interoperable, it helps enterprises gain scalability across diverse corporate environments with significant reduction in provisioning costs.

Physical Ethernet interfaces are available in 10-megabit, 100-megabit, 1 gigabit, 10-gigabit speeds, and up to 100-gigabit interfaces.

The Ethernet value proposition

- Scalable bandwidth for both point-to-point and multipoint-to-multipoint
- Reduced complexity due to familiarity of interfaces
- Lower operating costs (price per Mbps) and lower capital expenditure costs
- Appropriate level of control over security
- Flexible network architecture design
- Standards-driven, multi-vendor interoperability

Growth metrics

The global market for Carrier Ethernet Equipment is projected to reach US$38 billion by 2020, driven by increasing data traffic and rising adoption of Carrier Ethernet services.[1]

The need for encryption

Since organizations first began transmitting sensitive information over external networks, there's been a need for network security mechanisms. But service providers do not take measures to ensure data integrity. Generally, the solution they offer is the isolation of traffic or data. This approach doesn't safeguard against tapping of transmission lines, eavesdropping at switching and routing points, misconfiguration, and a host of other issues.

In addition, while threats have evolved, increasingly sensitive data is being transmitted, more transactions are being conducted over networks, and more value is moving through them, which means that even a small breach can result in staggering data leakage – with associated reputation, privacy, and financial losses.

The trend in IT has been towards increased security in all facets of data management: in systems, datacenters, and networks. While newer releases of applications and operating systems have improved security, the improvement in network security has been low. The development of IPv6, which has room for cryptographic information in its header, has been a slow process, with its widespread deployment still on the horizon. In the meantime, the use of IPsec with IPv4 has become the standard for securing data transfer over the network.

IMPORTANT THING:

A company whose sensitive data is sent over a shared Ethernet transport risks sustaining significant losses. In healthcare, financial, and governmental organizations, these losses can be even more devastating.

Key requirements for encryption solutions

Compliance

Beyond the obvious needs for encryption in safeguarding against security threats, many organizations need to ensure and demonstrate compliance with a host of mandates, including governmental, industrial, and regional policies. Encryption mechanisms in place need to support these efforts and provide advanced audit reporting.

Performance

Performance is a critical consideration. Because of its inherently CPU-intensive characteristics, encryption can cause significant performance degradation. However, depending on the WAN encryption solution and architecture deployed, there can be big discrepancies in performance realized. For example, some encryption approaches require tunneling, which utilizes additional bandwidth, and can deliver an additional performance hit above and beyond that of encryption itself.

Converged network support

Today, IP networks are relied upon to transmit voice, video, and data, so organizations require encryption solutions for transmitting these assets without introducing latency.

Robust scalability

For most organizations, networks are relied upon constantly, for virtually every aspect of business – everything from phone service to email to e-commerce. Consequently, it is vital that encryption and security don't hinder connectivity. For example, both GRE/IPsec VPNs and IPsec VPNs provide secure site-to-site communications, but are complex to manage and troubleshoot, and are not scalable. As a result, as the size and complexity of the WAN increases, many issues arise for organizations using these technologies.

Network topology flexibility

Any encryption solution must not hinder network connectivity and must be compatible with an organization's current and planned network topologies. For these reasons, organizations will invariably shy away from encryption solutions that are not flexible and that limit the types of topologies and designs that can be employed. This is a key consideration as organizations choose between integrated encryption solutions and dedicated encryption solutions.

Management

An encryption solution must provide easy and effective policy management and streamlined, role-based administrative capabilities to eliminate the need for highly technical personnel. Toward this end, integration with network management systems is a must. Built-in, easy-to-manage controls over the internal encryption network are required for protection against internal risk. In addition, the encryption solution must also support fault management systems, as well as such standards as SNMPv3.

Do you know where your fibre is?

For under $500 an individual can buy a "microbend tap" device that can tap into fibre – without removing the cable sheathing – and pull data off without anybody being able to detect the intrusion. At 10-gigabit speeds, tens of thousands of records can be compromised within seconds of breach. Commercially available fibre optic intrusion detectors using power measurement techniques are insufficiently sensitive against intrusions of this type. While some skill is required to implement data theft using this method, and to intepret the results, anyone with sufficient knowledge and access to your fibre could seriously compromise your organization.

Network encryption: integrated or dedicated?

In implementing Ethernet WAN encryption between sites, there are two types of solutions that are most commonly employed. The first type is comprised of solutions that integrate encryption capabilities within routers, sometimes called 'onboard encryption'. The second type implement encryption via dedicated, single-purpose hardware devices that are separate from all other network elements.

When employing encryption in a WAN, if both integrated and dedicated encryption solutions provide the same level of security, performance, and cost/benefit, then it's logical to prefer integrated solutions. But this is not the case, as we'll see later.

Integrated solutions are typically preferred because of lower upfront cost, communication with a single vendor, and so on. In addition, before choosing a dedicated encryption device, administrators need to consider other factors, such as its capacity restrictions and compatibility with existing WAN topology. Consequently, many organizations have employed Layer 3 encryption mechanisms integrated within the network's routers. But there are fundamental advantages to dedicated encryption devices that are not always well known, and which deliver significant benefits to those organizations that deploy them.

