Publication: Information Security Buzz
Date: 28.11.19
URL: https://www.informationsecuritybuzz.com/articles/shining-a-spotlight-on-uk-cyber-security-standards/
Title: Shining A Spotlight on UK Cyber Security Standards
Author: Matt Cable, VP Solutions Architect and MD Europe, Certes Networks

Shining A Spotlight on UK Cyber Security Standards

Matt Cable, VP Solutions Architect and MD Europe, Certes Networks

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. These standards are now mandated, along with a focus on continually "raising the bar". The 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.

In addition to setting today's 'minimum' standards, however, the guidance also sets a target date of 2023 by which public sector organisations will be expected to have adopted a 'gold-standard' cyber security profile. Matt Cable, VP Solutions Architect and MD Europe, Certes Networks, therefore outlines the essential considerations that will help organisations select an encryption solution provider that can easily integrate into any network infrastructure as they migrate from Legacy MPLS to SDN or SD-WAN network architectures.

The Principles

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.

Challenge #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.

Challenge #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.

Challenge #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.

The Solution

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.

Conclusion

There are many encryption solutions to help agencies and federal governments who want to move from Legacy MPLS to SDN or SD-WAN. Layer 4 encryption, for example, can integrate easily into any network and encrypt data in transit without disrupting performance or replacing the current network architecture.

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 cyber security 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.

Therefore, it is important to consider a vendor that can offer a security solution that is not only compliant but is simple and uncomplicated, minimising disruption, resources and costs.
