Trusted Cyber Technologies

THALES

Securing SD-WAN

End-to-End Encryption Solutions

White Paper

SD-WAN

IT networks are growing larger and becoming more widely dispersed. With endpoints stretching across multiple sites, national borders and remote locations, IT professionals are turning to more advanced ways to manage them.

SD-WAN, also known as software defined networking, does just this. Evolved to simplify the deployment and management of WAN infrastructure, its benefits range from improved agility and dynamic routing to cost efficiency and network standardization.

Its popularity is growing; between 2017 and 2022 IDC predict that the SD-WAN infrastructure market will see a 40.4% compound annual growth rate[1]. At this point, the market will be worth an estimated $4.5 billion [2].

The role of data networks

By 2023, Gartner predicts more than 90% of WAN edge infrastructure refresh initiatives will be based on virtualized customer premises equipment (vCPE) platforms or SD-WAN software/appliances[3].

As network administrators will be able to apply this orchestration layer remotely, SD-WAN is heavily reliant on data networks to work correctly. While core IT infrastructure - such as backup services and data center interconnects - rely on networks of 10Gbps or higher, wide-area networks will typically operate at speeds of 1Gbps or less.

One of the roles SD-WAN fills is to optimize network performance through dynamic routing, meaning that any security and encryption software deployed alongside it must be cost-effective. The makeup of these networks is different too; while core infrastructure will still run over private networks, many organizations will utilize public networks in an SD-WAN deployment.

Borderless infrastructure

As part of deploying SD-WAN, organizations must acknowledge the reality of borderless infrastructure. Digital transformation, the demand for agility and mobility, and the rise of the IoT means there is no longer a line where one network ends and another begins.

While these trends deliver innumerate advantages, they also pose a security challenge: Networks that are normally closed to the outside world become open and vulnerable to attack, while each endpoint added to the WAN represents another security risk.

Threats to SD-WAN

WAN technologies have expanded beyond the traditional barriers of IT infrastructure, adding risk and complexity to the network. While organizations may focus on protecting the high-speed links within their core network infrastructure, they must not forget to protect endpoints stretching out to the network edge.

Thankfully, securing WAN is a feat that is being recognized by the IT community, with 72% of technology managers stating that security is their biggest WAN concern[4] – placing it above both cost and performance.

The increasing volumes of data flowing across software defined networks is attracting the attention of cyber criminals, who are using anything from simple 'blunt force' attacks to more elaborate techniques in order to breach them. Once access is gained, these nefarious actors can either manipulate intercepted information or steal it for fraudulent use. The consequences of a breach can result in anything from a loss of IP and customer data to financial loss and reputational damage.

Alongside existing threats, organizations must also be aware of emerging technologies, such as the impending age of quantum computing.

SD-WAN security

While SD-WAN unquestionably brings a host of efficiencies, the technology also poses an inherent security risk if communication between endpoints is not properly protected. By encrypting data in motion across SD-WAN, it is possible to guarantee data integrity as, even in the event that this data is stolen, it will be unreadable and thus rendered useless.

In addition, organizations must find a cost-effective method of securing WAN data in motion as deploying hardware encryption across each endpoint is not financially viable.

This Solution Paper analyses the threats that organizations deploying SD-WAN face, explains why data in motion should be encrypted and offers guidance on choosing the right encryption solution.

[1] SD-WAN Infrastructure Forecast, IDC
[2] Ibid
[3] Gartner Magic Quadrant for WAN Edge Infrastructure via SDxCentral
[4] Gartner Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth via Fortinet

Why encrypt?

By utilizing both public and private networks, instead of relying on isolated MPLS networks for example, the data transmitted between endpoints via SD-WAN is vulnerable to attack.

Prevention technologies such as firewalls ensure data is protected at rest, yet data remains exposed when in motion. In order to guarantee the trust and integrity of the data being transmitted, organizations must act to secure it against a wide range of threats.