IMPORTANT THING:

If both integrated and dedicated encryption solutions provide the same level of security, performance, and cost/benefit, then it's logical to prefer integrated solutions. **But this is not the case.**

Layer 2 vs. Layer 3 – Security Overview

	Layer 2 (e.g. Ethernet)	Layer 3 (e.g. IPsec)
Performance	> No performance degradation for small-packet traffic (realtime VoIP, video) > Virtually no latency > No bandwidth wasted for security overhead	> Poor performance, especially for small-packet traffic > High latency, especially for small-packet traffic > Up to 50% of bandwidth wasted by IPsec overhead
Ease of integration and maintenance	> Easy to integrate, plug-and-play > Virtually no maintenance required > Separates physical or SDN network from security	> Hard to integrate into IP networks due to IP address management issues > Changes in network setup impact security > Changes to network require frequent policy changes and cause inadvertent outages
Depth of security	> Default mode of operation is fully secure > Not subject to common router OS vulnerabilities > Separates encryption from firewall function > FIPS 140-2 and CC-certified hardware > Supports latest encryption standards such as AES-256	> Provides more granular security options which leaves room for errors in security implementation (e.g. unencrypted connections) > FIPS 140-2 and CC-certified hardware > Supports latest encryption standards such as AES-256
Reliability	> Highly resilient > Changes in IP layer do not affect Layer 2 security	> Changes in IP network (e.g., IP address changes) can interfere with security setup
Cost	> Cost-effective solution requires only minimum number of encryptors to secure entire circuits	> Fast IPsec encryptors are expensive

In implementing network encryption, organizations can choose to encrypt data in one or more layers in the network stack:

Application layer	Layer 5	HTTP, FTP, SMTP, POP
Transport layer	Layer 4	TCP, SSL, TLS
Network layer	Layer 3	IP
Data link layer	Layer 2	Ethernet, Frame Relay, ATM
Physical layer	Layer 1	SONET, SDH, OTN, DWDM

In the following section, we'll take a closer look at some of the challenges organizations employing integrated router-based Layer 3 encryption have encountered. We'll then look at another form of encryption using dedicated Layer 2 Ethernet encryptors in an autonomous encryption network 'overlay', and reveal how this approach compares.

> Many companies have discovered the true cost of the overhead associated with encrypting at Layer 3 using IPsec in the router. At the small average packet sizes typical in today's converged networks, **IPsec overhead reaches 40% to 50% of total bandwidth**, with associated costs climbing to thousands of dollars per month. **Ethernet encryption at Layer 2 virtually eliminates overhead**, recovers network bandwidth, and lowers total cost of ownership by streamlining security measures, simplifying security policy management, and eliminating the inefficiencies associated with conventional Layer 3 security.

Layer 2 High Speed encryption with Gemalto

With a SafeNet High Speed solution, everything in a network pipe is either encrypted or not encrypted based on source and destination MAC addresses, removing complexity, providing clear evidence of encryption at appropriate places, and ensuring transparency for Layer3 data. This makes it possible for IPv4 or IPv6, or any other kind of Layer 3 traffic, to be transmitted transparently over high speed.

Ethernet encryption solutions can be used in a variety of enterprise configurations. For example, a company could use it for high speed intra-office connectivity, linking corporate LANs, core offices, data centers and network operations centers. High Speed encryption is also effective for high speed metropolitan area networks (MANs), protecting data and networks for captive networks and corporate campuses in the metro area. In addition, it is suitable for high speed edge applications, such as service aggregation, triple play (voice, video, data), VoIP aggregation, streaming video, and wireless LANs. It also makes sense for any situation where servers are being centralized, including server farms and SANs. Finally, high speed WANs are well served by Layer2 High Speed encryption solutions, where protection can be applied to network backbones, LAN extensions in multinational organizations, and wireless backhaul.

Gemalto offers advanced Layer 2 encryption solutions that eliminate the challenges and obstacles presented by Layer 3 encryption approaches while providing robust encryption.

Benefits of Layer 2 encryption

Lowest cost of ownership

- Better bandwidth efficiency (up to 50%)
- Minimal ongoing maintenance – routing updates transparent to encryption
- Lowest cost solution for aggregation of many sites

Maximum performance

- Low protocol overhead
- Low latency
- Eliminates GRE and complex QoS schemes

Enterprise scalability

- Fast, reliable network integration
- Siple architecture scales to thousands of devices
- Layer 3 transparent – all Layer 3 protocols supported (IPv4, IPv6, and legacy)

SafeNet High Speed Encryptors deliver maximum bandwidth, strongest available protection, the least administrative overhead, and the lowest total cost of ownership. Designed to overcome the fundamental technological limitations of IPsec encryption, SafeNet High Speed Encryptors move sensitive data faster and more efficiently at network Layer 2, thereby lowering the cost of network security and compliance.

Implemented as a network overlay and managed via a consolidated management center, SafeNet High Speed Encryptors are ideally suited to large-scale network encryption implementations. They operate on High Speed-based Layer 2 MAC transparent networks, which makes them well suited to metropolitan High Speed or High Speed WAN services, as well as remote backup, SAN, data center, and business continuity and disaster recovery sites.

