Pulse Zero Trust Access (ZTA) FAQ

July 21, 2020

This document discusses Frequently Asked Questions for Pulse Secure's upcoming ZTA product.

Table of Contents

Overview

What is PZTA?

Pulse Zero Trust Access (PZTA) is a new SaaS-based Zero Trust Secure Access solution from Pulse Secure. PZTA's Access Service is based on Cloud Secure Alliance's SDP model. On top of SDP connectivity, PZTA also includes advanced security and analytics features.

When was PZTA introduced?

PZTA was made generally available July 28, 2020

With PZTA, do I still need other products from Pulse Secure?

That depends. PZTA can be purchased and used separately from other solutions from Pulse Secure. PZTA provides granular per application access to end users irrespective of the location of the end user and the application. For customers with more traditional access needs, PZTA is designed to co-exist with current Pulse Secure products such as, PCS for remote network access and remote clientless application access and PPS for on premises Layer 2 network access control and Layer 3 Enforcement.

With PZTA, can I still use my existing Pulse Secure products?

Yes. PZTA can be complimentary to your existing Pulse Secure deployment. For customers with more traditional access needs, PZTA is designed to co-exist with current Pulse Secure products such as, PCS for remote network access and remote clientless application access and PPS for on premises Layer 2 network access control and Layer 3 Enforcement.

Can I migrate my existing PCS configuration to PZTA?

Some access in your PCS deployment may be migrated to PZTA, but tools for this migration are not available at the time of General Availability on July 28, 2020. For customers that are intending to deploy application-only access, migration tools are planned to help migrating existing PCS configurations.

Can I migrate my existing PCS licenses to PZTA?

No.

Can I demo PZTA at my organization?
Yes. Demos by Pulse Secure and our partners are available. Trial accounts are also available via our TryNow program.

Why is a new Zero Trust Access solution important to Pulse Secure?
Access needs are evolving: At Pulse Secure, we want to ensure that we offer a constantly evolving portfolio that meets the current security needs of our customers as well as future proofs their investments with us. This means extending our heritage into secure access by providing solutions that are not only more secure but also easy to deploy. Moreover, it means providing a solution that can seamless extend your Pulse Secure deployment by quickly integration with what your admins have deployed while making it very easy for your end users to securely access their applications and data without having to learn new access methods. Technology should enable productivity, not hinder it.

Competitors: Competitors are starting from scratch while Pulse Secure is building on our years of expertise in Secure Access. We looked at what the competitors were offering and built something that provides more than their simple connectivity and adds unparalleled value with insightful analytics, automated threat response, and data privacy.

Better security model: The SDP security model works to mitigate the top network-based attacks, such as DDoS, SQL injection, man-in-the-middle (MITM), cross-site scripting (XSS), cross-site request forgery (CSRF), etc. by unauthorized users. Additionally, this approach allows for the separation of control and data plane which essentially makes the solution much more performance oriented.

What's the difference between SDP & Zero Trust?
It's important to keep in mind that Pulse Secure has been providing Zero Trust since our inception. Zero Trust is a security model that embraces a "never trust, always verify". SDP, on the other hand, is a network architecture that requires authentication and authorization before a connection can be made. In effect, SDP is an enhancement of Zero Trust.

Who should consider PZTA?
Hybrid customers with SaaS, Cloud and on-prem applications who prefer to provide granular access based on users, devices and applications.

Deployment options

Does PZTA provide a full layer 3 tunnel?
No. PZTA provides granular application access.

What kinds of applications does PZTA support?
ZTA can support any type of Web/HTTP/HTTPS/TCP based applications, UDP applications will be supported in 2H 2020.

What is Dark Cloud?
SDP, also commonly referred to as "Black Cloud", is a relatively new approach to computer security. It evolved from the work done at the Defense Information Systems Agency (DISA) under the Global Information Grid (GIG) Black Core Network initiative around 2007 and is now growing in popularity.

With this approach, connectivity is based on a need-to-know model, in which device posture and identity are verified before access to application infrastructure is granted. Application infrastructure is effectively "black" (a DoD term meaning the infrastructure cannot be detected) without visible DNS information or IP addresses.

