Product Information

ZoneZero SDP On-Premise/Private Cloud

Specific

safe-t

High Level Use Case

This is a generic use case that describes the use of ZoneZero SDP to provide remote access as a fully on-premise customer-owned solution

Target Market/Customers

- All verticals and any size customer
- Regulated and OT environment that do not typically consume cloud services.

The Challenge

Traditional access solutions operate on an access-first, authentication later model which allows user connections to be established to a resource first for the purpose of then authenticating on the application layer. This is analogous to allowing a person to walk into a highly secure facility to provide an ID card, but that person may already be carrying a bomb.

Most successful cyber attacks circumvent the authentication mechanism using an application-layer vulnerability and therefore any protection placed after a session is allowed to be established is extremely dangerous.

The Need

As organizations continue to "go digital" and become more connected, they open their networks and internal applications to remote employees, customers, business partners, 3rd party vendors, mobile devices, and connected devices.

Enhanced connectivity is necessary to remain business-relevant, but it comes at a cost; Research shows that six out of ten organizations around the globe have suffered at least one cyber-attack on their enterprise services.

This shouldn't be the case in our technologically sophisticated world. But it is, because organizations typically expose their services to the internet in order to interact with their many 3rd party vendors and external partners. The fact is that organizations are still using legacy methods such as VPN and virtual desktop solutions of designing perimeter networks that don't account for modern connectivity and application access challenges.

It is clear that organizations need a paradigm shift to overcome the challenges of providing simple, cost effective, and transparent access to internet facing services, while effectively combatting cyber-attacks and threats.

ZoneZero® SDP Solution

Safe-T's ZoneZero SDP changes the way organizations grant secure external access to their services. This product is part of the ZoneZero Perimeter Access Orchestration platform that provides central management of all secure access technologies and helps organizations achieve Zero Trust Network Access (ZTNA).

ZoneZero SDP offers secure and transparent access for all types of entities (people, applications, and connected devices) to any internal application, service, and data, such as HTTP/S, SMTP, SFTP, SSH, APIs, RDP, and WebDAV. ZoneZero SDP implements Safe-T's patented reverse-access (outbound) technology which eliminates the need to open incoming ports in the organization's firewall.

The Safe-T SDP Flow

The following describes the process flow of an access request while the service is unpublished to world (no active listeners, service inaccessible):