The breach landscape

According to Gemalto's breach level index, over 14 billion data records have been lost or stolen since 2013 - equating to almost six and a half million records per day. Of those, a mere 4% were secure breaches where encryption was used and the data was rendered useless. Malicious outsiders and accidental loss account for a combined 85% of incidents (61% and 24% respectively), with 88% of this data being used for a combination of identity theft, financial access and account access.

While data breaches occur across all industries, they are most frequent in the technology, social media, retail and government sectors due to the quantity and detail of information exchanged. It takes organizations an average of 197 days to identify a data breach and a further 69 days to contain it[5]. The consequences of these breaches include:

- Intellectual property theft
- Business disruption
- Compliance issues
- Loss of customer data
- Privacy breaches
- Financial loss

Alongside this, organizations must address the loss of trust and reputation amongst stakeholders; something that is much more difficult to attribute a value to.

Popular trends and emerging threats

Alongside existing threats, organizations must be aware of technologies that are gaining popularity, as well as those about to be introduced. The growth in SD-WAN deployment itself is an area of particular interest, with the market expected to see a compound annual growth rate of 40.4% between now and 2022 [6].

When asked about their main reasons to use SD-WAN technology, Infrastructure & Optimization (I&O) leaders indicate four key drivers: To increase availability (41%), to increase performance/reliability (41%), to reduce recurring WAN costs by using less-expensive transport (38%) and agility (36%) [7]. Additionally, 64% of IT budget increases are being driven by the need to upgrade outdated IT infrastructure[8].

The rapid growth in IoT devices and the introduction of borderless infrastructure by default will also impact data security greatly. If organizations fail to protect devices at the network edge (Layers 3 and 4), they provide hackers with opportunities to gain access to networks and farm sensitive information or input rogue data.

There has also been a notable rise in the theft of metadata (data about data). Despite the common myth, this information is sensitive and can provide a wealth of exploitable information if not properly encrypted.

The coming age of quantum computing also plays a growing part in cyber security. While the immense computing power of quantum computers will have a transformative effect on computing, there is also a risk of the technology being used for harm. Quantum computers will be able to break current AES encryption standards in a fraction of the time taken by traditional computing methods, threatening the protocols that underpin much of the world's data security.

While this seems like a distant concern, the reality is much closer. It is estimated that a quantum computer capable of breaking today's cryptography will be available within the next 10 years, meaning organizations need to introduce quantum-ready encryption now or risk the integrity of their data.

Protection vs prevention

There is a common misconception within many organizations that a robust firewall is enough to prevent unwanted access to their network. Another is that networks - private or Carrier - are inherently secure. Unfortunately, this is not the case. While the firewall can detect and eliminate a variety of penetration or denial of service attacks, it is no protection against a physical tap either inside or outside the firewall.

The only fail-safe solution to ensure that your data is secure as it travels across the network is encryption. Furthermore, your encryption solution should be de-coupled from any specific network architecture and accredited against recognized world-wide security standards.

Securing SD-WAN

By tapping into data in motion flowing across the networks utilized by an SD-WAN solution, hackers can bypass security systems in place around the data when it is at rest. Upon accessing the network, cyber criminals can intercept and steal data as it flows between the point of origination and endpoint. By gaining unsolicited access, hackers can also inject rogue data into the network compromising the integrity of the data and the platform as a whole. Network administrators must take steps to secure this data in motion, while ensuring that the performance of the network is not adversely affected.

[5] 2018 Cost of A Data Breach Study – Ponemon Institute
[6] SD-WAN Infrastructure Forecast, IDC
[7] Gartner Technology Insight for SD-WAN
[8] The 2019 State of IT, Spiceworks

End-to-end encryption

Encryption is crucial to SD-WAN and should form part of any security solution the IT community desires. Moreover, it should be deployed as an end-to-end solution. Importantly, this end-to-end crypto solution should also be network transport layer independent, allowing it to be deployed across all layers of the network (Layers 2, 3 and 4) – extending to the virtual edge. It should also secure metadata alongside main data packets.

