Pulse Secure®

Pulse Zero Trust Access (PZTA)

Defense-In-Depth for Easy, Direct, Anywhere Access to Multi-Cloud and Data Center Applications with Zero Trust Assurance

WHITE PAPER

www.pulsesecure.net

Table of Contents

Table of Contents

Pulse Zero Trust Access

This document is for CxOs, network architects, security teams and cloud teams, and others who want an understanding of the Zero Trust architecture of Pulse Zero Trust Access (PZTA). When considering a cloud-based solution, organizations often ask "If we let our data reside outside our data centers, how secure is it?"

This document discusses the security posture of PZTA in detail, laying out the Defense-in-Depth (DiD) approach, leveraged to ensure security, reliability, scalability, and availability.

Executive Summary

Pulse Zero Trust Access is a hosted service that eliminates the distinction of being inside or outside of a corporate network, treating every instance of user access with zero trust until their security posture—which includes user identity, device identity and device posture—is verified.

The security architecture and posture of Pulse Zero Trust Access (PZTA) solution is critical to providing confidence to enterprise IT security and risk leaders onboarding it in their enterprise environments. It facilitates secure access to their most valuable assets -- applications and data -- across multiple cloud environments and data centers. Naturally, when it comes to cloud-based services, security is a key consideration.

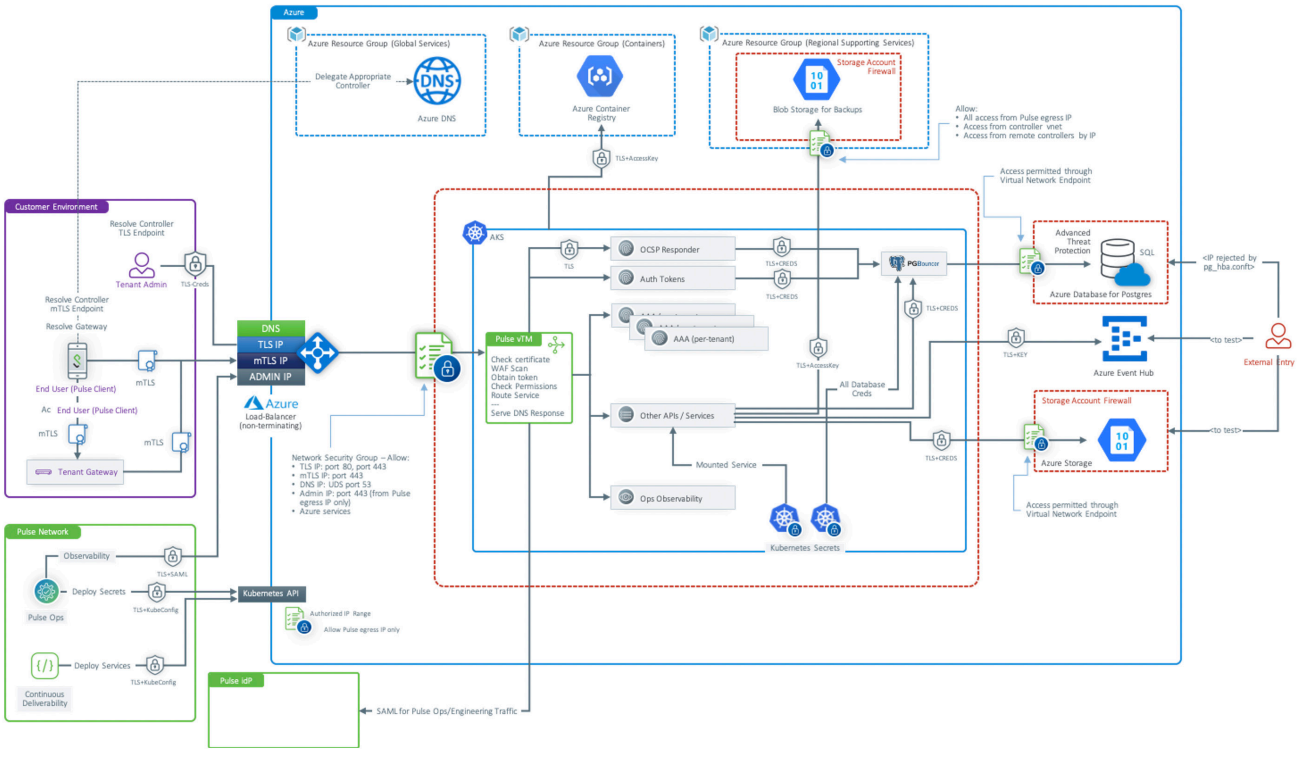


Figure 1. Pulse Secure Zero Trust Architecture Defense-in-Depth diagram

Cloud Infrastructure Security

Pulse Secure operates the PZTA service in the Pulse Secure cloud. The Pulse Secure cloud is a Platform-as-a-Service (PaaS) that runs on Microsoft Azure Cloud.

