NIST Zero Trust Architecture and Certes Networks Zero Trust Platform

Introduction

The US National Institute of Standards and Technology's (NIST) recent Special Publication (SP 800-207) has changed the table stakes when it comes to cybersecurity best practice. While its traditional role in enhancing economic security cannot be under-estimated, following President Biden's recent cybersecurity executive order, federal agencies must now adopt its refined concept of Zero Trust as well as its standardised approach to a Zero Trust Architecture. State government is expected to follow suit.

Certes Networks' solutions can help organizations meet several requirements of NIST's Zero Trust Architecture Publication (SP 800-207). This White Paper sets out how Certes Networks' solutions, through Policy Definition, Micro-segmentation and Observability, enable organizations to meet each of the tenets of Zero Trust set out in SP 800-207.

Certes Networks enables organizations to secure data in transit, across any network, with zero impact to performance, scalability or operational visibility. From working with large Government agencies to small enterprises operating in regulated industries, Certes helps organizations secure their sensitive data in a way that is completely independent of the underlying network infrastructure with its patented Layer-4 encryption solution. Decoupling security from network hardware in this way is a unique approach and enables security teams to be confident that their organization's data is assured, regardless of what is happening to the network and where their data is.

Tenets of Zero Trust Architecture

Each of the numbered entries below is a direct extract from NIST Special Publication 800-207, followed by a Certes solution brief specific to that individual core tenet.

1. All data sources and computing services are considered resources. A network may be composed of multiple classes of devices.

Certes Networks provides a transparent overlay regardless of underlying network or transport infrastructure that encrypts, drops or sends in the clear, data traversing between Policy Enforcement Points regardless of the class of device or location.

2. All communication is secured regardless of network location. Trust should not be automatically granted based on the device being on enterprise network infrastructure. All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide authentication.

Certes Networks' platform provides the capability to micro-segment your network by creating granular polices to match business intent. Our patented Layer-4 solution encrypts the payload only, leaving the headers in the clear. This gives organizations the ability to create business intent policies and create crypto-segmented networks. Access to resources is not inherently granted based upon location or other inherent factors. All packets traversing between Certes' Policy Enforcement Points (CEP's) are fully protected via authentication, authorization and encryption. The approach stops lateral movement across the network.

3. Access to individual enterprise resources is granted on a per-session basis. Authentication and authorization to one resource will not automatically grant access to a different resource.

On a network level and by creating fine grain policies, Certes Networks' platform grants access to individual resources on a per packet basis only allowing access to the resources required. Authentication and authorization is also done at a per packet level. At the user level, we seamlessly integrate with any authentication software or tools an organization deploys.

4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. Requesting asset state can include device characteristics such as software versions installed, network location, time/date of request, previously observed behavior, and installed credentials.

Certes Networks helps organizations or third-party services to achieve this by programming our REST API to proactively enforce a policy decision based upon various data. Additionally, our platform can contribute additional data to the 3rd party service in order to make better overall cyber security decisions.

5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.

No asset is inherently trusted. The enterprise evaluates the security posture of the asset when evaluating a resource request. An enterprise implementing a ZTA should establish a continuous diagnostics and mitigation (CDM) or similar system to monitor the state of devices and applications and should apply patches/fixes as needed. As a transparent overlay that does not interfere with the existing security stack, Certes Networks can integrate with a CDM System by using our REST API to create dynamic policies to block assets, services, or users that are not in compliance.

6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed. This is a constant cycle of obtaining access, scanning and assessing threats, adapting, and continually reevaluating trust in ongoing communication. An enterprise implementing a ZTA would be expected to have Identity, Credential, and Access Management (ICAM) and asset management systems in place. This includes the use of multifactor authentication (MFA) for access to some or all enterprise resources. Continual monitoring with possible reauthentication and reauthorization occurs throughout user transactions, as defined and enforced by policy (e.g., time-based, new resource requested, resource modification, anomalous subject activity detected) that strives to achieve a balance of security, availability, usability, and cost-efficiency.

Certes Networks interoperates with existing security stacks such as enterprise Identity and Access Management (IAM) tools to authenticate users to allow for basic network access. Once user access is established, all resources can only be reached by traversing between Certes' Policy Enforcement Points (CEPs) where each policy workflow is encrypted separately from one another. Every packet is authorized and authenticated to ensure a bad actor has not breached the data.

7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. An enterprise should collect data about asset security posture, network traffic and access requests, process that data, and use any insight gained to improve policy creation and enforcement.

