USE CASE: STATE GOVERNMENT

Using Crypto-Segmentation™ to Protect Your Data

SITUATION ANALYSIS

For CSOs and CISOs within State government, breaches are damaging and controversial as trust is eroded and difficult to regain. Breaches aren't just devastating to the integrity of the institution, but possibly damaging to the citizens that government is pledged to serve. While information integrity and data privacy are critical issues, the notion that a perpetrator can plan an attack that significantly disrupts government operations and creates vulnerabilities is indeed real.

A NEW APPROACH: CRYPTO-SEGMENTATION™

There is a better way to approach security. Crypto-Segmentation™ takes on the mission of the old-style router Access Control Lists (ACLs), but with an entirely new approach that allows government to quickly and easily divide physical networks into thousands of logical segments. Even if adversaries infiltrate one segment, they would not be able to laterally move across to other parts of the agency's environment.

Crypto-Segmentation™ is a new security approach for government. It offers a simple way to mitigate risk by taking back control of an enterprise network without having to deal with firewall rules, outdated applications, remote users, cloud-based services, and third parties that all have become attack vectors in today's world.

Crypto-Segmentation™, removes the implicit trust we traditionally place in our network and creates a reduced scope of trust per policy, protection by encryption, to securely separate data flows between applications and workloads as defined by fine-grained policies.

Crypto-Segmentation™, commonly associated as a key function of the Zero Trust architecture, is where all networks are considered untrusted. 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. For example, various types of policies can be applied to workloads and regulatory compliance requirements (e.g., GDPR, FIPS, CJIS, HIPAA. etc.).

As state government continues to expand their network capabilities with limited budgets, especially in light of federal guidance to modernize toward Zero Trust and SD-WAN architecture by 2021, state agencies will need to expand and migrate more citizen services to the cloud. Crypto-Segmentation™ will enable secure separation of these expanding services. It is estimated that 75 to 80 percent of public and enterprise traffic is of East-West nature and the ability to segment by application or data flows, as well as, provide visibility is critical.

CHALLENGES

1 NETOPS AND SECOPS COLLABORATION

In order for Crypto-Segmentation™ to be truly effective, state governments require open communication and information sharing across their application/ virtualization, NetOps and SecOps teams.

Defining communication policy rules on switches and routers falls within the domain of NetOps and typically occurs through the configuration of VLANs and access control lists (ACLs). These hardware-based policies only come into play, however, when traffic traverses the physical network.

SecOps is responsible for measuring and reducing the risk to the network. They evaluate and implement technology and processes in the name of risk reduction. SecOps must continually run vulnerability assessments and keep up with a dizzying pace of patch management efforts, know what applications are live, and understand which operating systems and versions are deployed.

Effective communication and cross-domain collaboration are vital for government to properly protect data and applications from potential cyber-attacks.

2 RISE OF PHISHING ATTACKS

Phishing attacks and user credentials are being stolen at an alarming rate. For example, should one bad actor obtain account credentials that allow access to the State's DMV or Social Security databases without Crypto-Segmentation of these large data sets, the resulting breach could compromise all the State's citizens data and most certainly be viewed as catastrophic.

3 DISPARATE DATA SILOS

State government is notorious for silos of networks, interfaces and tools they use to do their jobs every day. For example, most micro-segmentation-related products today fall within the domain of the application and virtualization teams. Without API integration across network monitoring platforms, security systems, and visualization management tools, NetOps and SecOps can only get the data they need by directly interacting with the virtualization team. This leads to critical errors, workflow gaps, and increased risk.

