CERTES NETWORKS

USE CASE
SD-WAN AND NCSC PRIME

Supporting the emergence of internet and SD-WAN supplier network solutions

SITUATION ANALYSIS

Customers:

Defense – Use System Integrators (SIs) for connectivity who have data centers that are used by the U.K. defence.

Central Government (foreign office, home office, government departments) – Use MSPs (Tier 1 and Tier 2) who will either provide the connectivity or utilize carriers (who will manage connectivity on behalf of the central government entity)

Blue Lights (similar to central but are local government) – Have latency requirements for emergency services as well as the security required.

Public sector organisations in the UK are in the midst of changing cyber security regulations. In mid-2018, the Government, in collaboration the NCSC, published a minimum set of cyber security standards called PRIME. These standards are now mandated, along with a focus on continually "raising the bar".

The PRIME standards set minimum requirements for organisations to protect sensitive information and key operational services, which – given the way in which these services are increasingly dispersed – is driving significant changes in public sector network architecture and security.

PRIME is required for all of public organisations and will be mandatory by 2023, if not sooner as Foundation standards for IPsec expire and public sector organisations move quickly from legacy platforms to support internet and SD-WAN supplier network solutions. In the interim, public sector organisations will be expected to have adopted a 'gold-standard' cyber security profile along with Common Criteria EAL 4+/ISO1540 certification.

There are some essential considerations that will help organisations select a "gold standard" cybersecurity provider. Some of the considerations will include:

- An encryption management solution that can easily integrate into any network or transport as customers migrate from Legacy MPLS to SDN or SD-WAN network architectures.
- This will require a scalable solution that is a network agnostic that does not impact current network functionality.
- However, the main challenge for governments who are looking to implement a proven framework encryption solution that meets PRIME standards (UK local, national and defence) will be maintaining separation of duties to keep security separate from the network infrastructure.

With the move toward SD-WAN, security may be built into SD-WAN services but customers' data is not separate from the SD-WAN. How do governments ensure customer data is secure without being liable for any data compromise by taking responsibility for this mission-critical requirement?

Connectivity (whether internet or MPLS) is primarily, but not always, managed by either an SI or MSP. However, the MSP does not want to entrust the carriers providing connectivity with the end-user data.

Conversely, the MSP's customers do not want to entrust the security of their data to the MSP. The customer wants to eliminate risk to their data from both the MSP and whatever carriers the MSP may be using for the connectivity. Using a solution that provides clear separation of duties allows the customer to encrypt and protect their data prior to sending it over the MSP/carrier networks. This takes the MSP and carrier sub-contractors out of scope of the customers risk management program.

Moving from Legacy to SD-WAN

For both public and private sector organisations, customer experience is key. From finance and utilities, to local authorities and smart cities, customer touchpoints are increasingly dispersed, remote and application-driven, necessitating a move from Legacy MPLS to SDN or SD-WAN.

However, under the Government's new minimum cyber security standards framework, ensuring sensitive information and key services are protected is a critical consideration.

The UK's National Cyber Security Centre (NCSC) has therefore issued principles for cyber secure enterprise technology to organisations, including guidance on deploying and buying network encryption, with the aim of reducing risks to the UK by securing public and private sector networks. This guidance bears parallels with the US National Institute of Standard and Technology's (NIST) Cybersecurity Framework and therefore applies equally to US and other federal organisations in a similar scenario.

Similar to the NIST framework, the NCSC guidance shares the same principle that networks should not be trusted. It recommends that to keep sensitive information protected, encryption should be used between devices, the applications on them, and the services being accessed. IPsec is the recommended method for protecting all data travelling between two points on a network to provide an understood level of security, with further guidance outlining a specific 'gold-standard' cipher suite profile known as PRIME.

The guidance is based on the network vendor being CAS(T) certified (CESG (Communications Electronics Security Group) Assured Services (Telecommunications)), which involves an independent assessment focused on the key security areas of service availability, insider attack, unauthorised access to the network and physical attack. However, there are challenges.