Certes Enforcement Points sit in line and therefore allow an enterprise to collect data based upon packet header information that allows for granular enforcement of security policies. All packet header information is collected and therefore allows for full visibility and observability. Certes Network Visibility and Observability tools are the linchpins that provide 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.

Logical Components of a Zero Trust Architecture

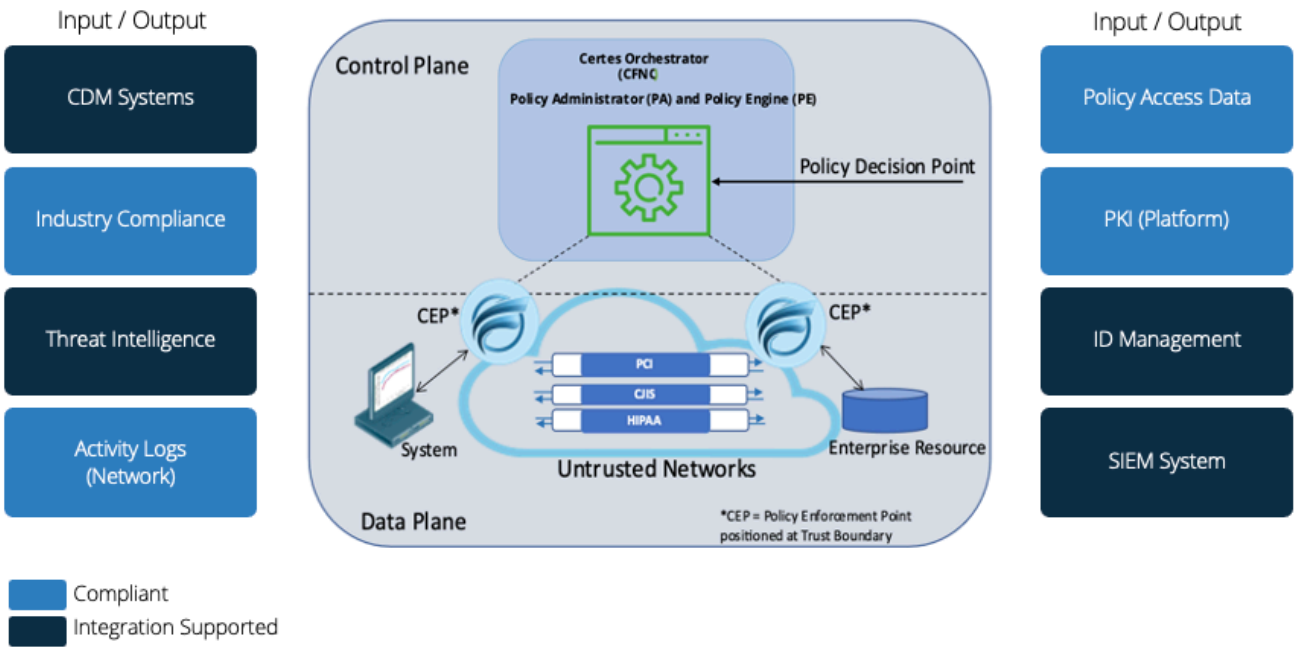
Each of the Components below is a direct extract from NIST Special Publication 800-207, followed by a Certes solution brief specific to that Component.

Policy Engine (PE):
This component is responsible for the ultimate decision to grant access to a resource for a given subject. The PE uses enterprise policy as well as input from external sources (e.g., CDM systems, threat intelligence services described below) as input to a trust algorithm to grant, deny, or revoke access to the resource. The policy engine makes and logs the decision (as approved, or denied), and the policy administrator executes the decision.

Policy Administrator (PA):
This component is responsible for establishing and/or shutting down the communication path between a subject and a resource (via commands to relevant PEPs). It would generate any session-specific authentication and authentication token or credential used by a client to access an enterprise resource. It is closely tied to the PE and relies on its decision to ultimately allow or deny a session

Policy Enforcement Point (PEP):
This system is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The PEP communicates with the PA to forward requests and/or receive policy updates from the PA.

The components of a Certes Networks deployment match NIST's vision of what an organization must deploy to achieve Zero Trust. Certes' CFNC or policy engine (PE) and policy administrator (PA) provide the interface for managing policies, granting, denying or revoking access to a resource that is located behind the Policy Enforcement Point (CEP). The CFNC is also responsible for establishing and/or shutting down a communication path via commands to PEPs (CEPS). It also generates any session-specific authentication credentials. CEPs are PEPs that are responsible for enabling, monitoring, terminating connections creating a trusted zone. All communications between CFNC and CEPS (aka. PE, PA, PEP) are done in the secure control plane.



