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 for banking customers

SITUATION ANALYSIS

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

End-User: Banking customers that the MSP Services

Multiple Carriers: Banking customers (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. To provide a more secure SD-WAN for customers, separating security from the WAN infrastructure (SD-WAN) would be needed which would include a secure overlay whereby customers could maintain full control of the key management platform and segmentation of policies. Without these, the SD-WAN could be compromised and not only would data be accessible but so would access to security, thus increasing network vulnerabilities.

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 being liable for any data compromise for this mission-critical requirement of data assurance.

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

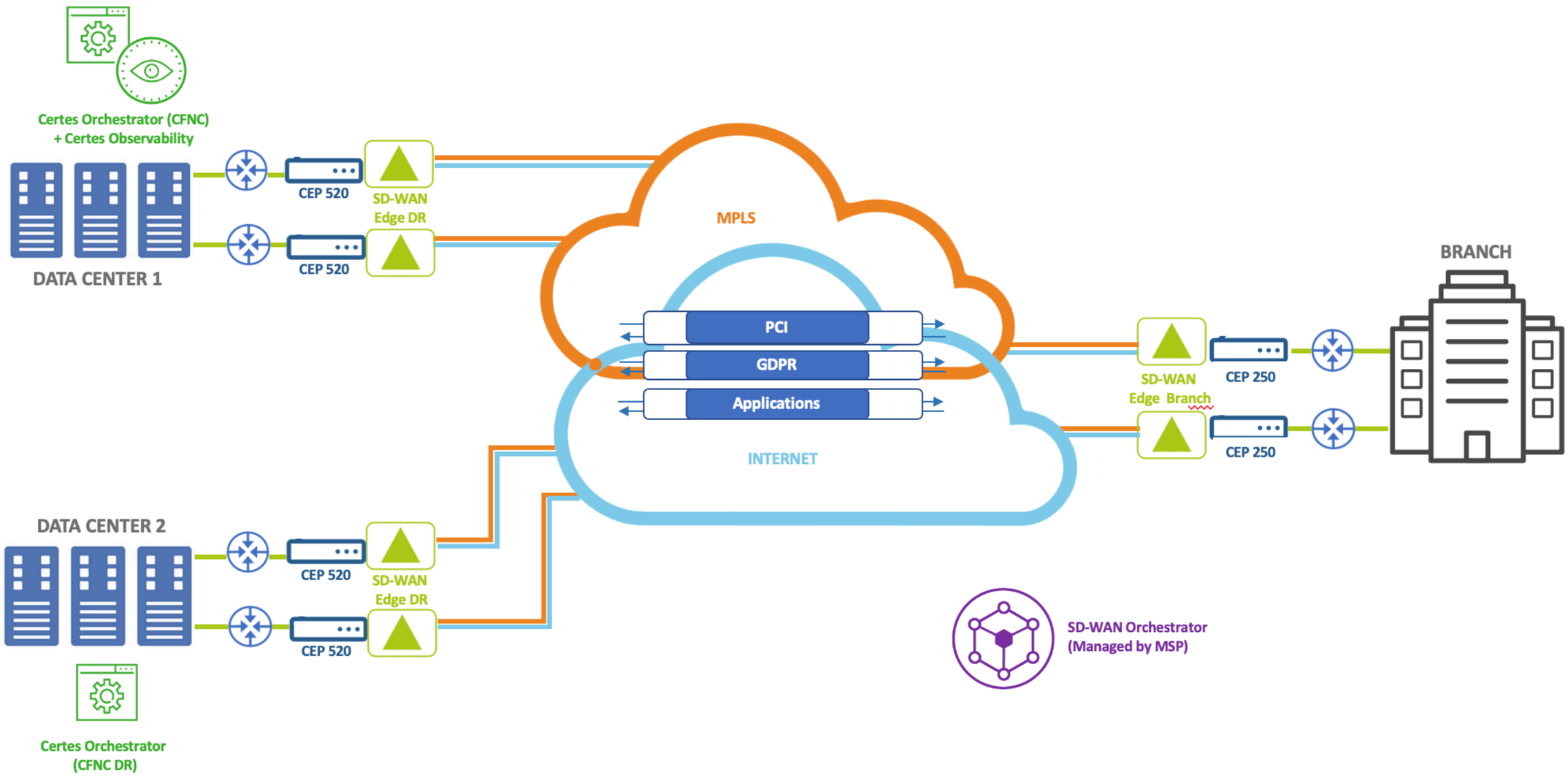
The global MSP approached Certes Networks to inquire about whether they had a scalable encryption management solution that would integrate into an SD-WAN without disrupting their environment.

In addition, the MSP had banking 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 applications and regulations.

The MSP had a customer with 100 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 10Gg links at Headquarters (HQ) Data Centers, and varying speeds at each branch based on the local availability of internet bandwidth ranging from 20 Mb to 100 MB 1Gb.

