

ZoneZero SDP Hybrid/Public Cloud

High Level Use Case

This is a generic use case that describes how to use of ZoneZero SDP to provide remote access as a hybrid/public-cloud based solution

Target Market/Customers

- + Any vertical and any size customer
- + Organizations that may 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 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 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 for 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 other threats.

ZoneZero® SDP Solution

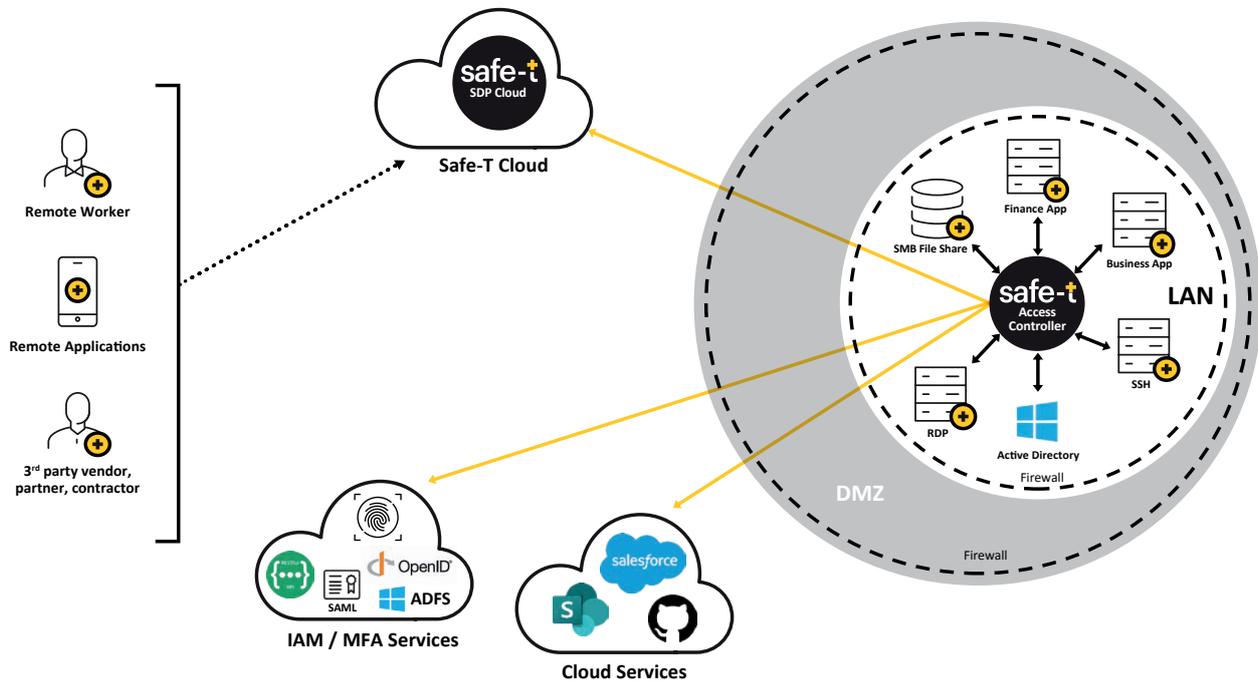
Safe-T's ZoneZero SDP changes the way organizations grant secure external access to their services.

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 steps describe the process flow of an access request while the service is unpublished to world (no active listeners, service inaccessible):

1. A user requests access to an 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>) which resides on the Safe-T Cloud
3. The user inputs authentication credentials to the web portal
4. The on-premise Access Controller creates an outbound connection to the Authentication Gateway on the Safe-T Cloud and pulls the user input into the private network
5. The Safe-T Access Controller authenticates the user internally by connecting to the local Active Directory service
6. After 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 a native client (such as RDP and SSH). The connection is established to Access Gateway on the Safe-T SDP Cloud
8. Access Controller pulls (on an outbound connection) the user traffic from Access Gateway on the SDP Cloud 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



Features & Benefits Include:

- + Based on Safe-T's patented Reverse Access
- + Non-web protocols ready – SMB, RDP, SSH
- + On-premises implementation
- + 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)
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 support any TCP-based application
- + **Does ZoneZero SDP change policies on the firewall?**
No. ZoneZero SDP creates outbound connections only from Access Controller to the SDP cloud
- + **Does ZoneZero SDP connect to a cloud service?**
Yes. The Authentication Gateway and Access Gateway reside on the Safe-T SDP Cloud from which the on-premise Access Controller pulls traffic. However, all the access decisions, user information and sensitive data are not shared in any way with the Safe-T SDP Cloud and reside exclusively on Access Controller. The Safe-T SDP Cloud cannot connect back to the organization and cannot provide unauthorized access