Lower total cost of ownership

A basic, immediate cost saving is that Layer 2 devices eliminate bandwidth overhead for expensive transport pipes, and provide the full throughput available with Layer 2 High Speed.

They also reduce administrative costs. By virtue of their functioning at the data link layer, SafeNet High Speed Encryptors are far easier to deploy and administer. Compared to Layer 3 encryption approaches, administrators only need to manage a fraction of the settings, variables, and interrelationships when setting up and maintaining SafeNet High Speed Encryptors. With Layer 3, administrators must continually cope with VPN rules, policies, and the tunneling of data or connections from point to point.

SafeNet High Speed Encryptor key features

- Full-duplex line-rate encryption of Ethernet networks up to 100 Gbps
- Meets rigorous FIPS 140 2 Level 3, Common Criteria, NATO, UC APL, CAPS* security requirements
- Bump-in-the-wire design for easy installation into existing network environments
- Minimal latency, zero protocol overhead enables transparent operation
- Standards-based authentication, digital certificates, and key management
- Central configuration, monitoring, and management
- Minimal administrative setup and low total cost of ownership

*specific models

Every time a new device is added to a mesh architecture, for example, all the connections have to be configured in complex routing tables. By contrast, the same change with Layer 2 security would only require adding a security authentication certificate, allowing other devices to talk to the new device securely without excess management time and costs. Overall advantages include simple deployment, ease of management, and lower total cost of ownership.

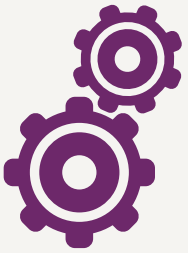
SafeNet High Speed Encryptors are managed by a robust web-based policy management application that is both easy to use and secure, and provides the advanced audit and monitoring capabilities necessary for security compliance.

Integrated management allows administrators to remotely configure, monitor, and update all SafeNet High Speed Encryptors on a network. It enables administrators to define integrated security policies that can be distributed across multiple devices, reducing management complexity and cost. Gemalto also has a number of high-assurance, carrier class, high availability options to ensure your management system is resilient to network and system outages.

Easier compliance

Verifying compliance is much more straightforward than in Layer 3 environments. Gemalto provides a detailed, centralized log archive, which significantly streamlines compliance reporting and remediation. All SafeNet High Speed Encryptors are FIPS certified to current 140-2 Level 3, ensuring compliance with a host of government and commercial compliance mandates. Gemalto also offers a range of encryptors that are Common Criteria, NATO, UC APL and CAPs (UK) certified, as well as FIPS 140-2 L3. In addition, Gemalto, through its acquisition of SafeNet, is one of the few security vendors that for years has been delivering products for highly secure government networks, as well as commercial networks. 85% of inter-bank transfers are carried on SafeNet High Speed encryptors.

Performance Improvements



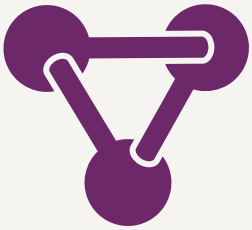
As opposed to IPsec encryption, SafeNet High Speed Encryptors encrypt the entire IP packet without the overhead of separately encrypting an additional IP header. This means that as the Layer 2 High Speed frame moves through the intermediary networks between the two primary sites the MAC address of the original frame must not be altered. Because routers, operating at Layer 3, change the MAC address of the High Speed frame, the encrypted frame cannot pass through a router prior to being decrypted.

Compared to using IPsec, SafeNet High Speed Encryptors are better suited to WAN links because they are less complex and more efficient. By encrypting sensitive data at Layer 2 the entire High Speed frame, and consequently all data traversing the network, is encrypted. In addition, by replacing a legacy IPsec encryption solution with a SafeNet High Speed Encryptor, bandwidth availability is effectively doubled and latency through an IPsec network connection is reduced by as much as thirteen times. This is a more attractive alternative than purchasing or leasing costly bandwidth upgrades with high monthly charges.

Architecture

Because of their streamlined implementation, SafeNet High Speed Encryptors provide a great deal of flexibility in deployment approaches. With these solutions, full mesh deployments across a large number of sites are both feasible and cost-effective. Further, with their VLAN support, SafeNet High Speed Encryptors streamline hub-and-spoke deployments as well.