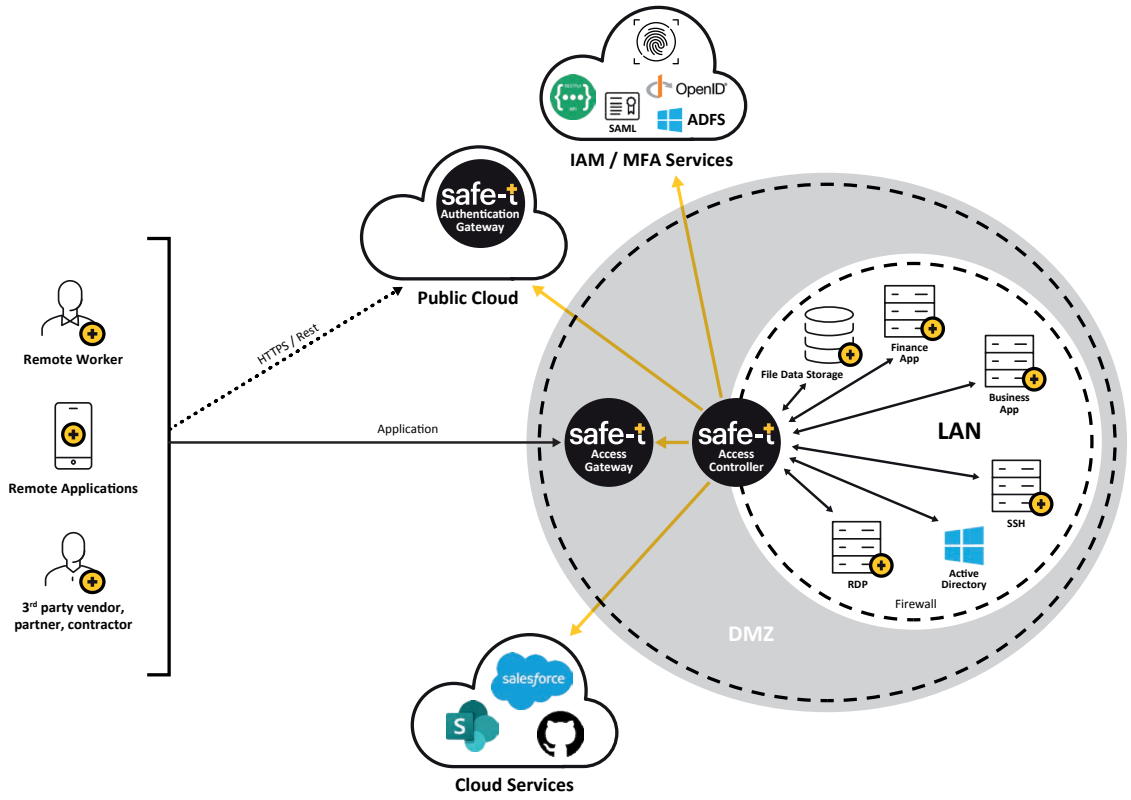
1. A user requires access to a destination on-premise service or application
2. The user opens a web browser and types in a URL for the Safe-T Authentication Gateway (such as https://auth.company.com)
3. The user inputs authentication credentials to the web portal
4. The on-premise Safe-T Access Controller creates an outbound connection to the Safe-T Authentication Gateway and pulls the user input into the private network environment (no access is provided at this point)
5. The Safe-T Access Controller authenticates the user internally by connecting to the local Active Directory service
6. Once the user is authenticated, Access Controller instructs the public cloud-based Access Gateway (on an outbound connection) to open a port to accept traffic from the user's unique IP address
7. The user is presented with a web portal containing a list of now-accessible applications. The user clicks on a link to be opened in a web browser, or switches to native client to seamlessly (such as RDP and SSH)
8. Access Controller pulls (on an outbound connection) the user traffic from Access Gateway and sends it to the destination application. The response is pushed back to Access Gateway and relayed the user in a seamless way
9. The user connection is established while the service remains inaccessible and hidden to other users

Product Information

ZoneZero SDP On-Premise/Private Cloud

Specific

safe-t



Features & Benefits Include:

- Based on Safe-T's patented Reverse Access
- Non-web protocols ready – SMB, RDP, SSH
- Cloud and on-premises implementations
- Clientless – seamless implementation
- Works in parallel with existing technologies (VPN)
- Scales precisely according to usage

Frequently Asked Questions (FAQ)

- **How can ZoneZero SDP provide access with no inbound open ports?**
  ZoneZero SDP utilizes Safe-T's patented technology called Reverse Access, which reverses the direction of the network traffic.
- **What types of authentication methods are supported?**
  Active Directory, Azure AD, ADFS, Duo (including Duo Host Checker), and any REST-API based authentication
- **What types of applications are supported?**
  ZoneZero SDP operates on the network layers (layers 3/4 of the OSI model) and can therefore seamlessly support any TCP-based application.
- **Does ZoneZero SDP change policies on the firewall?**
  No. ZoneZero SDP does not require the direct integration with the organizational firewall and is therefore vendor agnostic. Access Gateway resides behind the external firewall and acts as an additional firewall, dropping all inbound packets by default. This achieves a closed port with no active listener without requiring real time changes to the external firewall.
- **Does ZoneZero SDP connect to a cloud service?**
  In this on-premise customer-owned model, the platform is exclusively managed by the customer and does not connect to any third party.

Version 2 | 二版
www.version-2.com

Hong Kong
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

Taiwan
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw

Singapore
Tel : (65) 6296 4268
Email : sales@version-2.com.sg