CHALLENGES

1

Public Sector Adherence to CAS(T)

Many public sector organisations are no longer mandating CAS(T) based services and therefore the risk appetite is expected to be lowered, mainly to support the emergence of internet and SD-WAN suppliers network solutions. This is key as the current NCSC recommendation Foundation standards for IPsec will expire in 2023, and users are being encouraged to move quickly off legacy platforms.

2

Impact to Cloud Service Providers and Bearer Networks

This guidance, such as the protection of information flows on dedicated links between organisations, also applies to cloud service providers, or in the inter-data-centre connections in such providers' networks.

The underlying bearer network is assumed not to provide any security or resilience. This means that any bearer network (such as the Internet, Wi-Fi 4/5G, or a commercial MPLS network) can be used. The choice of bearer network(s) will have an impact on the availability that an encrypted service can provide.

3

Partner Collaboration

NCSC explicitly states in its guidance that establishing trustworthy encrypted network links is not just about technology. It is also important that the management of these networks links is carried out by appropriate individuals, performing their assigned management activities in a competent and trusted fashion, from a management system that protects the overall integrity of the system. Thus, for encryption solution providers, the partner's service credentials impact how the end user may use the technology.

PRIME PRINCIPLES

IPsec helps protect the confidentiality and integrity of information as it travels across less-trusted networks, by implementing network-based encryption to establish Virtual Private Networks (VPNs).

Under PRIME principles, devices which implement cryptographic protection of information using IPsec should:

- Be managed by a competent authority in a manner that does not undermine the protection they provide, from a suitable management platform
- Be configured to provide effective cryptographic protection
- Use certificates as a means of identifying and trusting other devices, using a suitable PKI
- Be independently assured to Foundation Grade, and operated in accordance with published Security Procedures
- Be initially deployed in a manner that ensures their future trustworthiness
- Be disposed of securely

Keeping the network design simple is one of the most effective ways to ensure the network provides the expected security and performance. The use of certificates generated in a cryptographically secure manner allows VPN gateways and clients to successfully identify themselves to each other while helping to mitigate brute force attacks.

SOLUTION

There are many encryption solutions to help agencies and governments who want to move from Legacy MPLS to SDN or SD-WAN. Selecting a provider that can offer a PRIME compliant solution – such as Layer 4 encryption – is key in conforming to both today and tomorrow's cybersecurity standards.

And with NCSC starting to treat all networks as untrusted networks (especially those agencies using internet), PRIME is becoming the gold standard for which NCSC will measure regulatory compliance.

Certes Networks offers CC EAL 4+/ISO1540 certification, promoted by NSCS, and a security management solution that can measure regulatory compliance.

Certes Layer 4 solution encrypts data in transit allowing for secure encryption of only the payload enabling transparent deployment that operates independently of applications and the underlying network with zero changes to routers, switches and firewalls. Network visibility and operational functionality are thereby fully maintained with zero impact to performance.

The Certes Layer 4 solution that is not only compliant with PRIME, but is simple and uncomplicated, minimising disruption, resources and costs integrating easily into any existing network or transport.

And, with Certes Enforcement Point (CEP) encryptor appliances, we offer scalability with the ability to support multiple deployments across a multi-vendor environment on any network or transport. With Certes Layer 4 technology, a customer can be sure that their data assurance posture will scale to support the depth and breadth of a customer's environment, whether deployed top-of-rack, in a virtual environment, between data centers and applications (east to west) or simply just across the WAN or SD-WAN.

Based on this scalability, security is built into the SD-WAN services but customers' data is not separate from SD-WAN, enabling encryption between all sites, whether one-site or remote and regardless of geographic location.

In addition, using the Certes Layer 4 solution provides clear separation of duties and allows the customer to encrypt and protect their data prior to sending it over the MSP/carrier networks. This takes the MSP and carrier sub-contractors out of scope of the customers risk management program.

Measuring Regulatory Compliance with Certes Networks Provable Security™

To help network security teams to achieve their PRIME goals of data assurance, organisations must begin to think of data security as a measurable contribution to the organisations.