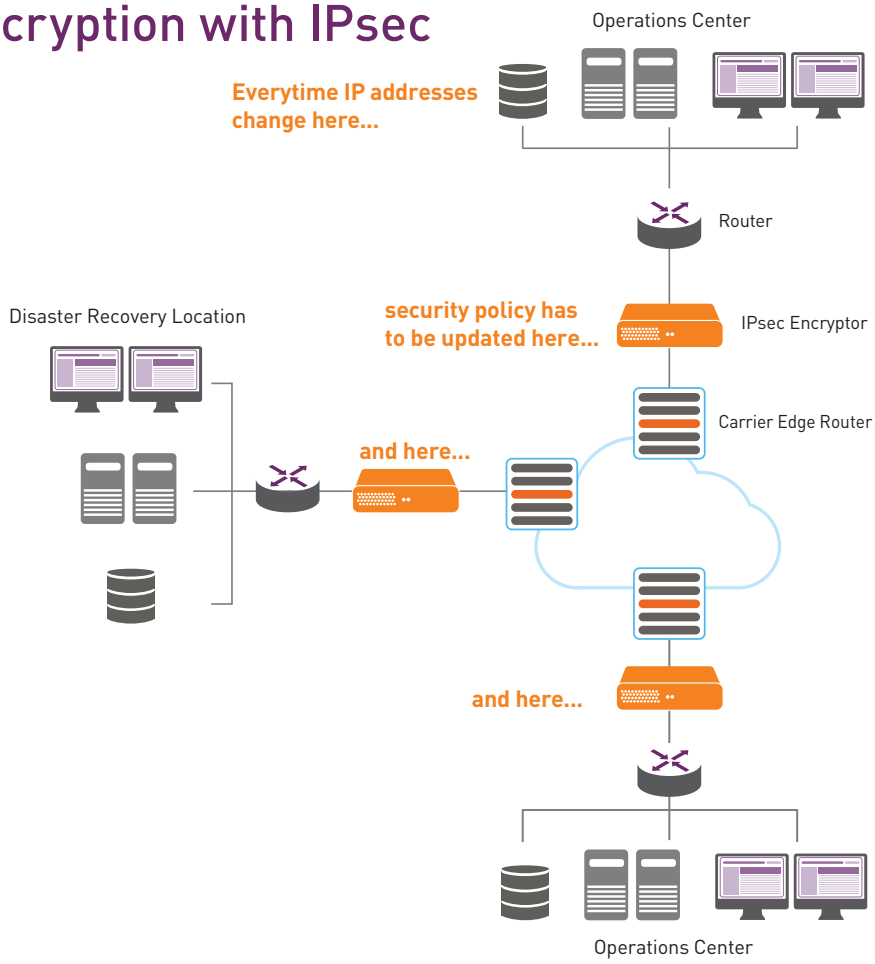
Interoperability



The deployment of SafeNet High Speed Encryptors is unobtrusive, deployed as a core overlay on Ethernet. As a result, all the systems in place in a given network still work, without any modification whatsoever. This gives organizations the flexibility they need to maximize their existing investments, and to have complete flexibility in the future. SafeNet High Speed Encryptors are compatible with the following network types:

- Carrier High Speed (E-Line / E-LAN)
- DWDM/Dark Fibre
- High Speed over MPLS
- High Speed over OTN (G.709)
- High Speed II, IEEE 802.3
- Jumbo Frames
- VLAN, QinQ.

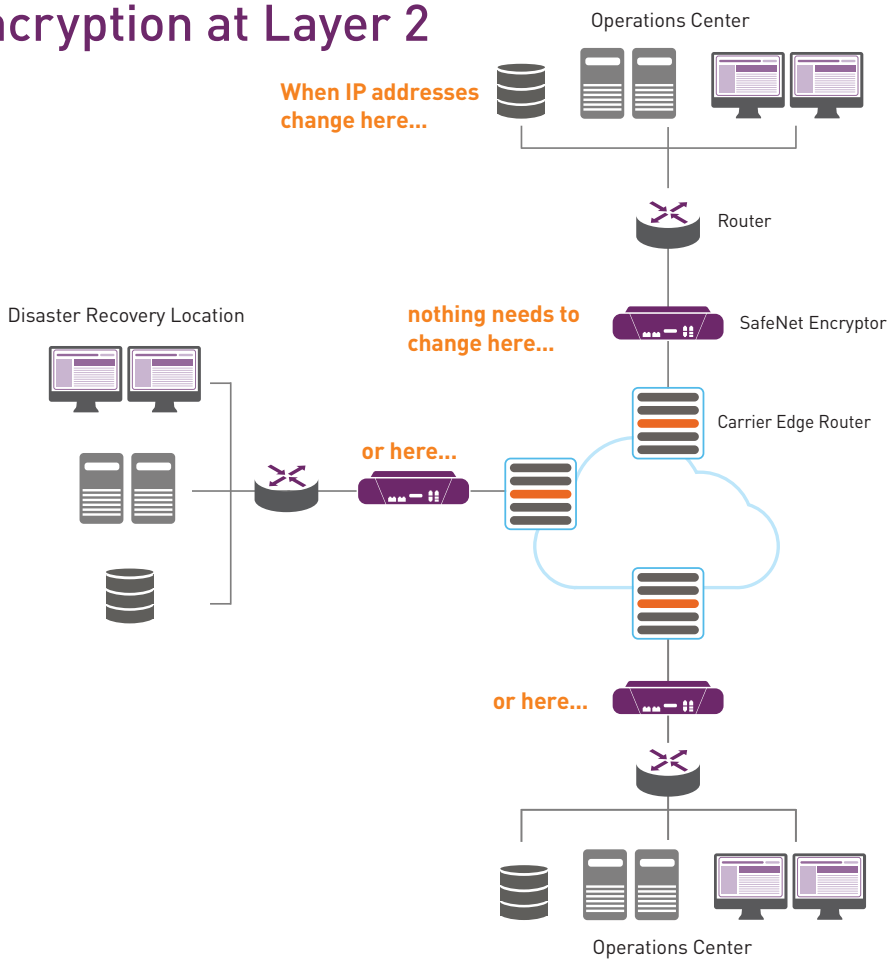
Encryption with IPsec



IMPORTANT THING:

IPsec: creates the potential for network outages and security vulnerabilities.