Azure Cloud Security Standards

The Pulse Secure Zero Trust Access cloud platform inherits the underlying security and standards of the cloud service provider. For more information, please see Microsoft's Azure Cloud security standards.[1]

Azure Cloud Compliance

Azure Cloud is compliant with numerous standards such as ISO 27001, ISO 9001, SOC, PCI Data Security Standard, and the US Government's Federal Risk and Authorization Management Program (FedRAMP). For more information, see Microsoft's Azure Audit Reports.[2]

Note: While Azure conforms to the stated standards, PZTA as-a-service is pending certification to these standards.

Azure Load Balancer Service

Each availability zone is provisioned with multiple load balancers for performance and availability. The load balancers automatically ensure that traffic is directed to healthy servers, spreading the load across servers in all three availability zones.

PZTA uses Mutual TLS End Points for establishing trust with both Pulse Secure's single, unified clients and Pulse gateways which are terminated at the Redundant Load Balancers deployed within the Kubernetes Clusters. These load balancers are also front-ended by Azure Load Balancers which expose Public IP Addresses for communication with the external end points. These exposed Public IP adresses are protected, as mentioned, in the above section using Azure DDoS Protection.

Azure VNET

The PZTA cloud-hosted service is isolated and protected from external access using a Virtual Private Network (Azure VNET). Strict security and network access controls restrict the traffic that can enter and leave Azure VNET as well as who can access the Azure VNET for operational reasons.

Azure DDoS Service

The Pulse Zero Trust Access Solution running in Azure takes advantage of Azure DDoS Protection Standard Service to protect itself against common Layer 3 and Layer 4 Network Attacks such as TCP SYN Flood Attacks. It's automatically tuned to protect specific Azure resources in a virtual network such as Azure Public IP addresses that are exposed via Azure Load Balancer & Azure DNS.

Network Security Groups

Network Security Groups are used to block internet-based attacks and maintain high availability for the public-facing web application and API web service endpoints. Customers are not required to open any special ports on their firewall. All traffic from on-premises gateways and browsers is outbound-initiated on the standard HTTPS port 443. The cloud service will not be able to directly reach into a customers' data center. See the 'Encryption of Data in Transit' section for more details on the encryption of data sent between the cloud and on-premise gateways and browsers.

[1]https://azure.microsoft.com/en-us/overview/trusted-cloud/
[2]https://servicetrust.microsoft.com/Documents/ComplianceReports

Pulse Virtual Traffic Manager

Pulse Secure's Virtual Traffic Manager features high-performance load balancing and application delivery. Application delivery controllers (ADCs) are a critical part of modern enterprise applications -- they improve load-balancing, reliability, availability, and security. With unmatched scalability and performance, unique customization and fine-grained control of users and services, Pulse Virtual Traffic Manager is a network traffic manager purpose-built for the most demanding virtual and cloud application environments.

Pulse Web Application Firewall

Regarding resource attacks at the application layer, the Pulse Zero Trust Access Solution uses a Web Application Firewall (WAF) to help secure web resources/APIs that are part of the Pulse Zero Trust Access Solution. The WAF inspects inbound web traffic to block SQL injections, cross-site scripting, DDoS, and other Layer 7 attacks. Even web application firewalls are susceptible to volumetric and state exhaustion attacks. To protect against these, the Pulse Zero Trust Access controller has Azure DDoS Protection Standard enabled on the WAF virtual network.

Network ACLs

Azure Managed Postgres Service used by PZTA restricts access to requests originating only from within Pulse Secure Azure Virtual Networks, thereby reducing the attack surface of customer data managed in the Azure Managed Postgres Service.

Azure Advanced Threat Protection Service

Pulse Zero Trust Access Solution makes use of Azure Advanced Threat Protection for Azure Managed Postgres database to detect anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases.

Zero Trust Session Security

Mutual TLS

Mutual TLS (mTLS) is an important step (mandated by Cloud Security Alliance SDP specification), where the ZTA client authenticates to ZTA Controller and ZTA Gateway as well as between the ZTA Gateway and the Controller. By default, the TLS protocol only proves the identity of the server to the client using X.509 certificates and the authentication of the client to the server is left to the application layer.

TLS also offers client-to-server authentication using client-side X.509 authentication – this is mTLS. The following are the benefits of mTLS:

1. Prevent man-in-the-middle (MITM) attacks
2. User, device & machine (ZTA Gateway) authentication and trust
3. Another layer of encryption beyond that which is provided by the application

User Authentication

Please refer to the User Authentication sub-section under Platform Security.

Gateway Authentication (Gateway Trust)

The communication between the ZTA Gateways and the Controller is also protected using mTLS after the initial registration, thereby reducing the attack surface of the controller. This also establishes trust between the Gateway and the Controller and ensures that the Controller APIs that are non-administrative in nature are protected from attacks.

