portnox™

Portnox CLEAR Security Architecture and Principles

August 3, 2017

Introduction

Portnox CLEAR enables IT security personnel to discover, monitor and manage endpoint security postures, threats and vulnerabilities, and to make real-time access decisions (Network and Cloud), based on the determined endpoint risk.

CLEAR risk assessment is built as an ongoing, continuous process of collecting and analyzing hundreds of different end-point parameters and activities, which are used to determine an endpoint risk score.

To provide these capabilities, CLEAR accesses, collects, and stores data from organizational devices that are enrolled in the CLEAR system. Data is an organization's most valuable and irreplaceable asset and as such, Portnox CLEAR utilizes the most advanced security measures available on the market.

In this document, we describe in depth Portnox CLEAR's security principles as they apply to every layer of the Portnox CLEAR architecture:

- **Data at Rest** – Describes how Portnox CLEAR uses highly secure, encrypted Azure Storage to store customer data.
- **Data in Transit (Motion)** – Describes the data and privacy protection measures employed when data travels from the CLEAR Agent, CLEAR AD Broker, Wireless controllers, Ethernet switches, VPN Gateways and admin browsers to and from the CLEAR services in the Azure Public Cloud and back.
- **CLEAR Administrator Access and Role Management** – Describes the identity and authorization model used for administrators accessing the CLEAR Portal.
- **Cloud Service Security** – Describes the security measures that protect the CLEAR cloud services.

Data at Rest

Cryptographic protection of data in the cloud

Portnox CLEAR stores all of its customers' data on the Azure Storage Service in various formats (Big Data model). Azure storage is known as a highly secure data storage because it implements strong (256-bit AES) encryption for stored data, also known as Azure Storage Service Encryption (SSE). Portnox CLEAR utilizes SSE to protect and safeguard customers' data to meet customers' security and compliance commitments. All collected data is automatically encrypted prior to persisting to storage, and decrypted prior to retrieval.

For highly sensitive data, such as CLEAR administrator passwords, RADIUS pre-shared keys, and encryption keys, CLEAR uses Azure Key Vault.

With Azure Key Vault, keys are stored in Hardware Security Modules (HSMs). For added assurance, keys are also generated in HSMs. Keys are protected in FIPS 140-2 Level 2 validated HSMs (hardware and firmware). The Azure Key Vault is designed so that no one, even Microsoft, can see or extract the stored secrets.

Data engineering security principles in Portnox CLEAR

- Portnox CLEAR AgentP never saves any collected data locally (on the endpoint device). All collected data is processed and resides only in the endpoint device RAM and is sent immediately / periodically to the CLEAR cloud service, which is saved in CLEAR storage in the cloud.
- Data is always stored separately from data identifications, so based on the stored data it is impossible to identify to which organization or device owner the data belongs.
- CLEAR never collects any PII information to protect customer privacy.

Data in Transit

Portnox CLEAR protects all data traveling from various CLEAR components to and from the CLEAR cloud services, based on the following security principles:

- Data sent by any CLEAR component, on all platforms, is always sent using the industry-standard secure transport protocol called Transport Layer Security (TLS) and is therefore always encrypted in transit. Client-to-Cloud applications use the TLS protocol to communicate across a network in a way designed to prevent eavesdropping and tampering. The protocol uses a handshake with an asymmetric cipher to establish cipher settings and a shared key for a session; the rest of the communication is encrypted using a symmetric cipher and the session key.
- CLEAR services use an authorization model for allowing any access, data extraction, or data submission from any CLEAR or third-party components (API calls). The authorization model is based on periodically rotated API Tokens that are presented by the service caller in any request. There are no anonymous calls, session management, "trusted IP" caches or any other well-known techniques that jeopardize data-in-motion security; and any data submission or fetching request from CLEAR components is re-authenticated and authorized anew.

Portnox CLEAR AD Broker

The Portnox Active Directory (AD) Broker is a software application that runs on-premises on the customer network, and acts as a mediator between the Portnox CLEAR cloud services and the customer's corporate Active Directory.

Since Active Directory users and groups are among an organization's most valuable information, extra security measures are taken to safeguard that information:

- The CLEAR AD Broker must be installed on a Domain member server, Windows 2008 server and above (it can also be installed on the AD Domain controller).
- The CLEAR AD Broker connects to the AD Domain controller with a domain account that has read-only access on the organizational Active Directory.
- The CLEAR AD Broker can connect to the organizational Active Directory using the LDAP or SLDAP (Secure LDAP) protocols, according to the customer's preference.

- The CLEAR AD Broker connects to the CLEAR cloud service using the outbound TCP ports 8081 and 443. Cloud traffic is always initiated by the CLEAR AD Broker.
- The CLEAR AD Broker communicates with the CLEAR cloud services over TLS. All traffic between the CLEAR AD Broker and the CLEAR cloud services is encrypted.
- The CLEAR AD Broker updates the CLEAR cloud service *only* with AD users and groups. Even so, the CLEAR AD Broker never handles user passwords. User authentication is performed by utilizing the MS-CHAP-V2 challenge/response protocol so the password never travels within the TLS encrypted tunnels, only the challenge/response hashes do.