Certes Networks Provable Security™ is compliant with PRIME standards and is a proven framework and solution that goes well beyond the requirements. It introduces a new way to think about data security and the effectiveness of a security strategy based on the Certes Five Pillars, key performance indicators (KPIs) that are quantifiable, measurable and outcomes driven.

The Certes Layer 4 solution, provided via the Certes Enforcement Point (CEP) encryptor appliances, and the Certes key management and observability software features, delivers on these KPIs in order to quantify security's role to build, modify and measure a security strategy that aligns and protects the needs of the retailer.

Certes Layer 4 technology securely encrypts data while mitigating the risk of a data breach and also allows for observation and analysis of contextual meta-data in order to improve their security strategy.

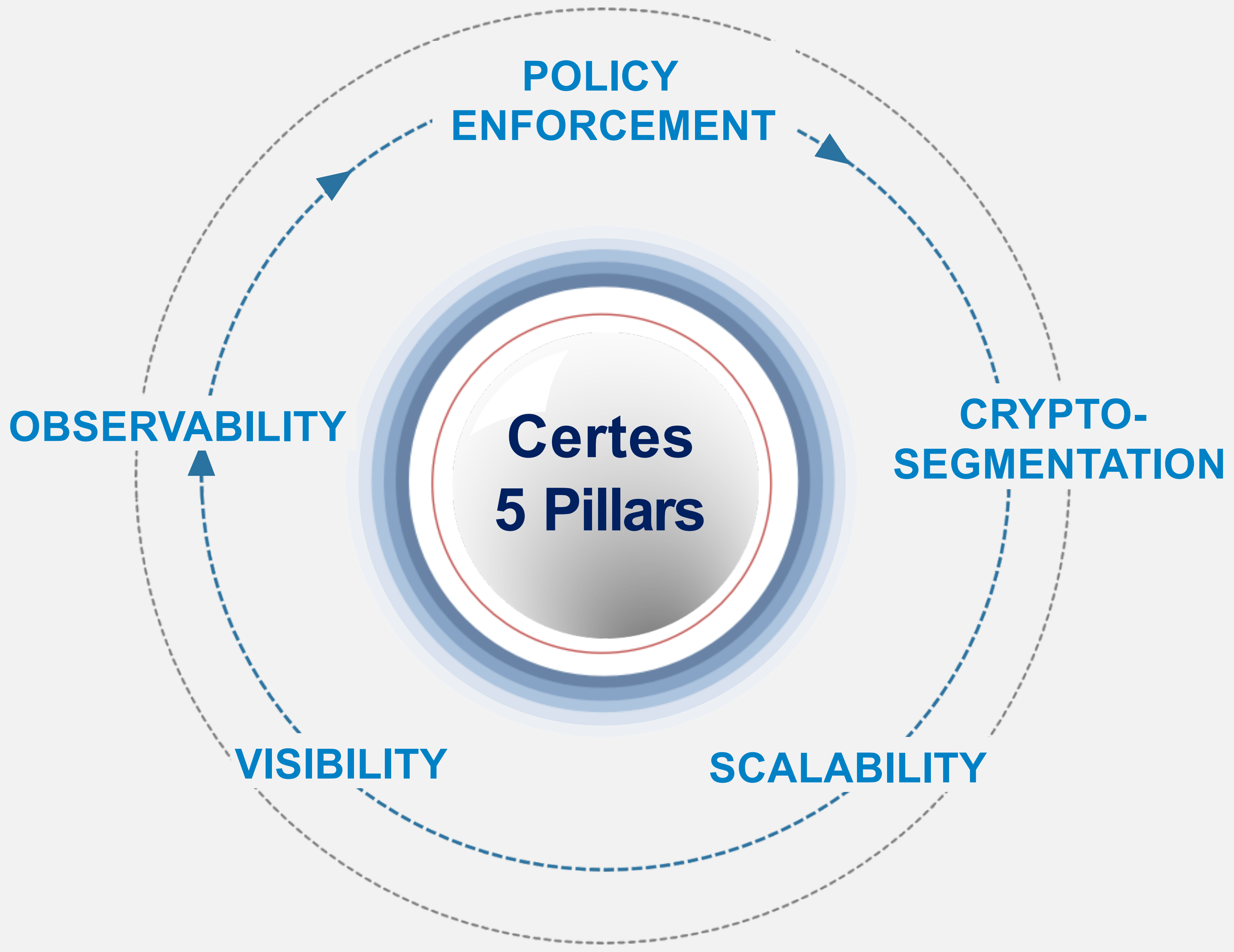
CERTES FIVEPILLARS

Pillar One: Policy Enforcement

Certes Networks Provable Security™ starts with the premise that policy enforcement is only as good as the policy defined and how that policy is enforced.

While threats are virtually infinite, access to data is defined and is therefore finite and measurable. By enabling policy and enforcing that policy at a highly granular level, risk can be eliminated and data security can be quantified, measure and outcomes driven.

CERTES NETWORKS PROVABLE SECURITY™



Quantifiable, Measurable and Outcomes Driven

Pillar Two: Crypto-segmentation

Certes Networks Provable Security™ is based on the Certes Five Pillars or KPIs. Pillar Two, Crypto-segmentation, removes the implicit trust we traditionally place in our network and creates a reduced scope of trust per policy, protected by encryption, to securely separate data flows between applications and workloads as defined by fine-grained policies.

This security control is simple to deploy, however it increases the complexity involved and reduces the attack surface over which targeted data flows. This is a quantifiable and measurable metric.

Pillar Three: Scalability

Scalability, refers to the Certes Layer 4 technology, a simple and scalable, end-to-end encryption management solution that is network agnostic easily integrating into any network infrastructure, fully interoperable with the existing security stack with zero impact to performance.