In addition to the core components of enterprise ZTA, several data sources provide input and policy rules used by the policy engine when making access decisions. These include local data sources as well as external (i.e., non-enterprise-controlled or -created) data sources. These can include:

Continuous diagnostics and mitigation (CDM) system: This gathers information about the enterprise asset's current state and applies updates to configuration and software components. An enterprise CDM system provides the policy engine with the information about the asset making an access request, such as whether it is running the appropriate patched operating system (OS), the integrity of enterprise-approved software components or presence of non-approved components and whether the asset has any known vulnerabilities. CDM systems are also responsible for identifying and potentially enforcing a subset of polices on non-enterprise devices active on enterprise infrastructure.

Certes Networks is fully compatible with CDM tools by utilizing our REST API to create dynamic policy to block assets, services, or users that are not in compliance.

Industry compliance system: This ensures that the enterprise remains compliant with any regulatory regime that it may fall under (e.g., FISMA, healthcare or financial industry information security requirements). This includes all the policy rules that an enterprise develops to ensure compliance.

In implementing Certes Networks' solutions, an organization can easily segment their network by implementing business intent granular policies. Each policy workflow has its own set of encryption keys creating crypto-segmentation at the policy workflow level. This stops lateral movement within the network, therefore reducing the attack surface. Our powerful auditing and logging make it easy to demonstrate compliance with security mandates, such as HIPAA, CJIS, and other PII legislation. Certes Networks' platform is both FIPS 140-2 and Common Criteria Certified.

Threat intelligence feed(s): This provides information from internal or external sources that help the policy engine make access decisions. These could be multiple services that take data from internal and/or multiple external sources and provide information about newly discovered attacks or vulnerabilities. This also includes newly discovered flaws in software, newly identified malware, and reported attacks to other assets that the policy engine will want to deny access to from enterprise assets.

Our platform can provide metadata that contains detailed information related to every packet traversing between CEPs. This information can be integrated into any third-party analytic tools such as SIEM, ML, AI, etc. and used to discover malware, vulnerabilities, or attacks as an example. external sources such as analytic tools, SIEM, ML and AI and used to identify vulnerabilities, malware on any IP traffic traversing the network and between CEPs (PEPs).

Network and system activity logs: This enterprise system aggregates asset logs, network traffic, resource access actions, and other events that provide real-time (or near-real-time) feedback on the security posture of enterprise information systems.

CEP (PEP) logs keep track of network messages and events generated by various processes, such as encryption, certificates, rekeys, and SNMP. The logging information can be viewed via the CFNC (PE and PA) or can be integrated into an organization's current logging infrastructure. In addition, all network activity, network security data (Discards, Policy Action, and systems activity of admin users which is in IPFIX standard format can be sent to our Observer for further analyses in real time.

Data Access Policies: These are the attributes, rules, and policies about access to enterprise resources. This set of rules could be encoded in or dynamically generated by the policy engine. These policies are the starting point for authorizing access to a resource as they provide the basic access privileges for accounts and applications/services in the enterprise. These policies should be based on the defined mission roles and needs of an organization.

Certes Networks enables business intent micro-segmentation by allowing for granular policy creation and enforcement at the workflow level. Each policy workflow can either be encrypted, discarded or sent in the clear. This removes the implicit trust of any resource, application or asset protected by the Policy Enforcement Point. These policies can be defined based upon the roles or needs of an organization. Enabling crypto-segmentation prevents the lateral movement within the network between policy and workflows.

Enterprise public key infrastructure (PKI): This system is responsible for generating and logging certificates issued by the enterprise to resources, subjects, services and applications. This also includes the global certificate authority ecosystem and the Federal PKI,4 which may or may not be integrated with the enterprise PKI. This could also be a PKI that is not built upon X.509 certificates.

Certes Networks' platform provides a built in PKI system for securing the identity of all of the components of its platform. Support for external Certificate of Authority (CA) is fully supported if a customer prefers to utilize an existing certificate. We can support external CAs that the customer may already have in place.

ID management system: This is responsible for creating, storing, and managing enterprise user accounts and identity records (e.g., lightweight directory access protocol (LDAP) server). This system contains the necessary subject information (e.g., name, email address, certificates) and other enterprise characteristics such as role, access attributes, and assigned assets...

This system often utilizes other systems (such as a PKI) for artifacts associated with user accounts. This system may be part of a larger federated community and may include non-enterprise employees or links to non-enterprise assets for collaboration.