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.

CERTES NETWORKS SOLUTION & DEPLOYMENT DIAGRAM



Current equipment consisted of two (2) SD-WAN routers in a failover pair at the Headquarters (both Data Centers) with the need for an Ethernet handoff from LAN to WAN edge via Fibre at 10 Gb. At the branches from LAN with the same equipment and requirements needed at the Branch (see deployment diagram and Certes Networks solution above).

SOLUTION OVERVIEW

Certes Networks offers a unique Layer 4 encryption management solution that is a 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 is located at HQ so that each customer can maintain full control over keys and their respective security posture.

DEPLOYMENT AND BILL OF MATERIALS

At Data Center 1:

- Two SD-WAN routers in a failover pair
- Two CEP* 520s for redundancy
- Ethernet handoff from LAN to WAN via 10Gb Fibre SFP+ between LAN switch to CEP Local port and CEP remote port to SD-WAN edge
- Certes Cryptoflow Net Creator (CFNC) hardware with Quantum Random number generator (QRNG)
- Certes Observability (flow export) to customer analytics server

At Data Center 2:

- Two SD-WAN routers in a failover pair
- Two CEP 520s for redundancy
- Ethernet handoff from LAN to WAN via 10Gb Fibre SFP+ between LAN switch to CEP Local port and CEP remote port to SD-WAN edge
- Certes Cryptoflow Net Creator Hardware (CFNC in DR mode) with Quantum Random number generator (QRNG)

At Branch:

- Two SD-WAN routers in a failover pair
- Two CEP 250s for redundancy
- Ethernet handoff from LAN to WAN via 1Gb Copper RJ45 between LAN switch to CEP Local port and CEP remote port to SD-WAN edge

* 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 introduces Certes Networks Provable Security™ a novel way to think about data security and the effectiveness of a security strategy based on features that are ***quantifiable, measurable and outcomes driven.***

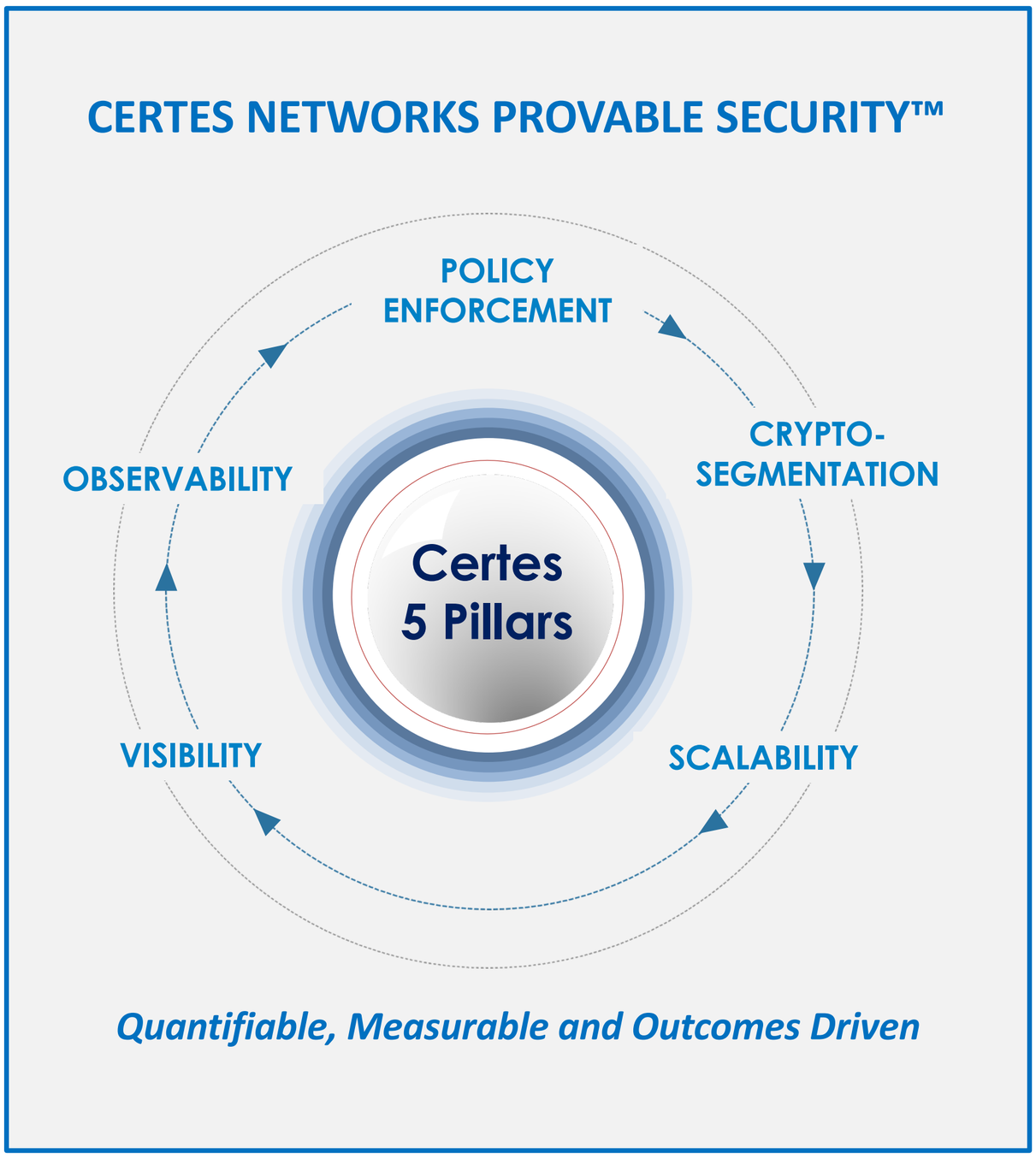
Certes Layer 4 Technology Delivers on Provable Security to Measure Security Effectiveness