4 POLICY ENFORCEMENT VERIFICATION

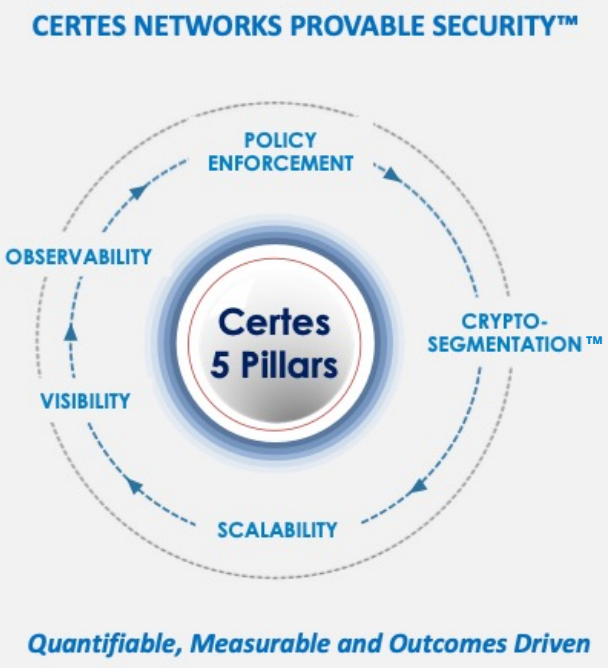
A good first step of Crypto-Segmentation™ is defining a policy and key management for only those who need to access specific data, but how does Operations know the policy is working as expected? How does it know if/when a bad actor is able to circumvent the rules applied? How do they identify human error or small security holes that hackers can leverage as footholds?

In short, how do security teams verify that what they *think* happened… happened? State government recognizes the need to incorporate new technology tools that are currently available to overcome these challenges. But many times, delays due to unexpected challenges will complicate deployment and integrations. This requires ways to see the communication in their virtualized data center, and to distribute that information to NetOps and SecOps. Both teams must have a mechanism to see into that traffic from the products and platforms they use every day.

SOLUTION REQUIREMENTS

It is important that the technology provider's products integrate with Crypto-Segmentation™. While Crypto-Segmentation™, SDN, and software-defined data center (SDDC) solution vendors provide the core foundation, other technology, like Certes Networks solutions, integrate and enrich the implementation of Crypto-Segmentation™. These include enhanced workload visibility, encryption segmentation policy and breach detection, as well as, threat detection and response capabilities. Solutions should also provide the NetOps content visibility and metrics of each flow (e.g., workload, process, user, etc.) to allow for analytics to be used.

And, all of this should be enabled through an encryption management solution that does not disrupt or require replacing the current network infrastructure thus eliminating unbudgeted costs for additional resources and equipment.



THE SOLUTION

Certes Networks Provable Security™

To help network security team to achieve their goal of keeping the regional bank's data safe, the team must begin to think of data security as a measurable contribution to the organizations. Certes Networks Provable Security™ introduces a new way to think about data security and the effectiveness of your security strategy based on the Certes Five Pillars, key performance indicators (KPIs) that are quantifiable, measurable and outcomes driven.

How We Deliver on Provable Security™

Certes Networks Provable Security™ is supported and interconnected by the Certes Five Pillars. Each pillar is a KPI that measures the value that the security strategy delivers to an organization as a whole.

The Certes Layer 4 technology solution delivers on these KPIs and is able to quantify security's role to build, modify and measure a security strategy that aligns and protects the needs of agency while mitigating risk.

The 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, measured and outcomes driven.

PILLAR TWO: CRYPTO-SEGMENTATION™

Crypto-Segmentation™, removes the implicit trust we traditionally place in our network and creates a reduced scope of trust per policy, protection 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 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.

PILLAR FOUR: 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 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.

And, as most state governments and agencies are governed by state or federal cybersecurity regulations, Certes Networks encryption solution will be best for compliance assurance.

OBSERVABILITY

With the Certes Observability release, organizations 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 and users are communicating with one another while enabling agencies to meet their own governance, security, and compliance requirements.

Certes Observability 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, all the while monitoring pathways for potential threats because each policy is observable in real-time.

RESULT

By implementing Certes Networks security solutions we help state government 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 package.

Moving forward, Crypto-Segmentation™ is a capability that will improve the security posture of cloud infrastructures, including private, public and hybrid environments. Governments can achieve positive outcomes by comparing their data protection and infrastructure requirements against their security and compliance requirements and gain the added confidence that both are possible.

[1] Hide and Seek – Cybersecurity and the Cloud, Vanson Bourne, 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.