Encryption at Layer 2



IMPORTANT THING:

Layer 2: no administrative burden, no outages and no security policy changes.

The IPsec throughput implosion

An independent study by the Rochester Institute of Technology (RIT) demonstrated that the potential benefits of costly high speed networks can be seriously overshadowed by loss of throughput, often increasing rather than decreasing total cost of ownership due to excessive management and bandwidth overhead issues. The findings determined that SafeNet High Speed Encryptor Layer 2 encryption technologies provide superior throughput and far lower latency than IPsec VPNs operating at Layer 3. In fact, because of the large drop in throughput when using IPsec solutions, it could be called a 'throughput implosion'. Let's look at some of these differences in detail.

R·I·T

NSSA Department

Comparative Performance of Layer 2 and IPsec Encryption on Ethernet Networks

The exposed IP header problem

In transport mode, IPsec has less data overhead but does not provide confidentiality for the Layer 3 IP header. This means that sensitive information about the addressing of the internal network can be maliciously acquired by monitoring the public network over which the traffic travels.

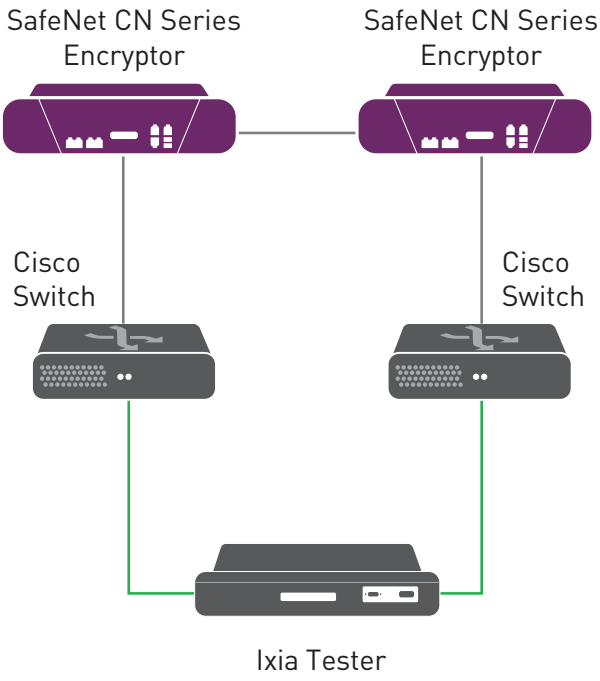
Tunnel mode IPsec addresses this security concern by encrypting the entire IP packet and encapsulating it into another IP packet. This packet contains only the address of the encryption devices at either end point and not of the actual hosts communicating on the internal network.

However, while tunnel mode does address the security and privacy concerns of transport mode IPsec, it also adds a significant amount of data overhead. Processing of this extra IP header also has some performance issues in terms of latency.

SafeNet High Speed Encyptors address the issues encountered with IPsec tunnel mode. The SafeNet High Speed Encryptor is placed on the network edge and encrypts the entire IP packet without adding the overhead of an additional IP header.

Test setup

The RIT tests, modeled on RFC 2544, used two Cisco gigabit Ethernet line cards installed in two high performance Cisco Catalyst 6509 Switching Chassis, two Cisco Systems IPsec VPN Services Modules, two SafeNet dedicated High speed Ethernet Layer 2 Encryptors, and an Ixia 250 test platform connected in a simple network. The tests established an infrastructure baseline to account for the bandwidth reduction introduced by the Ethernet protocol overhead. Measurements then included frame loss, throughput, and latency of encrypted and unencrypted data for a range of frame sizes.



Frame loss

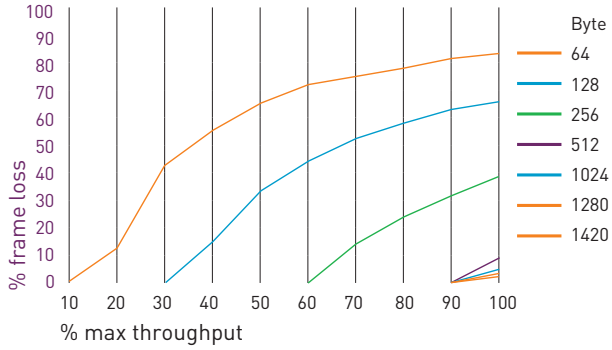
Frame loss is the difference between the number of frames transmitted by one interface and the number of frames received by another. The RIT tests determined the maximum speed at which the devices could operate without frame loss.

The SafeNet High Speed encryption solution experienced less than 1/1000th of 1% frame loss for each given frame size. This amount of frame loss is statistically insignificant and resulted in an average frame loss of 0 for 100% of line speed.

In comparison, the IPsec encryption test found that loss was significant for all frame sizes. As load increased, so did frame loss. As frame sizes decreased, frame loss increased in a logarithmic fashion. At 64-byte frame sizes (the small frame sizes typical in latency-sensitive video and VoIP applications) over 40% frame loss was encountered at only 30% of the maximum theoretical throughput.

