USE CASE
Managed Service Provider and Multiple Carrier Networks over an SD-WAN

Global Managed Service Provider uses Certes Networks for an on-premise SD-WAN solution to provide improved services across multiple carrier networks

SITUATION ANALYSIS

MSP: Global Managed Service Provider ("MSP") that provides SD-WAN services– this is the Certes Networks Customer

End-User: Customers that the MSP Services

Multiple Carriers: End-users may use multiple carriers to transport their data

A global Managed Service Provider (MSP) using an SD-WAN wanted a more secure, on-premise solution to improve services and data security for its end-users who used multiple carriers to transport their data.

The MSP was concerned about the safety of the end-user data as it passes over the carrier networks that the MSP resells. The MSP did not want critical data to pass through the carrier networks without security measures and data protection in place and did not want to outsource this.

CHALLENGES

The challenge the MSP faced started with maintaining separation of duties to keep security separate from the network infrastructure. How do they ensure the end-user data is secure without taking responsibility for this mission-critical requisite.

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

Conversely, the MSP's end user does not want to entrust the security of their data to the MSP. The end user wants to eliminate risk to their data from both the MSP and whatever carriers the MSP may be using for the connectivity. Using Certes Networks to provide clear separation of duties allows the end user 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 end-user's risk management program.

SOLUTION REQUIREMENTS

The global MSP approached Certes Networks to inquire about whether they had a scalable encryption management solution that would integrate into an SD-WAN without disrupting their environment.

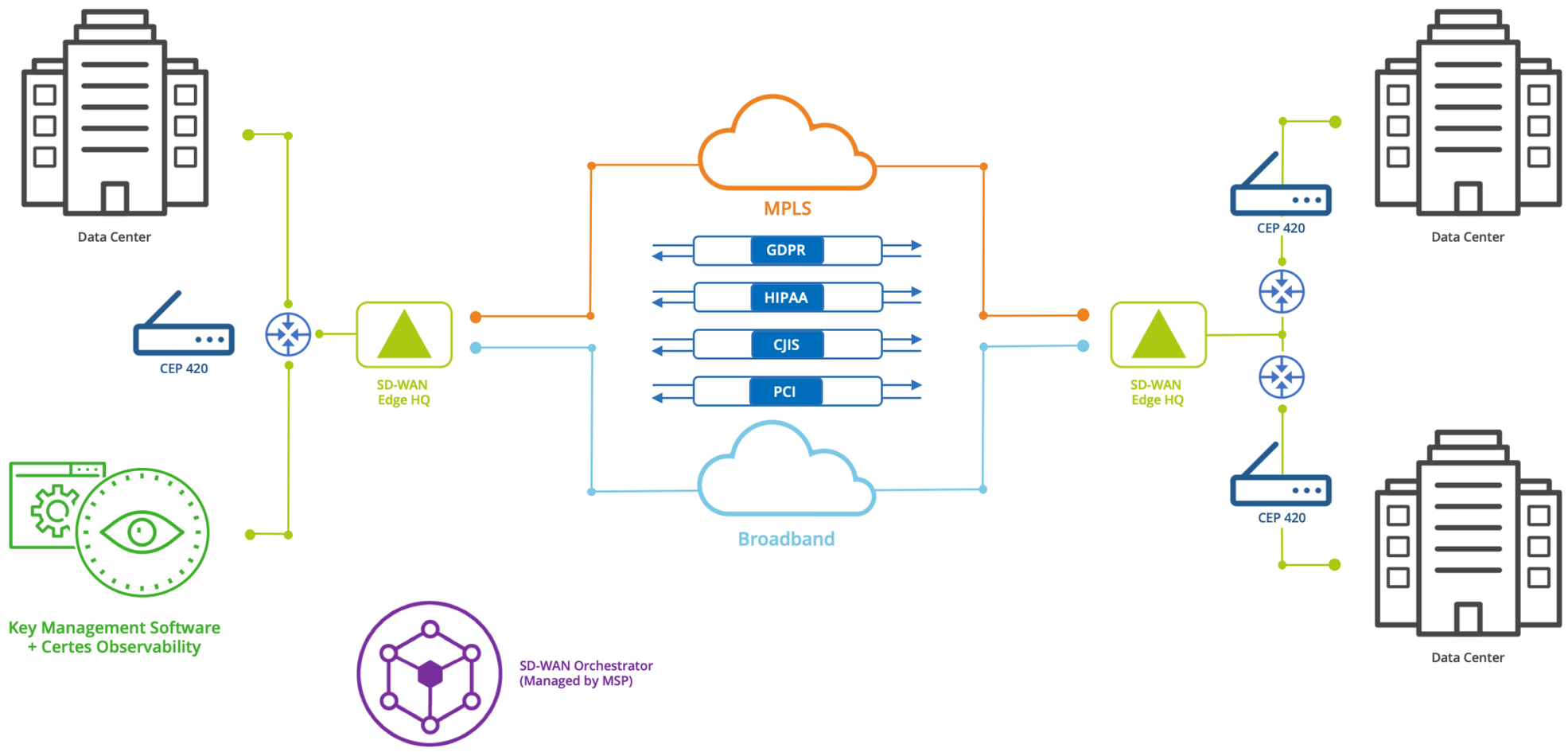
In addition, the MSP had enterprise, government and high assurance customers, all of whom were under varying data protection regulations. Not only did the MSP have a great need to keep the customer data separate to mitigate risk, but also the ability for each of the customers to create fine-grained policies and enable crypto-segmentation segment for all the varying regulations. And, some of the customer would require FIPS 140-2 or Common Criteria certified equipment to do so.