In the event of a breach, encrypted data is unreadable by hackers and is therefore rendered useless. In addition, the forward secrecy provided by encryption solutions prevents rogue data being injected into systems.

Encrypting data also benefits organizations from a compliance perspective, with data protection regulations such as the GDPR treating 'secure breaches' differently to those that are not; potentially saving organizations from hefty fines as they demonstrate the importance of protecting the sensitive information they collect.

Network and application performance

It is crucial that an encryption solution does not impact network speed or performance.

Any increase in latency will impact the performance of the WAN; an area that an SD-WAN solution looks to improve via dynamic routing. Of equal concern is that some organizations opt for 'low-grade' data encryption technologies that appear to be effective, but come at a cost:

- Compromised network performance
- Hidden costs of lost effective bandwidth

Choosing the right encryption solution

When it comes to choosing an encryption vendor for your SD-WAN solution, it's important to consider all the possible applications. Just as important is the realization that all encryption solutions are not created equal. The very nature of SD-WAN sees data flowing from devices across the network, meaning this data must be secured throughout its journey. So-called 'hybrid' encryption devices – such as network routers/switches with embedded encryption or those using MACSec or similar standards (not originally intended for WAN security) provide "low assurance" data protection.

Meanwhile, MPLS networks are falling out of favor because of the cost and efficiency benefits SD-WAN brings in its stead. Most modern infrastructure comprises multiple network Layers; typically featuring Layer 2, 3 and 4 elements. So, organizations should look for a vendor that provides Layer agnostic encryption where possible.

There is also a cost element to consider when encrypting WAN traffic; protecting each network link with dedicated hardware encryption isn't cost-effective. While hardware encryption (such as the Thales CN Series) should be used to protect core IT and network infrastructure, organizations must look to protect their virtual CPE and virtualized WAN with virtualized encryption.

Thales CV Series virtualized encryption provides concurrent, multi-Layer encryption and support DPDK for up to 5Gbps performance.

Like the CN Series hardware encryptors, our virtualized encryption support all topologies, from P2P to Hub & Spoke and fully meshed networks. It is the ideal application to deploy alongside an SD-WAN. CV Series virtualized encryption is also highly cost-effective. There is no need to deploy large numbers of hardware encryptors and it can be easily deployed as a software implementation, with 'zero touch' provisioning.

Thales CV1000 virtualized encryption

The CV1000 is a Virtualized Network Function (VNF) providing strong and effective data encryption security with designed-in crypto-agility. Designed for large-scale WANs, the CV1000 delivers transport-Layer agnostic encryption for high-speed networks at >1Gbps.

As an VNF the CV1000 stands out from the crowd. Instant scalability means it may be deployed rapidly across thousands of network links. It delivers the same flexibility and scalability as other virtualized network functions.

The CV1000 offers state-of-the-art encryption security and key management without impacting on network or application performance*. Unlike IPSec-type encryption solutions, the CV1000 is transparent to the network; making it ideal for securing your WAN, right to the virtual edge.

Integrated support for Thales' enterprise key manager (the industry-leading centralized cryptographic key management solution) provides maximum security for the storage of master keys, the integrity of security policies and the source of entropy for the generation of cryptographic keys.

How is the CV1000 implemented?

The CV1000 is a guest virtual machine (VM) that runs on industry standard x86 hosts and hypervisors. Large-scale WAN customers do not need to be operating network visualization to implement the CV1000 as a secure and efficient security solution.

Like any VM, the performance of the CV1000 is customer target specific and dependent upon the operating environment and platform. This means that implementation specifications are a guide only.

- Vendor agnostic x86 hardware
- Host configuration – minimum recommended:
- Number of cores – three
- RAM – 2GB
- Virtual disk storage – 2GB
- DPDK Intel library packet acceleration support -enabling
- 1Gbps and up to 5Gbps bandwidth performance.