This significantly limits the available bandwidth that can be used with IPsec encryption.

fig. IPsec frame loss



IMPORTANT THING:

SafeNet High Speed Encryption:
0 frame loss at 100% line speed
IPsec encryption:
40% frame loss at 30% line speed

Throughput... or not

A standard Ethernet frame has the capacity to carry a 1500-byte payload, not including the CRC, MAC, control field, UDP, link or Ethertype data. Ethernet includes a preamble of 8 bytes at the start of the frame and an inter-frame gap of 12 bytes which together reduce the maximum theoretical throughput of a given link.

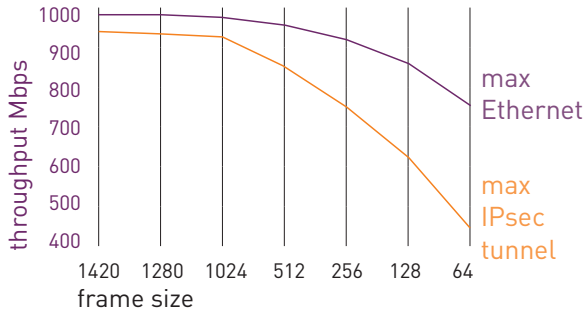
The SafeNet High Speed Encryptors were found to have no effect on throughput, in either direction, regardless of frame size, and throughput remained at 100% of maximum theoretical throughput.

Using IPsec encryption adds 57 bytes of overhead to encapsulate the IP header of the original packet and to add an additional authentication header and trailer. As can be seen in the figure to the right, at smaller frame sizes adding 57 bytes has a significant impact on the maximum theoretical throughput.

The IPsec encryption solution was unable to achieve maximum theoretical throughput at smaller frame sizes. At 512-byte, 1024-byte and 1280-byte frame sizes, approximately 100% of maximum theoretical throughput was achieved. But at 256-byte frames that performance was just 73%, at 128-byte frames it dropped further to 47%, and at 64-byte frames it was just 27% of maximum theoretical throughput.

Effectively, this means a gigabit-rated link using IPsec encryption can only transmit small packets (used in real-time voice and data applications) at close to 100 Mbps.

fig. Comparison of theoretical throughput



IMPORTANT THING:

SafeNet High Speed Encryption:
100% throughput (all frame sizes)
IPsec encryption:
27% throughput (64-byte frames)

Latency

The RIT tests measured the time it takes for the first bit of the frame to traverse the test network topology from source to destination, using an average of ten trials. Comparison of the results was performed as a percentage increase over the respective unencrypted baseline latency for each test.

It is expected that every networking device added to a system introduces additional latency. The average latency for traffic traversing the test network ranged from 1210 µsec (1.2 ms) for 64-byte frames up to 1308 µsec (1.3 ms) for 1420-byte frames. Adding SafeNet Ethernet encryption added less than 1% above this baseline.

The IPsec encryption solution, on average, added over 13 times the latency of the SafeNet High Speed Encryptors.

fig. Comparative encrypted throughput data

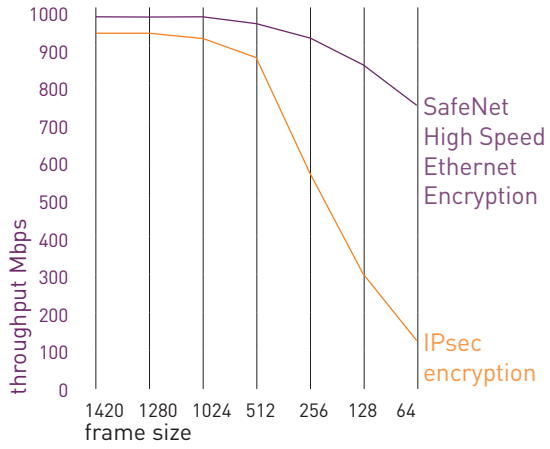
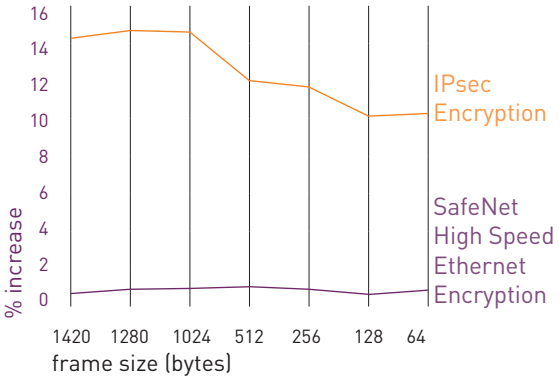


fig. Comparative latency of IPsec and SafeNet High Speed encryption



IMPORTANT THING:

SafeNet High Speed Encryption average:
1% latency, 7 µsec
IPsec encryption average:
13% latency, 95 µsec

Conclusions

We'll leave it up to RIT to make the case:

"Overwhelming logic suggests that, from a theoretical performance perspective, Layer 2 Ethernet encryption should be superior to Layer 3 IPsec encryption. The current battery of tests, and data generated in the previous study, confirm the reality of the throughput and latency limitations induced by the IPsec wrapper overhead. Testing exposed the detrimental effect on network performance that is typically imposed by IPsec's innate processing requirements, as well as the processing limitations of the tested IPsec hardware.