Wireless controllers and Ethernet switches

Wireless controllers and Ethernet switches send RADIUS authentication requests to the Portnox CLEAR RADIUS server, to perform validation and allow access of endpoint devices with the CLEAR agent installed or agentless devices. The following security measurements are taken to ensure secure communication between the organizational network equipment and CLEAR RADIUS in the cloud:

- All communications are always carried out over TLS and are encrypted at the transport level to protect traffic privacy and prevent man-in-the-middle attacks.
- All communication messages inside a TLS tunnel are also encrypted by a dedicated per-organization Shared Secret Key which validates that the message was not tampered with in transport, and only the trusted CLEAR RADUIS can open these messages.
- In the case of an EAP_PEAP authentication model, the end-user credentials never travel across networks. Instead, only the challenge/response hashes travel, enabling CLEAR to reliably validate user credentials without knowing them, by using the organization's authentication repository.

Portnox CLEAR guest management for wireless networks

With Portnox's CLEAR guest management for wireless networks, CLEAR uses the built-in captive portal capabilities of each supported wireless controller vendor.

CLEAR replaces the following vendor-specific components as follows:

- Replaces the original vendor captive portal web page with the CLEAR cloud webpages
- Replaces the AAA server with the CLEAR cloud RADIUS
- Replaces the user repository with the CLEAR Guest Management repository

The Portnox CLEAR Captive Portal can be accessed only via HTTPS/SSL, unlike some vendor solutions that allow plain unencrypted HTTP access.

Guest credentials are sent to the wireless controller using SSL. The controller then authenticates them against the Portnox CLEAR cloud RADIUS using the Challenge-Handshake Authentication Protocol (CHAP) over a TLS encrypted tunnel.

With this architecture, traffic between the wireless controller and the Portnox CLEAR cloud RADIUS is encrypted using TLS; in addition, passwords are never sent inside the tunnel; instead, authentication is done using challenge/response hash interchanges.

Note that some wireless controller vendors do not support CHAP authentication when using their captive portal infrastructure. In those cases, CLEAR uses PAP authentication with a TLS encrypted tunnel between the wireless controller and the CLEAR cloud RADIUS.

VPN Gateways

Portnox CLEAR can be used to authenticate VPN users using two-factor authentication, with the second factor being a strong factor. Portnox CLEAR can also add an additional layer of security for users connecting remotely via VPN with the VPN Gateway using the CLEAR cloud RADIUS service as an authentication authority.

The connection security type, tunnel encryption and challenge/response protocol are **determined exclusively** by the VPN terminator itself.

The Portnox CLEAR cloud RADIUS service supports the highest and strongest secure connection type available today by VPN terminators vendors: TLS tunnel, MS-CHAP-V2, CHAP and even (unsecure) PAP.

Portnox CLEAR Administrators - Securing Privileged Accounts

The process of securing privileged accounts should be on-going, with continuous evaluation and adjustments to improve security as the business and threat landscape change.

Portnox CLEAR utilizes the following methods to secure privileged admin accounts and to minimize exposure to these kinds of attacks:

- CLEAR enables configuration of two-factor authentication (code sent in a text message to a pre- registered number) for any administrator to use as an additional strong factor in admin access authorization.
- The failed authentication attempts policy starts with showing a CAPTCHA after a few failed attempts and progresses to locking the account after a number of subsequent failures.
- Admin password complexity enforcement is built into the product and cannot be turned off.
- The admin password expiration policy is built into the product and cannot be turned off.
- Granular admin role management allows assigning a superset of permissions to each CLEAR administrator.

Cloud Service Platform Security and Protection

Portnox CLEAR utilizes Microsoft Azure as its Public Cloud provider. One of the key factors in choosing Azure was its approach, implementation and integration of all security aspects and measures at all platform levels.

Security and privacy are built into the Azure platform, beginning with the Security Development Lifecycle (SDL). The SDL addresses security at every development phase, from initial planning to launch, and ensures that Azure is continually updated to make it even more secure. Operational Security Assurance (OSA) builds on SDL knowledge and processes to provide a framework that helps ensure secure operations throughout the lifecycle of cloud-based services.

The Azure Security Center makes Azure the only public cloud platform to offer continuous security-health monitoring.

For detailed information about Azure Security, visit https://www.microsoft.com/en-us/trustcenter/security/azure-security.

In addition to inherited environmental security, Portnox CLEAR takes the following measures to ensure security of cloud services:

- Portnox conducts periodical Penetration Tests with a third party that specializes in security testing of cloud services.
- Portnox's development team uses an automated code scanning tool to identify vulnerabilities in code, third party components that are not up-to-date, and other security issues.
- The Portnox DevOps procedure ensures the periodic rotation of all relevant credentials and secrets, including TLS and encryption certificates rotation, as well as the secret keys and passwords used by the system and supporting personnel.