In implementing a Zero Trust Architecture, a multi-dimensional approach may be required. Certes Networks interoperates with the existing security stack and strongly suggests an enterprise level user authentication tool such as LDAP or others to manage user and identity accounts. A layered approach to ZTA will enhance the strict separation of duties required to ensure the security posture of an organization at both the data and network security level.

Security information and event management (SIEM) system: This collects security-centric information for later analysis. This data is then used to refine policies and warn of possible attacks against enterprise assets.

Certes' patented solution of encrypting the payload only, leaving the headers in the clear, provides full visibility and observability of data traversing the network. Utilizing the NetFlow protocol IPFIX, the metadata generated by the CEP's can be used to generate real-time visuals through our observability feature as well as integrate into SIEM or other analytic tools. This will allow a customer to make informed decisions based upon real time data that will ultimately allow them to meet their required security posture.

Network Requirements to Support ZTA

Each of the numbered Requirements below is a direct extract from NIST Special Publication 800-207, followed by a Certes solution brief specific to that Requirement.

1. Enterprise assets have basic network connectivity. The local area network (LAN), enterprise controlled or not, provides basic routing and infrastructure (e.g., DNS). The remote enterprise asset may not necessarily use all infrastructure services.

Certes Networks is a transparent overlay supporting any underlying IP transport or hardware infrastructure. The components of our solution sit in line on the network and perform no routing or switching. Each packet header is processed to determine if there is a policy match and the packet is either encrypted, discarded, or sent in the clear. Polices are created and managed utilizing the CFNC, a single pane of glass that acts as the policy engine and policy administrator. The CFNC is an orchestrator that generates the key material and communicates via the control plane to all policy enforcement points (CEPs).

2. The enterprise must be able to distinguish between what assets are owned or managed by the enterprise and the devices' current security posture. This is determined by enterprise-issued credentials and not using information that cannot be authenticated information (e.g., network MAC addresses that can be spoofed).

In implementing a Zero Trust Architecture, a multi-dimensional approach may be required. Certes Networks interoperates with existing security stack such as enterprise Identity and Access Management (IAM) tools and strongly recommends using Multi-Factor Authentication (MFA) to authenticate users to allow for basic network access. Once user access is established, all resources can only be reached by traversing between Policy Enforcement Points (CEPs) where each policy workflow is encrypted separately from one another. Every packet is authorized and authenticated to ensure a bad actor has not breached the data.

3. The enterprise can observe all network traffic. The enterprise records packets seen on the data plane, even if it is not be able to perform application layer inspection (i.e., OSI layer 7) on all packets. The enterprise filters out metadata about the connection (e.g., destination, time, device identity) to dynamically update policies and inform the PE as it evaluates access requests.

Our Policy Enforcement Points (CEPs) sit in line on the network processing each packet header to determine how the enterprise wants the packet to be treated (Encrypt, Drop, Clear). The collected Metadata provides end-to-end visibility and observability and allows an organization to make informed business decisions that will ultimately meet the security posture required.

- Other capabilities of Certes Visibility and Observability Feature:
- Packet capture for troubleshooting and advanced anomaly detection.
- Global view and correlation of data from all Certes Enforcement Points
- Rich context provided based on the metadata exported
- Visual proof of the efficacy enforced by CryptoFlow solution security posture
- Audit your network to see what applications are active and who is accessing them
- Rich reporting to management, complete with graphs and dashboards for compliance assurance.

4. Enterprise resources should not be reachable without accessing a PEP. Enterprise resources do not accept arbitrary incoming connections from the internet. Resources accept custom-configured connections only after a client has been authenticated and authorized. These communication paths are set up by the PEP. Resources may not even be discoverable without accessing a PEP. This prevents attackers from identifying targets via scanning and/or launching DoS attacks against resources located behind PEPs.

Certes' Policy Enforcement Points (CEPs) are deployed at an organization's various trust boundaries. An example of these boundaries would be edge of WAN, top of rack or in front of a host. All communications between the CEP's are strictly authenticated and authorized and either dropped, sent in clear or encrypted at the policy workflow level. Certes' patented solution allows for creation of policies based upon the OSI Model Layer 2, 3, 4 headers. Policies can be created based upon a combination of selectors such as Protocol, Port, Location, IP Address, Application, etc.

5. The data plane and control plane are logically separate. The policy engine, policy administrator, and PEPs communicate on a network that is logically separate and not directly accessible by enterprise assets and resources. The data plane is used for application/service data traffic. The policy engine, policy administrator, and PEPs use the control plane to communicate and manage communication paths between assets. The PEPs must be able to send and receive messages from both the data and control planes.