In contrast, the SafeNet Ethernet Encryptor operates at line speed. Testing also revealed no significant frame loss with the SafeNet Ethernet encryption solution, whereas significant frame loss was encountered at comparatively low data rates with the IPsec solution. This resulted in a significant reduction of the data rate, as seen in throughput testing, and indicates that achieving line rate encryption, even at the reduced maximum theoretical throughput of IPsec, is impossible regardless of frame size with the IPsec solution.

Finally, the measured latency of the Cisco IPsec encryption solution was found to be over 13 times that of the SafeNet Ethernet encryption solution. In environments where Ethernet encryption technology meets the needs of the organization, its performance is clearly superior to IPsec."

IMPORTANT THING:

Testing exposed the detrimental effect on network performance that is typically imposed by IPsec's innate processing requirements, as well as the processing limitations of the tested IPsec hardware.

FAQs

1. Isn't WAN security taken care of by the telco or service provider with our Service Level Agreement?	Generally, service providers only offer the isolation of traffic or data. This approach doesn't safeguard against equipment failure, eavesdropping at switching and routing points, misconfiguration, and a host of other issues. Regardless of regulatory requirements, it is not good business practice to trust another organization with your entire business data without securing it first.
2. Aren't Ethernet, SONET/SDH, ATM, and fibre links inherently secure?	Fibre links, and anything transmitted on it, are as vulnerable as any other form of network transport. It is possible to read the data on a fibre link with inexpensive equipment. This kind of data theft has been going on for years. So called "dark fibre" (in various geographies) is no more secure from this type of attack than any other fibre.
3. Isn't the risk of data disclosure low compared to the cost of protection?	The Ponemon Institute released their 2016 study reporting that the average consolidated total cost of a data breach is $4 million[2].The report highlights breaches at well-known companies that could have been thwarted by encryption. Corporations are high profile targets, and with attackers having more resources and technology available, the risk of a data breach is constantly increasing.
4. Can't I protect data for virtually no cost by adding encryption to my router or firewall?	The cost of integrated encryption solutions is hidden in the form of implementation, configuration, management overhead, and significantly lower network performance. Autonomous encryption solutions suffer none of these limitations.
5. Surely, above a certain speed of network link, there is so much data passing through that an attacker would not be able to get anything meaningful?	The power of today's network devices and computers allows for any data to be captured from links of all speeds and processed in any way the attacker chooses. The network speed actually assists the attacker because so much data can be captured in so short a time period.
6. Everybody else in this industry uses router or firewall encryption, so why isn't it OK for me?	More and more companies are adopting Layer 2 encryption. As interactive applications such as video conferencing and VoIP, and new computing technologies such as virtualization, become more common, bandwidth and network performance becomes an issue. Only the most efficient encryption solutions become viable.
7. Won't additional network equipment add more management burden in patches and updates?	Gemalto's SafeNet High Speed Encryptor solutions do not routinely require security updates and do not suffer the same constant stream of vulnerabilities that router and firewall products do. They are designed from the ground up as security devices.
8. Won't key management for a large deployment be prohibitive?	SafeNet High Speed Encryptors have fully automated key management for day-to-day operations. For authentication, the SafeNet High Speed Encryptor management platform will act as either a stand-alone certificate authority or interface to an existing PKI.

SafeNet High Speed Encryptor product information

SafeNet High Speed Encryptors use dedicated security engines that are separate from the network infrastructure. This approach has intrinsic advantages compared to integrated solutions. Whether you are operating a traditional enterprise data center or moving your data and processing into the cloud, data confidentiality and infrastructure isolation are assured without impacting the day to day operations of the network. Infrastructure security is administered separately from the network administration function allowing separation of duties even when operating in the cloud. Our technology operates at the highest performance levels without negatively impacting network capacity or speed and without adding network complexity. The encryption devices and their management function exist as a network 'overlay' that is highly reliable, highly resilient, easy to deploy and maintain, and can be rapidly expanded as needs change.

SafeNet High Speed Ethernet encryptor products

SafeNet High Speed Encryptors are high-assurance, high performance Layer 2 security appliances that protect up to 100 Gbps Ethernet networks. With seamless end-to-end integration on Ethernet WANs, SafeNet High Speed Encryptors deliver instant protection across the network at Layer 2, adding far less latency to mission-critical applications than traditional Layer 3 solutions like IPsec VPNs. Unlike Layer 3 encryption solutions, SafeNet High Speed Encryptors have minimal impact on the network.

With SafeNet High Speed Encryptors, payload data is encrypted up to the MAC address, ensuring that data is completely secure. A cryptographic payload offset feature permits users to offset deeper into the frame (supporting VLAN tagging and MPLS shims), thus permitting the solution to accommodate multiple architectures. These devices are also designed and certified to FIPS security standards (FIPS 140-2 Level 3 accredited).