How does PZTA provide dark cloud?
Gateways are protected with mTLS, no connection is accepted by gateway unless is presented with valid mTLS certificate by user.

- Gateways and application servers are not exposed to the end users.
- Users access to Applications on-demand without interacting with client.
- End user portal is dynamically updated with only the applications that user have access to.

Does PZTA use single packet authentication (SPA)?
No, PZTA uses mutual TLS (mTLS) rather than SPA for many reasons.

Why mTLS?

- Well known Crypto Standard
- PKI infrastructure is well managed and supported
- All known platforms have inbuilt x509 certificate management and basis for platform trust verification
- Easy integration possibilities with third-party systems
- Support can be extended to hardware-based keys like smart cards/CAC or any x509 supported systems

Why not SPA?

- SPA requires some type of crypto seed to be induced.
- No standard mechanism to do this
- Makes the enrollment of devices across platforms more difficult
- Browsers do not support it
- A special packet is introduced before sending actual protocol packet
- UDP ports are blocked by default on firewalls, it is hard to know if SPA is handled as there is no response or firewall dropping
- Intermediate devices like firewalls looking into packet headers might need tweaking or special configuration
- Requires accepting TCP connection before sending SPA packets

Does any of my user data go to Pulse Secure's cloud?
No. The PZTA gateways are the only appliances that see user data and those are deployed, maintained, and controlled completely by the customer.

Is Single Sign-On (SSO) supported to Cloud Apps?
Yes, SSO is available via SAML.

Is Single Sign-On (SSO) support to on-prem Apps?
Yes, on-prem apps that support SAML are support. Other forms of SSO, such as form posts, are not available at this time.

How do I import licenses to the PZTA Controller and/or PZTA Gateway?
This is not required as the entitlements are automatically added to tenants.

What's the difference between the Control Plane and the Data Plane?

SDP separates the control of connections from the actual connections used to transfer data.

- The Control Plane governs the authentication and authorization of users, their devices, and whether they're allowed to connect to applications and resources.
- The Data Plane consists of two-way encrypted connections using mutual TLS or another mutual authentication mechanism.

PZTA Controller

Where is the PZTA controller hosted?
The PZTA controller is hosted in three major Azure regions: U.S., Western Europe and APJ (Singapore). We are also planning on adding the China region after General Availability (GA).

Can I deploy the PZTA controller on-prem?
Not at this time. Currently, PZTA controller is only available as a SaaS solution. Our plan is to make PZTA Controller available on-prem after General Availability (GA), possibly as a virtual PZTA controller only.

Is the PZTA controller certified?
Pulse Secure is looking into various compliance options including SOC2, ISO27001 and others.

Can I use a physical PSA for the PZTA controller?
Not at this time. Currently, PZTA controller in our SaaS deployment is only available. Our plan is to make PZTA Controller available on-prem after General Availability (GA), possibly as a virtual PZTA controller only.

How is the PZTA controller secured?
PZTA Controller follows a Defense In-Depth Strategy to secure the Controller and in doing so leverages the following:

- Azure DDoS Protection at the Virtual Network Level
- Mutual TLS end points for communication with the Clients and the Gateways terminated in the Public Virtual Network using Virtual Traffic Manager
- Web Application Firewall for protection against OWASP Top 10 Attacks and HTTP based DDoS
- Advanced Threat Protection enabled at the Data Layer for Postgres DB and also Firewall Rules configured. Communication only allowed from within the Private Virtual Networks.
    - Per Tenant Schemas used for achieving Tenant Level Data Isolation
    - Sensitive Data Encrypted in the Database in addition to Encryption done at the Disk Level
    - Communication over TLS enabled.
- Egress Firewall for communication controls on what services deployed within the Private Virtual network can talk to.

Is the PZTA controller highly available?
Controller clusters are spawns in different Availability Zones (AZ) in Azure. If an AZ goes down, tenants are automatically transferred to other nodes in the same cluster. This process takes only a few minutes.