Certes Networks Provable Security™ is supported and interconnected by the Certes Five Pillars or key performance indicators (KPIs). Each pillar will quantify and measure the value that the security strategy delivers as a whole.

The Certes Layer 4 solution, provided via the Certes Enforcement Point (CEP) appliances, Certes key management platform 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 MSP and end-user. Certes Layer 4 technology securely encrypts data in transit providing the data assurance banking customers are seeking along with ability to observe and analyze contextual meta-data in order to improve their security strategy.

Data Assurance over a SD-WAN with Certes Networks Provable Security™

A challenge that most Managed Service Providers (MSP) is ensuring that their customers' data is encrypted safely in an SD-WAN environment and the integrity and confidentiality of that data is assured. Through Certes Networks Provable Security™, data assurance is solved with Certes crypto-segmentation in which fine-grained policies are easily defined per policy and application across the SD-WAN. Whether it is keeping the end-user's encrypted data secure and separate from the MSP network and/or defining fine-grained policies for customers to classify important data, Certes Networks Provable Security provides the data assurance MSPs and their end-users are seeking while mitigating risk and reducing the attack surface for everyone.



Certes Networks Provable Security focuses on three key solutions that must be delivered in order to provide data assurance over a affect SD-WAN:

DATA ASSURANCE WITH SEPARATION OF DUTIES SECURING POLICIES OVER AN SD-WAN

Certes Networks Layer 4 solution eliminates the risk for the Managed Service Provider (MSP) and end-user(s) with the separation of duties.

Through crypto-segmentation, fine-grained policies are defined and enforced to protect the confidentiality and integrity of the end-user's data.

Benefit to MSP

- Carrier does not take on the risk of having to manage and protect confidentiality and integrity of customers data
- Carrier does not have to accept risk to protect end-user data when it's on their network – it remains the responsibility of the end-user

Benefit to Banking Customers

- End-users do not have to entrust carrier with security of their data
- Eliminates risk with separation of duties
- End-users do not have to trust carrier team or network to be secure
- End-users are only responsible for encrypted data before it enters the carrier network, which is out of scope of end-user's risk management program

GENERATING FINE-GRAINED POLICIES

Certes Networks Layer 4 solution eliminates the risk for the Managed Service Provider (MSP) and end-user(s) with separation of duties generating fine-grained policies for customers.

Crypto-segmentation for fine-grained policies

Separate policies and distinguish between banking data applications and/or regulatory standards, such as GDPR and PCI.

Certified Equipment

Ensure maximum security and control for an always operational network with FIPs 140-2 and Common Criteria EAL4+ certified equipment

NETWORK AGNOSTIC OVERLAY

Scalable Implementation into any network or transport

Certes Networks Layer 4 solution is a network agnostic overlay which integrates easily and sits on top of SD-WAN to make the SD environment more secure and to meet the needs of Managed Service Providers and their banking customers.

Ease of Integration

- Network agnostic overlay that sits on top the SD-WAN

Fully Interoperable

- Simple solution that interoperates with SD-WAN

Zero Impact to Performance

- No latency or impact to network performance

Scale to Support Customer's Environment

- Supports depth and breadth of a customer's environment

Maintain SD-WAN Operations

- Operate without impacting SD-WAN core functionality

RESULTS

With the successful installation of the Certes Layer 4 encryption solution, the MSP was able to mitigate risk by providing on-premise data encryption solution that added a substantial security measure to eliminate risk and secure data flows for the carriers and respective customers.

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

Moreover, with Certes Networks Provable Security™, the benefit of separation of duties through crypto-segmentation created secure separate data flows between applications and workloads as defined by fine-grained policies for each banking customer. This security control was simple to deploy and decreased the attack surface over which targeted data flows.

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

CERTES NETWORKS

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.