Platforms supported by the CV1000 include:

- VMware
- KVM/QEMU
- Microsoft Hyper-V

Other features and technologies supported by the CV1000 include:

- Interoperability with all Thales CN Series hardware encryptors
- Transport Independent Mode - Concurrent multi-Layer encryption (Layers 2, 3 & 4)
- Symmetric and asymmetric cryptography
- Thales' Enterprise Key Manager for master key security and random number generation
- Sentinel for simplified licensing
- Virtualized interfaces 3x para-virtualized NICs

CV1000 - key benefits

Unmatched benefits of the CV1000 expressed by end-user customers and service providers include:

- The CV1000 enables adoption of a virtualized encryption solution that does not compromise on security or network and application performance
- Instant scalability to match the scale and flexibility of virtual and software-defined networks
- No requirement to deploy large numbers of hardware encryption devices to achieve high-scale implementation of network encryption
- The CV1000 encryption security and key management model is optimized for strong and effective encryption security
- Through Transport Independent Mode, the CV1000 is suited to a multi-Layer network environment
- Competitively, the CV1000 delivers up to 30%network performance benefit over other solutions
- Ease of deployment with centralized, 'zero-touch' provisioning
- 100% interoperability with Thales CN Series encryptors
- As a software implementation of the Thales high-assurance encryption platform, the CV1000 provides a flexible, cost-effective way to encrypt all the way to the virtual edge
- Data center service providers identified the CV1000 as an optimal solution; providing strong and effective encryption security among devices within the data center itself

Maximum performance

DPDK acceleration - performance up to 5Gbps

DPDK Intel libraries enable x86 host device performance acceleration. If the host x86 device and DPDK are optimally configured, the CV1000 will deliver enhanced performance of >1Gbps up to 5Gbps.

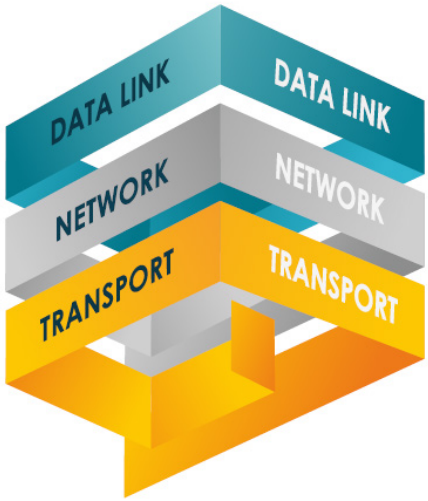
Consistent performance up to 5Gbps is dependent upon host configuration and expertise in DPDK setup and configuration. Environment and architecture factors may also play a role in virtualized encryption performance, as they do in virtualized networks.

Transport Independent Mode – concurrent multi-Layer encryption

Many organizations utilize multiple data network Layer protocols (Layer 2, 3 and 4) to help deliver their business applications and communications services. Recognizing this, Thales has designed-in Transport Independent Mode.

This advanced, transport Layer agnostic encryption technology enables destination policy-based, concurrent multi-Layer encryption.

Significantly, customers are still assured of strong, end-to-end encryption as the protected data traverses the various network Layers, for example: from Layer 2 Ethernet to Layer 3 IP network destinations.



Enhanced key security

The CV1000 is fully compatible with Thales' Enterprise Key Manager; the industry's leading centralized key management platform.

Available as a hardware appliance or a hardened virtual security appliance, Thales' Enterprise Key Manager; provides support for multiple key types: symmetric, asymmetric, secret data and X.509 certificates.

Thales' Enterprise Key Manager; simplifies the management of encryption keys across the entire life-cycle; including key generation, storage, backup, distribution, deactivation and deletion.

Thales CV1000 use case examples

Following extensive network performance testing, and a broad range of customer and service provider Proof of Concept trials, the CV1000 proved its security and performance credentials in a variety of use-cases.