For extended periods of downtime, a new Controller can be spawn in other Azure Regions.

Are the PZTA log in or landing page customizable?
Not at this time.

How long does the PZTA controller store logs?

Logs are stored for 30 days.

Can I export my logs to other tools like syslog?
Exporting of logs to tools like syslog servers or SIEM is planned for Q3 2020.

PZTA Gateway

Where can I deploy PZTA gateways?
PZTA virtual gateways can be deployed in your datacenter or in your cloud deployments. Virtual gateways are available for VMware ESXi and ….

Is the PZTA gateway certified?
PZTA gateway is a headless gateway and will be certified as a part of the PZTA solution.

Can I log in to the PZTA gateway console or admin UI?
No. PZTA gateways are completely headless and all of the configuration needed to management them is done using the PZTA controller.

Can I use a physical PSA for the PZTA gateway?
Not at this time however, our plan is to make PZTA gateway functionality available on physical PSAs in 1H 2021.

Do the PZTA gateways support redundancy?
Yes. Gateways can be load-balanced in an Active-Active Gateway Group.

PZTA Client

What platforms is the client supported on?
Windows, macOS, iOS, and Android versions are supported at General Availability. Linux client will be supported shortly after.

Where can I install the PZTA client from?
The PZTA Client is the Pulse Client. The Pulse Client for desktops is downloaded during the PZTA enrollment process. The Pulse Client for mobile devices can be downloaded from the respective app stores for Apple and Android.

Is the PZTA client new?
The PTZA Client is an updated version of the Pulse Client. For existing customers, the same upgrade process is used to get you from the existing version of the client to the client that is needed for PZTA support (version X).

Can PZTA use BYO devices?
Yes. An enrolled BYO device can be used.

How do I enroll a PZTA client?
You must first log into the PZTA end user portal to begin the enrollment process. To learn more the enrollment process, see X.

How do I unenroll a PZTA client?
To learn more about the unenrollment process, see X.

Is PZTA client FIPS enabled/certified?
PZTA uses the same unified client as the existing portfolio. FIPS can be enabled on ZTA once the Controller is FIPS certified.

Can I continue to use the Pulse Client for PCS (VPN) and PPS (NAC)?
Yes. The Pulse Client is now a multi-tunnel and multi-mode client which can simultaneously connect to PPS, PCS, and PZTA.

Do I need to configuration many "connections" in the client?
No. A single connection to your PZTA Controller tenant is needed. Once the connection is established, all necessary backend (and hidden from user) connections are established as needed when accessing applications.

Is client customization available at this time?
Basic customization of the client is available. Please refer to the Pulse Client Branding Guide.

Purchasing, packaging, and pricing

How is PZTA licensed?
Named user subscription licenses are sold annually.

How is PZTA packaged?
At GA, PZTA is offered as a single SaaS package with name user based annual subscription. PZTA subscription includes access to the ZTA Controller, ZTA virtual Gateways, ZTA Clients, and Gold support. There is also a platinum service add-on that can be subscribed.

Is PZTA Controller priced and purchase separately?
No. PZTA Controller is included in the subscription pricing.

Is PZTA Gateway priced and purchased separately?
No. PZTA Gateway(s) are included in the subscription pricing. This allows for flexibility of deployments and makes deciding on how you want to deploy based on business needs rather than appliance budget.

Is PZTA included in Suites Plus?
No.

Is PZTA an option for Suites Plus?
Not at this time.

Where can I get more information about PZTA pricing?
Yes, please reach out to your Pulse account team.

MSSP-Readiness

Is PZTA included in the MSSP Program?
Not at the time of General Availability (GA) on July 28, 2020, however, it is being discussed.

Does PZTA include an MSSP tenant-management portal?
Not at the time of General Availability (GA) on July 28, 2020, however, the functionality is planning and will be available in 2H 2020.

Will MSSP's be able to brand/customize the portals or client?
The PZTA portal doesn't allow for customization yet, however, this is under consideration. The Pulse Desktop Client can be branded.

I have additional questions. Who do I reach out to?
Please reach out to your local Pulse Secure account team.