USE CASE:
EU Government & Member States

The Move to SD-WAN Makes Zero Trust a Best Practice

SITUATION ANALYSIS

European Governments and Member States ("Governments) are turning to SD-WAN to modernize their wide area networks. Governments are bolstering their networks with new technology.

Given the threat to national security, data, and our overall critical national infrastructure, Governments are finding it evident that they need to find ways to aggressively develop a WAN that operates over a very high band-width optical backbone, with LAN circuits in peripheral offices running from that WAN.

Governments are collecting more data from multitudes of sources and aggregating that data to use new technologies such as Artificial Intelligence (AI) and Machine Learning (ML). These sources range from remote employees to automated sensors that are very likely to be distributed and are no longer located in one central site. Strong connectivity is essential in today's government, and agencies are turning to a variety of methods – from WANs to SD-WANs – to keep communications safe and moving. Some government agencies are now testing SD-WANs in their global data centers using products from approved suppliers in hopes to make the technology standard across the governments over the next few years.

Yet, SD-WAN technology is still in its early adoption stage in the this sector. However, the benefits and flexibility of the rapid adoption of these resources will make government networks more secure and resilient. And, as a software-defined perimeter it would make it easier to microsegment each network, allowing access only to verified applications, devices, and users. Modernizing network infrastructure with Zero Trust architecture functionality and SD-WAN will help governments get closer to a modernized Zero Trust Architecture by 2021.

CHALLENGES

Traditionally, organizations have operational WANs over MPLS lines leased from major telecoms. To ensure high availability, many organizations lease two lines from two separate carriers for a failsafe.

Some governments evolving toward SD-WAN run over a standard broadband connection and use 4G wireless as backup. This may give some more control over the networks, but SD-WAN can complement or replace legacy WAN.

But the transition from WANs running over MPLS to SD-WAN will not happen rapidly. Three-year telecom contracts need to expire, routers and switches must be updated and many agencies fear their entire network infrastructure will have to be replaced. And, all without a budget to allow for the capability of SD-WAN.

Additionally, maintaining fast, reliable connections to government regional offices is crucial, especially as agencies expand their use of VoIP, adopt cloud-based office automation and migrate their constituent services on-line.

And, to compound matters, some agencies still operate relying on landlines, mobile phones and emergency radios. This constant worry about limitations due to the failure of cellular, fiber-optic and landline networks seems unnecessary in today's sophisticated technology environment.

SOLUTION REQUIREMENTS

Certes solutions are FIPS 140-2 validated and Common Criteria certified. And, as supplier who is PRIME Compliant, Certes Networks is able to work with governments in SD-WAN modernization.

Delivering new technology across such large government networks is a perfect opportunity for Certes Networks. Our encryption management solution is simple, scalable and uncomplicated and does not require a rip and replace of current WAN technology – our technology is network agnostic using our software-defined Layer 4 encyrption solution. Connecting our CEPs and CFNC™ software over an SD-WAN can provision a network without the need to replace major infrastructure components. And with the Certes vCEPs, virtualization can give governments the scalability and flexibility government CIOs are looking for.

THE SOLUTION

SIMPLE, SCALABLE & UNCOMPLICATED

Certes Networks can help governments make the move toward SD-WAN and Zero Trust without the complexity that comes with the deployment of a more automated infrastructure. The vulnerabilities and threats associated with trying to protect large volumes of data moving across a vast multi-user network involves a security strategy that is simple, scalable and uncomplicated in order to avoid any disruption to the national network architecture and the critical services provided by these governments.

CRYPTO-SEGMENTATION

Advanced persistent threats even within Zero Trust zones go undetected for months (266 days average to detect/contain) during which sensitive data is compromised. [2]

Crypto-segmentation removes the implicit trust and helps prohibit lateral movements. Crypto-segmentation creates small zones by which organizations can separate applications and workloads from each other to secure each one individually.

Certes CryptoFlow® Network Creator software is a Zero Trust crypto-segmentation solution that now makes crypto-segmentation possible. Certes adds policy-based segmentation and metadata that enhances the detail of network visualization and allow organizations to visualize how applications communicate in real time.

They help you monitor your environment to identify unexpected or unusual traffic patterns that may indicate a threat.

And, with the Certes Observability feature, you can see all assets and applications that are attempting to access your network. This transparency allows you to analyze the potential risk of communicating applications, which serves to build the foundation for security policy enforcement. Enhanced visualization with Certes Observability gives you controlled policy-based security access of your network environment.

OBSERVABILITY

With Certes Observability, IT security teams are now doing more than just trying to monitor and identify threats to keep them out of the network. Through generating and defining policies, network policy enforcement will ensure that only authorized applications are communicating with one another while enabling agencies to meet their own governance, security and compliance requirements.

Certes Observability is configured to encrypt specified business data between network sites. Network policies and applications data are exported by our 5.6 CEP appliances in NetFlow format and also contain Certes-specific metadata. This combination of raw data can be used to analyze and gain a deeper understanding of network policy deployment and enforcement to analyze every application that tries to communicate across the network. And, all the while monitoring pathways for potential threats because each policy is observable in real-time. As most governments need to comply with cybersecurity regulations like PRIME, please be sure to understand which Certes Networks encryption solution will be best for compliance assurance.

THE RESULT

By implementing Certes Networks security solutions we help governments easily transition to an SD-WAN and work toward a Zero Trust network environment. The Certes Layer 4 solution offers a simple, scalable and uncomplicated solution without having to disrupt, replace or move the current network infrastructure. Certes can also provide MPLS application visibility while also adding policy-based value with our Observability feature.

[1] Agencies Turn to SD-WAN to Modernize Wide Area Networks, FedTech, August 2019

[2] Hide and Seek – Cybersecurity and the Cloud, VansonBourne, *Aug 2017*

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@certesnetworks.com

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