The MSP had 50 locations around the world using local carriers at each location. At least two links from different carriers in all locations would be needed to provide redundancy, including 1Gg links at Headquarters (HQ) and the data center, varying speeds at each branch based on the local availability of internet bandwidth ranging from 20 MB to 100 MB.

Requirements included the need for management tools that did not blind their existing networks with IPSEC tunnels, simple policy management and the ability to keep control of the keys.

Current equipment consisted of two (2) SD-WAN routers in a failover pair at the Headquarters with the need for an Ethernet handoff from LAN to WAN via Copper RJ45 at 1 GB from LAN with the same equipment and requirements needed at the Branch (see deployment diagram and Certes Networks solution on Page 2).

CERTES NETWORKS SOLUTION & DEPLOYMENT DIAGRAM



SOLUTION OVERVIEW

Certes Networks offered a unique Layer 4 encryption management solution that was network agnostic overlay with the ability to integrate easily into the SDN with zero impact to performance.

This on-premise transparent secure overlay 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 technology can create L4 encryption policy to keep the L3/L4 headers in the clear and enable the existing SD-WAN solution to perform routing on encrypted traffic. In addition, the key management software, CryptoFlow Net Creator, could be located at HQ so that each customer can maintain control over keys and their respective security posture

DEPLOYMENT AND BILL OF MATERIALS

Deployment:

AT HQ:

- Two SD-WAN routers in a failover pair
- Two CEP420s for redundancy
- Ethernet handoff from LAN to WAN via Copper RJ45 at 1Gbs from LAN switch to CEP Local port

AT Branch:

- One SD-WAN router
- One CEP250
- Ethernet handoff from LAN to WAN via Copper RJ45 at 1Gbs from LAN switch to CEP Local port

* Encryptors or Certes Enforcement Point Appliances (CEP)