Certes uses separate management (control) and data planes. OpenSSL (TLS) is used to encrypt management traffic over the management plane between CFNC (PA and PE) and the CEPs (PEPs). The TLS protocol allows secure communication between the devices in the system, while providing information about the secure stream to CFNC. The CEPs can send and receive messages on both the data and management (control) planes. The actual encryption of the information takes place on the data plane.

6. Enterprise assets can reach the PEP component. Enterprise subjects must be able to access the PEP component to gain access to resources. This could take the form of a web portal, network device, or software agent on the enterprise asset that enables the connection.

Certes Networks' Policy Enforcement Points (CEPs) have flexible deployment options that are dependent upon an organization's requirements. As a software company, whether the PEP's are deployed physically, virtualized, as a NVF, or any combination, bit for bit the software and capabilities are identical.

7. The PEP is the only component that accesses the policy administrator as part of a business flow. Each PEP operating on the enterprise network has a connection to the policy administrator to establish communication paths from clients to resources. All enterprise business process traffic passes through one or more PEPs.

Only the components of the Certes Networks' platform - the CFNC (policy administrator) and CEPs (PEPs) - can establish communications paths between one another. This is done via a secure TLS connection via the management (control) plane.

8. Remote enterprise assets should be able to access enterprise resources without needing to traverse enterprise network infrastructure first. For example, a remote subject should not be required to use a link back to the enterprise network (i.e., virtual private network [VPN]) to access services utilized by the enterprise and hosted by a public cloud provider (e.g., email).

Certes Networks is fully flexible and transparent overlay supporting any deployment for remote users to access cloud resources.

9. The infrastructure used to support the ZTA access decision process should be made scalable to account for changes in process load. The PE(s), PA(s), and PEPs used in a ZTA become the key components in any business process. Delay or inability to reach a PEP (or inability of the PEPs to reach the PA/PE) negatively impacts the ability to perform the workflow. An enterprise implementing a ZTA needs to provision the components for the expected workload or be able to rapidly scale the infrastructure to handle increased usage when needed.

Our platform is designed from the ground up to be a simple and scalable transparent overlay, providing an end-to-end encryption solution that is network agnostic. The solution is fully scalable and runs almost at wire speed. It easily integrates into any network infrastructure, is fully interoperable with the existing security stack and with zero impact to performance. Adding additional PEPs and pushing policies to them can be done within minutes. Also, PEPs (CEPs) and PA (CFNC) can be deployed redundantly and run in active/active mode for resiliency.

10. Enterprise assets may not be able to reach certain PEPs due to policy or observable factors. For example, there may be a policy stating that mobile assets may not be able to reach certain resources if the requesting asset is located outside of the enterprise's home country. These factors could be based on location (geolocation or network location), device type, or other criteria.

The ability to create policies, not only to encrypt the workflow at a granular level but to drop traffic based upon certain considerations, is fully supported. Asset requests can be discarded based upon selectors such as Protocol, Port, Location, IP address, Application, etc.

In summary, Certes Networks Zero Trust Architecture is fully aligned with NIST's vision of protecting an organization's most valuable asset, its data. Certes Networks provides encryption of the packet payload only leaving the headers in the clear that allows for granular policy creation as well as encryption key generation and automatic rotation per policy. As it is a transparent overlay, it is network and transport agnostic and easily integrates into any infrastructure at top of rack or edge of WAN, physically or virtually.

In Conclusion

The technology is fully interoperable with the existing security stack. No changes to routers, switches or firewalls are required. The platform is fully managed via a web-based, single pane of glass that provides the interface for creating and implementing policies as well as generating the key material for encryption. Using the Certes metadata, an organization can create real-time customized reports detailing their security posture as well as identify out of policy traffic. These reports can be utilized for audits or any other organizational requirements. The metadata also integrates with other 3rd party analytic, AI and SIEM Tools.

Certes Networks Key Differentiators

- Significantly simplifying the provisioning and deployment of end-to-end encryption.
- Reducing the attack surface and the ability for threats to move laterally using Crypto Segmentation with automated key generation and rotation in quantum physics
- Patented and undetectable Layer 4 encryption that preserves critical networking headers so that network devices and troubleshooting tools can perform effectively
- Customer has full control and exclusive ownership of the encryption keys and policies.
- End-to-end security de-coupled from the network infrastructure
- Easy to install, setup and manage, Zero Touch & Zero Impact.
- Single Point of Management and Enforcement (Crypto Flow Net Creator CFNC)
- Certes Observability providing a visual proof that your security strategy is working

CERTES NETWORKS

Contact Certes Networks
300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

Tel: 1 (888) 833-1142
www.certesnetworks.com
sales@certesnetworks.com