Device Authentication (Device Trust)

Pulse Zero Trust Access allows access to applications only from devices that are enrolled with the ZTA Controller thereby reducing the attack surface on the Controller and the Gateways. When the device is enrolled, the ZTA Controller distributes certificates to the devices signed by a per-tenant intermediate certificate authority (CA), thereby further establishing trust on a per-tenant basis and disallowing leakage of other tenants' devices.

Granular App Access & Session Security

PZTA allows Administrators to configure granular per-application access to end users (irrespective of their location and the device from which they are accessing a given application) only after assessing the environment context and security posture of the user and the device. The context and security posture are assessed continuously, and access to the applications are allowed or denied on a continuous basis throughout the lifecycle of the session.

Platform Security

Operating System Hardening

Pulse Secure's standard Linux server build aligns to industry best practices; only required services are enabled and system hardening measures are applied. Automated configuration enforcement agents ensure continuous baseline compliance.

RBAC

Pulse Zero Trust Access Solution provides pre-defined roles which customers can assign to users of the Pulse ZTA Administration Portal. A user can be assigned one or more of the pre-defined roles.

User Authentication

For application users, PZTA employs a secure, highly available Authentication & Authorization service. When provisioning user access to Pulse Zero Trust Access, customers can choose whether to create and manage users with the Pulse Zero Trust Access as a Local Identity Provider (IDP) or integrate with their own 3rd Party IDPs such as Azure Active Directory, Okta, Ping Identity, or use the option to integrate with their existing installation of Pulse Connection Secure (PCS) as the IDP. Administrators also have the ability to enforce Multi Factor Authentication (MFA) for end users when integrating with an external IDP as long as the external IDP supports MFA.

In future releases of the platform, MFA will be brought in as a secondary authentication mechanism on the platform itself and will also be used for Adaptive Authentication on a per-application basis.

PCS IDP Integration

For existing Pulse Secure customers who have deployed Pulse Connect Secure extensively, PZTA supports Single Sign On (SSO) through federated authentication to PCS using SAML 2.0, thereby allowing customers to leverage their on-premises active directories and other forms of legacy identity management solutions.

3rd Party IDP Integration

PZTA supports Single Sign On (SSO) through federated authentication to other IDPs using SAML 2.0. This enables customers to use their own IDP for user management and authentication. In this mode, the customer manages their user accounts, credentials, and password policies in their own IDP. PZTA then securely brokers the authentication process with the IDP and receives each authenticated user's identity such as their email address. In this mode, role-based access controls are still defined and managed within PZTA.

PZTA as IDP

PZTA user accounts are created and managed through the PZTA Administration Portal. The Pulse Secure IDP provides users the ability to specify and change their own passwords through an email-based password creation and reset workflow. All account passwords must meet the following complexity rules:

- Must be different from the user ID
- Between 8 to 15 characters long
- Contain at least one lower case and one upper case letter
- Contain at least one number

Non-persistent Session Cookies

PZTA uses non-persistent 'session-cookies' that ensure the user is logged out of the application as soon as the session times out, even if they don't select the 'Sign-out' option in the application. This means that when the browser is re-opened, the user must sign in again. The cookie stored in the user's browser contains a signed globally unique (GUID) session identification token that the Pulse Zero Trust Access web server uses to look up the user. This token is included in every request the application makes to the web server.

Certificate Management

Pulse Zero Trust Access platform comes with its own PKI infrastructure to generate certificates both for gateways and end user devices. This approach generates and stores certificates and keys on a per-tenant, per-device, and gateway basis. It also comes with full Certificate Lifecycle Management from generation to revocation and maintains revocation lists. A tenant has two intermediate CA certificates: one CA issues client certs for devices, and one for the gateways. The other CA will issue server certs for gateways. The intermediate CA certificates are generated during tenant on-boarding. In the future, this will be extended to work with 3rd Party PKI infrastructures.

Data Security

Pulse Secure employs a variety of security measures to ensure the security of data in transit and at rest in the cloud platform.

Data Residency

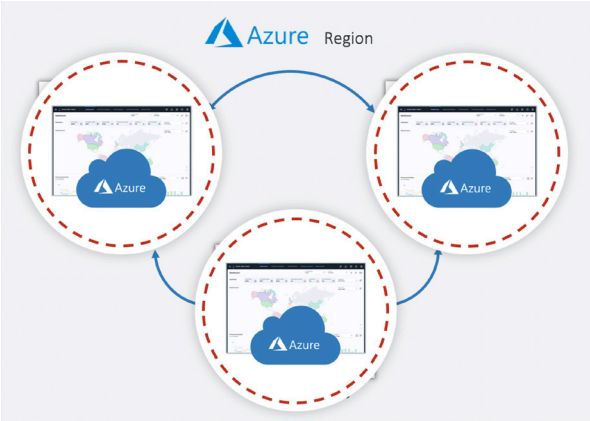
For data residency reasons, the PZTA cloud-hosted service is available in four standalone locations: Netherlands, United States, China, and Japan. Customers choose the location where they would like their data to be stored during the provisioning process. Thereafter, all data is sent to and stored solely in that location; it is not stored or replicated anywhere else. The choice of location makes no difference to where the service can be accessed from; all four locations are globally accessible.