Protecting the extended WAN to the 'virtual edge' (large-scale WAN deployments)

The most common use case for virtualized network data encryption is deployment across an extended WAN. The customer may or may not be adopting virtualization of the network environment itself, but will be seeking several benefits:

- Efficient use of physical IT and network resources
- Increased responsiveness and flexibility
- Low encryption-cost-per-link
- Overcome the constraints of physical asset deployment across large-scale networks
- A transport Layer agnostic solution - multi-Layer (Layers 2, 3 and 4) network security

Having decided upon a virtualized network solution for its large-scale WAN, the security conscious customer is now considering encryption security solutions.

Just as the customer uses Layer 2 Ethernet network links among core infrastructure assets, it likely protects those links (as illustrated) with hardware encryptors. To protect data travelling across the wider network, a virtualized encryption security solution may be a better fit:

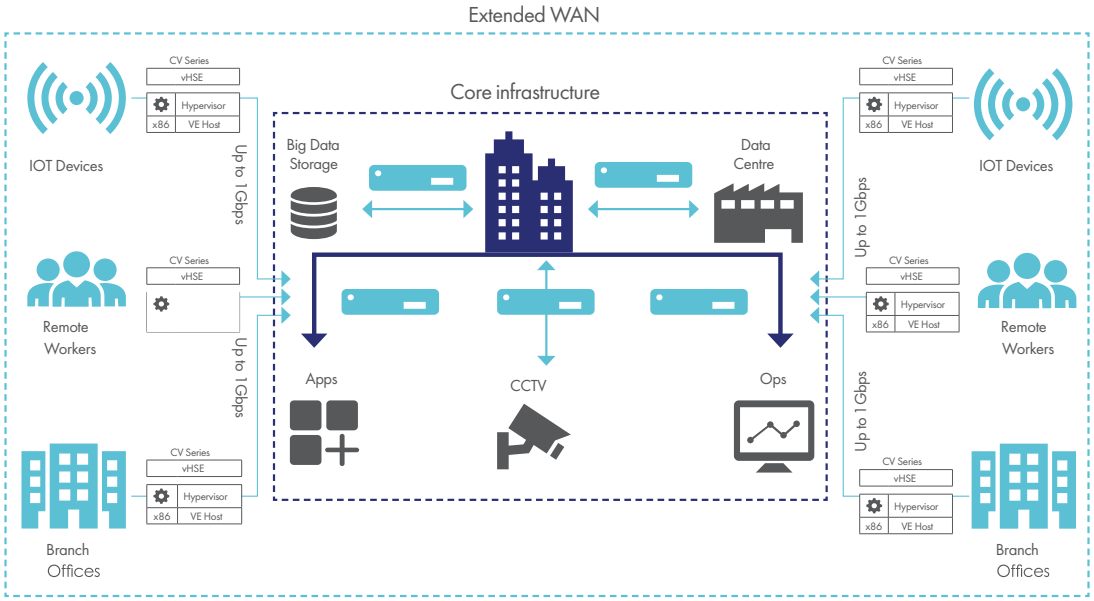
- Delivering the ability to scale rapidly
- Providing ease of deployment via a software implementation
- Enabling strong and effective security at a low cost-per-link

Because the CV1000 is transport Layer agnostic, it provides the flexibility of destination policy-based, concurrent multi-Layer (Layers 2, 3, and 4) encryption security. Customers' environments may include:

- A high-performance, multi-core (minimum recommended is four cores) x86 host for the CV1000
- DPDK Intel library for packet acceleration
- Multi-Layer (Layers 2, 3 and 4) network links
- VMWare or similar visualization environment
- CN Series hardware encryptors used for core Ethernet network infrastructure – 100% interoperable with the CV1000

An important issue of systems growth today is the infrastructure required to support it. Organizations are realizing that what is necessary to enable that growth need not be physical. By virtualizing some physical assets there are significant cost and utilization advantages. One key example is the network.

Protecting the extended WAN to the 'virtual edge' (large-scale WAN deployments)



About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

The Thales CN and CV Series Network Encryptors are available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technologies.

For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com