SOLUTION

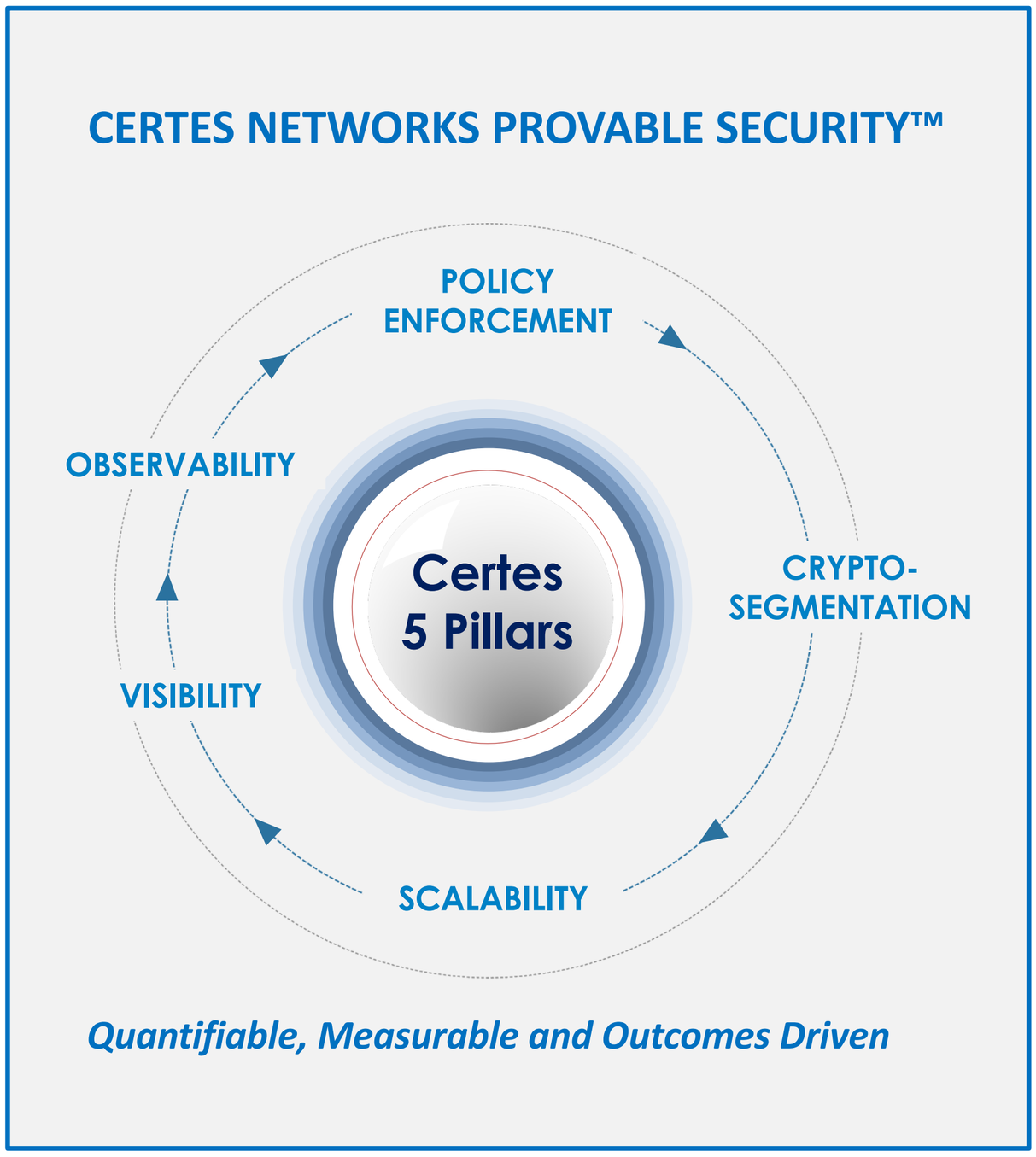
Certes Networks Provable Security™

To help the MSP and their network security team to achieve their goal of keeping end-user data safe, Certes Networks we were able to introduce Certes Networks Provable Security™ a novel way to think about data security and the effectiveness of the bank's security strategy based on features that are ***quantifiable, measurable and outcomes driven.***

Certes Layer 4 Technology Delivers on Provable Security to Measure Security Effectiveness

Certes Networks Provable Security™ is supported and interconnected by the Certes Five Pillars. Each pillar will quantify and measure the value that the security strategy delivers to the retailer as a whole.

The Certes Layer 4 solution, provided via the vCEPs, 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 FIVE PILLARS

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.

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 for any attacker trying to exploit a network 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.

RESULTS

With the successful installation of the Certes Layer 4 encryption solution, the multiple carriers were able to mitigate risk by separating the network security from the infrastructure. The CEPs provided an on-premise data encryption solution by adding a substantial security measure to eliminate risk and secure data flows for the carriers and respective end-users.

In addition, there was a significant cost savings with the easy to integrate Certes technology which supported the deployment request for an Ethernet handoff from LAN to WAN at both HQs and the one Data Center.

Moreover, with Certes Networks Provable Security™, the benefit of crypto-segmentation created 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 for each end-user. This security control was simple to deploy and increased the complexity involved for any attacker trying to exploit a network over which targeted data flows.

The Certes Layer 4 encryption management solution allowed the multiple carriers and end-users take advantage of the management services provided by the MPS while securely encrypting end-user data and separate these data flows from the MPS and SD-WAN.

Contact 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.