Certes Networks offers the ability to support multiple deployments across a multi-vendor environment on any network or transport. With the Certes Layer 4 solution a customer can be sure that their data assurance posture will scale to support the depth and breadth of a customer's environment, whether deployed top-of-rack, in a virtual environment, between data centers and applications (east to west) or simply just across the WAN or SD-WAN.

Pillar Four: Visibility

Certes Networks Provable Security™ is based on the Certes Five Pillars or KPIs and Pillar Four is Visibility. The Certes Layer 4 solution encrypts data in transit allowing for secure encryption of only the payload enabling transparent deployment that operates independently of applications and the underlying network with zero changes to routers, switches and firewalls. Network visibility and operational functionality are thereby fully maintained with zero impact to performance.

Pillar Five: Observability

Certes Observability is a mandatory KPI and completes the Five Pillars of Certes Networks Provable Security™ to quantify and measure a security strategy that aligns with the business needs of an organization while mitigating risk.

Certes Observability is the linchpin that provides real- time contextual meta-data enabling rapid detection of out-of-policy data and fast response and remediation to any non-compliant traffic flow or policy change to maintain the required security posture on a continuous basis. Certes Observability provides evidential and visual proof that an organization's security strategy is effective.

CERTES NETWORKS TECHNOLOGY IS PRIME COMPLIANT

Certes Networks encryption management solution is PRIME compliant. Certes encryption hardware and software technology can seamlessly integrate on tope of SD-WAN without disrupting or impacting the current network infrastructure. And, our L4 technology is not only compliant with PRIME but more advanced than the mandatory requirements themselves.

The Certes Network Layer 4 solution is the ideal solution for those public sector organisations who want to move from Legacy MPLS to an SDN or a SD-WAN architecture. And with NCSC starting to treat all networks as untrusted networks (especially those agencies using internet), PRIME is becoming the gold standard for which NCSC will measure regulatory compliance.

CERTES NETWORKS

300 Corporate Center Drive
Suite 140
Pittsburgh, PA 15108

Tel: 1(888)833-1142
Fax: 1(412)262-2574

info@certesnetworks.com
sales@certesnetorks.com

We offer an encryption solution that is simple, scalable and uncomplicated.