Gemalto's SafeNet Network Encryption products are a key component of Gemalto's comprehensive Data Protection solution to reduce the cost and complexity of regulatory compliance, data privacy, and information risk management.

SafeNet High Speed Encryptors deliver maximum performance, strongest available protection, the least administrative overhead, and the lowest total cost of ownership.

SAFENET ETHERNET ENCRYPTOR CN4010

SAFENET ETHERNET ENCRYPTOR CN4020

SAFENET ETHERNET ENCRYPTOR CN6010

SAFENET ETHERNET/FC ENCRYPTOR CN6040

SAFENET ETHERNET ENCRYPTOR CN6100

SAFENET MULTILINK ENCRYPTOR CN8000

SafeNet High Speed Encryptor encryptor features

Maximizes bandwidth and performance

- Full-duplex, line rate AES-256 encryption for up to 100 Gigabit Ethernet (100 GbE) networks
- Hitless 2048-bit key exchange
- Zero protocol overhead allows maximum bandwidth to be available for data – up to 50% more efficient than competing technologies
- Fastest network encryption available (true line speed)
- Microsecond latency (< 7 µsec) performance ensures high quality of real-time applications such as VoIP and video – IPsec can increase the latency by up to 13 times
- High availability features support architectures with over 99.999% uptime

Strongest available protection

- Strong SHA-256 hash function, 2048-bit digital certificates, and hardware-based key management
- Uses the strongest cryptographic algorithms publicly available (AES-256)
- SafeNet encryptors do not routinely require security patches, nor suffer the same constant stream of vulnerabilities that plague routers and firewalls
- Tamper-proof design certified to FIPS 140-2 Level 3

Lowest total cost of ownership

Minimal administrative overhead for low OPEX

- Fastest initial setup (in minutes)
- No need for network reconfiguration
- No need for routing table updates – routing updates are transparent to encryption
- Ease of setup and configuration requires less expertise
- Remote configuration and monitoring
- Automatic discovery of network MAC addresses – no need to manually build complex addressing tables and policies
- Automatic recovery from network outages
- Automatic discovery for new encryptors
- Integrates seamlessly into any network topology

Lowest capital cost (CAPEX)

- Lowest cost solution for aggregation of multiple sites and high speed networks.
- Fewer encryptors need to be installed compared to additional routers and IPsec encryption devices

Simplest network topology

- Bump-in-the-wire design for easy installation into existing network environments
- Compatible with all Ethernet topologies
- Decreases complexity of network infrastructure, maintenance and administration compared to Layer 3 solutions
- Scalable to thousands of devices using simple VLAN-based policy
- Layer 3 transparent, supports all layer 3 protocols

How to find out more

Find out more about the benefits of SafeNet High Speed Ethernet Encryptors.

Contact us

Follow us

Read more about network encryption

Acronyms

ACL	access control list
AEA	SafeNet Autonomous Encryption Architecture
AES	advanced encryption standard
ATM	automated teller machine / asynchronous transfer mode
BGP	border gateway protocol
CAGR	compound annual growth rate
CAPEX	capital expenditure
CEAP	carrier Ethernet access platforms
CPU	central processing unit
CRC	cyclic redundancy check
CSV	comma-separated values
DES	data encryption standard
DMVPN	dynamic multipoint virtual private network
DWDM	dense wavelength division multiplexing
E-LAN	Ethernet local area network
E-Line	Ethernet line
EIGRP	enhanced interior gateway routing protocol
EPL	Ethernet private line
ERP	enterprise resource planning
EVPL	Ethernet virtual private line
FIPS	federal information processing standard
FTP	file transfer protocol
GbE	gigabit Ethernet
GRE	generic route encapsulation
HSM	hardware security module
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol secure
ICMP	internet control message protocol
IP	internet protocol
IPsec	IP security
IPTV	internet protocol television
IPv4	internet protocol version 4
IPv6	internet protocol version 6
IT	information technology
LAN	local area network
MAC	media access control
MAN	metropolitan area network
MEF	metro ethernet forum
MPLS	multi-protocol label switching
NAT	network address translation
NHRP	next hop resolution protocol

OPEX	operational expenditure
OS	operating system
OSPF	open shortest path first
OTN	ptical transport network
PKI	public key infrastructure
POP	post office protocol
PPP	point-to-point protocol
QinQ	an amendment to IEEE 802.1Q for Ethernet frame formats
QoS	quality of service
RADIUS	remote authentication dial in user service
RFC	request for comments
RIT	Rochester Institute of Technology
SAN	storage area network
SDH	synchronous digital hierarchy
SLB	server load balancing
SMC	SafeNet Security Management Center
SMTP	simple mail transfer protocol
SNMP	simple network management protocol
SONET	synchronous optical networking
SSL	secure socket layer
TCP	transmission control protocol
TLS	transport layer security
UDP	user datagram protocol
UI	user interface
VLAN	virtual local area network
VoIP	voice over internet protocol
VPLS	virtual private LAN service
VPN	virtual private network
WAN	wide area network

1 Carrier Ethernet Equipment Market Trends
2 2016 Ponemon Cost of Data Breach Study

About Gemalto's SafeNet Identity and Data Protection Solutions

Gemalto's portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions– from the edge to the core. Gemalto's SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free