GDPR/CCPA Compliance

PZTA is GDPR/CCPA compliant from a data perspective, offering provisions for customers who request Audit Reports on how their data is being used.

Data Center Redundancy

Pulse Zero Trust Access service is deployed across three availability zones within each location. An Availability Zone is a logical data center, composed of physical data centers, each with their own redundant power, cooling and networking. Availability Zones are in distinct physical locations and engineered to isolate failure from each other so that a local incident does not impact the availability of other zones.



Data Protection & Availability

Customer data is protected and made highly available using industry standard protocols such as application consistent snapshots, disk snapshots, and managed services backup, so that it is available and protected even in the event of another zone becoming unavailable.

Encryption of Data in Transit

All data sent to or retrieved from the cloud service is over HTTPS -- encrypted and secured using Transport Layer Security (TLS). This security mechanism covers Pulse Zero Trust Access users interacting with the service through a browser as well as the on-premises agent which uploads metadata and retrieves configuration information. TLS is a standard encryption protocol that provides security for communications sent over private networks and the internet. TLS encryption maintains the integrity and confidentiality of data so that it can't be modified, intercepted, or viewed while in transit. Pulse Zero Trust Access supports only TLS version 1.2, which is the most recently approved version. TLS versions 1.0, 1.1 and SSL are not supported due to known security vulnerabilities.

Encryption of Data at Rest

All customer data in the Pulse Secure cloud is encrypted at rest using Advanced Encryption Standard (AES) encryption. This applies to all customer data whether uploaded, entered via a web application, or generated data such as exports.

Encryption Secrets Management

Pulse Zero Trust Access controller extensively uses Kubernetes Secrets to expose sensitive information to microservices. This reduces the attack surface by not exposing sensitive information as environment variables or configuration files.

Data Isolation – Secure Virtual Domains

The Pulse Zero Trust Access service is a multi-tenant solution that uses application security and logical boundaries to segregate and protect customer data. Data segregation is enforced across multiple layers by using a unique customer ID, logical database partitions, and logical partitions for all other data such as different folders on disk and different buckets within object storage. In order to access data, customer and user IDs are validated to ensure that data is only accessible to that customer and the appropriate users.

Data Deletion – Certificate of Data Destruction

Upon request to terminate the service, the customer's master key will be disabled and, in parallel, all of the customer's data that resides in the cloud platform will be deleted. A "Certificate of Destruction" will then be issued.

Overall Test Strategy

PEN Testing

Pulse Zero Trust Access Solution has extensive pen testing performed by an independent third party entity and has documentation to verify that it doesn't have any major vulnerabilities that can be exploited. Frequent vulnerability scanning and penetration tests help ensure that both internal and external threats are minimized.

Black Duck Scans

There are three different axes of evaluation in Black Duck: licensing risk, security risk, and operational risk. A given component can contribute in all of these dimensions.

Black Duck is configured with a Pulse-defined set of policies which are based around the OSTP approval requirements taking into account the nature of a ZTA SaaS delivery; any component that meets the policy requirements is automatically approved without any user intervention.

These scans are incorporated into continuous integration/continuous delivery (CI/CD) pipelines as well as the introduction of new packages into a microservice or a component such as client and gateway.

Conclusion

Security is not a point-in-time activity but rather a continuous process. Providing a high level of security and privacy protection for Pulse Zero Trust Access customers means that PZTA is continually adjusting the overall security control landscape to minimize risk to the changing business threat environment. PZTA is always re-evaluating individual security measures to ensure controls scale to meet business requirements and to combat a constantly evolving threat landscape.

About Pulse Secure

Pulse Secure, LLC offers software-defined Secure Access solutions that provide visibility and easy, protected connectivity between users, devices, things and services. The company delivers suites and a SaaS platform that uniquely integrate cloud, mobile, application and network access control for hybrid IT. More than 24,000 enterprises and service providers across every vertical rely on Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net.

Corporate and Sales Headquarters
Pulse Secure LLC

2700 Zanker Rd. Suite 200
San Jose, CA 95134

(408) 372-9600

info@pulsesecure.net
www.pulsesecure.net

linkedin.com/company/pulse-secure
www.facebook.com/pulsesecure1
twitter.com/PulseSecure
info@pulsesecure.net