

High Level Use Case

The Ariel University Work From Home (WFH) use case discusses the deployment of ZoneZero SDP in order to allow university faculty members, researchers and students to access university resources and desktops

Target Market/ Customers

Any organization with users working from home PCs

The Challenge

Ariel University has many researchers and faculty members who come to the campus every day. These people either have their own work desktop or they share desktops. In addition, they access corporate data bases and file shares.

When the Covid-19 pandemic started, Ariel University made a decision shut down the university campus and instead allow faculty members, researchers, and students to access corporate resources and desktops remotely.

The challenge was that since these people were used to arrive to the campus, most of them did not have a university laptop, and they were instructed to connect from their home PCs/laptops to their University located desktops.

This created a networking and security challenge, as it is against university policy to install VPN clients on non-university endpoints.

The Need

There was a need to deploy a solution which will address the following requirements:

- + Allow faculty members, researchers, and students to access corporate resources (e.g. corporate desktops and SSH servers) without installing a VPN client on their own PCs/laptops
- + Solution had to be rolled out quickly and easily in order to prevent university downtime
- + Solution had to be easy for users to learn and use
- + Maintain highest levels of security
- + Ensure a low attack surface for the university
- + Solution had to support Forti IDP

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).

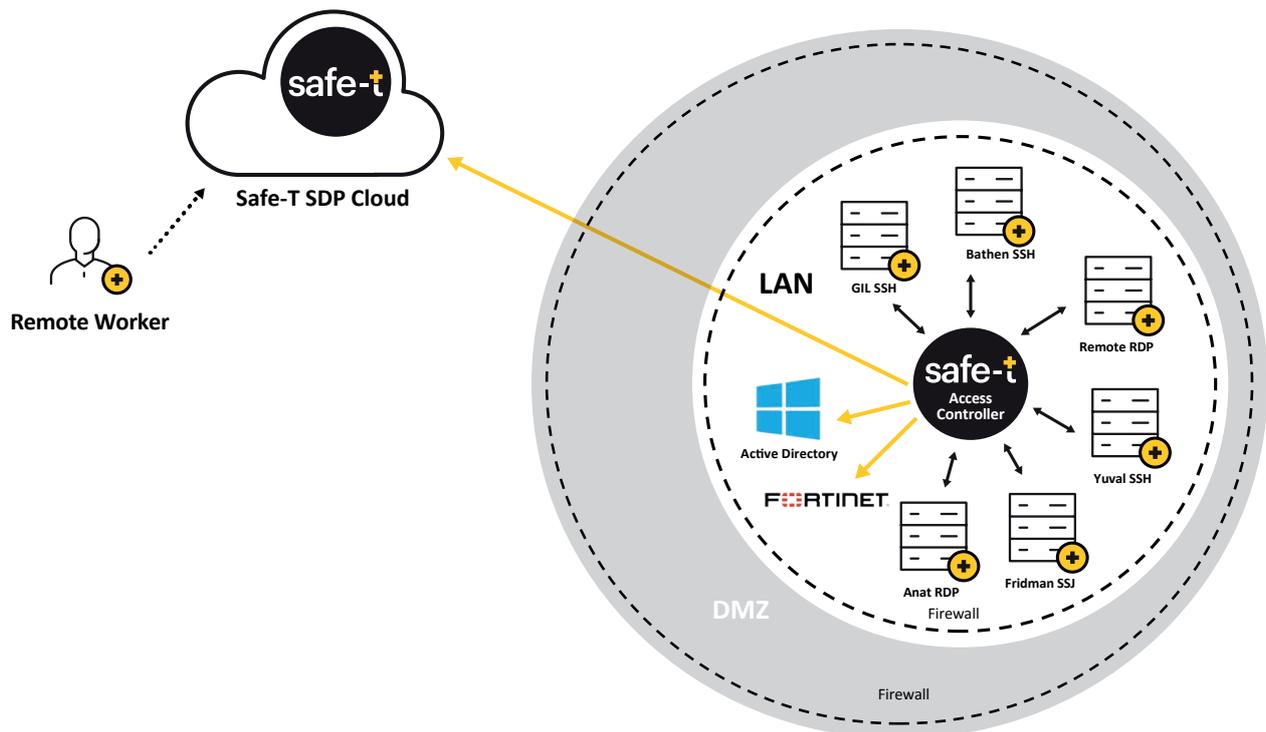
ZoneZero SDP offers secure and transparent access for all types of entities (people, applications, and connected devices) to any internal application, service, and data, such as HTTP/S, SMTP, SFTP, SSH, APIs, RDP, and WebDAV.

ZoneZero SDP implements Safe-T's patented reverse-access (outbound) technology which eliminates the need to open incoming ports in the organization's firewall.

As can be seen in the diagram below, the university deployed Safe-T's Hybrid SDP solution, allowing them to quickly roll out the remote access solution. They achieved this by deploying an Access Controller in their datacenter and connecting it to dedicated Access and Authentication Gateways that are located in Safe-T's SDP cloud.

The flow of traffic is as follows:

1. User logs into the authentication portal published by the **Authentication Gateway** (located in Safe-T's SDP cloud)
2. The user enters the credentials into the portal
3. The **Access Controller** retrieves the credentials from the **Authentication Gateway** over a reverse-access connection, and then authenticates the user using the organization's Active Directory / Azure Active Directory (depends on the user)
4. A SMS is sent for the user as 2nd factor of authentication, and the user is prompted to respond with the code
5. Once the user is authenticated, the **Access Controller** instructs the **Authentication Gateway** to display to the user the allowed services, and instructs the **Access Gateway** (located in Safe-T's SDP cloud) to provide (reverse) access to the specific user to the service
6. The user accesses the newly published service via the **Access Gateway**



Features & Benefits Include:

- + Clientless – seamless implementation
- + Works in parallel with existing technologies (VPN)
- + Scales precisely according to usage
- + Simple, cost effective, and secure deployment
- + Easily connect remote locations
- + Fast deployment
- + Protect networks from attacks
- + Enhance Zero Trust Network security
- + Improve data security by closing incoming firewall ports
- + Based on Safe-T's patented Reverse Access
- + Non-web protocols ready – SMB, RDP, SSH, any TCP
- + Cloud and on-premises implementations
- + Connect remote located networks and same location networks
- + Support humans, application, and connected devices
- + Grant none-domain user secure access

Frequently Asked Questions (FAQ)

- + **Is your solution software based or hardware based?**
Our solution is software based
- + **Does your solution require modifications to applications?**
No, our solution does not require any changes to applications
- + **Can you Safe-T ZoneZero SDP replace a VPN or MPLS?**
Yes, our solution can replace a VPN or MPLS for the specific discussed use case
- + **Do we have basic logging functions which are included in the core package?**
Yes, our solution includes logging of administrator and user actions
- + **Which applications does your solution support?**
Safe-T ZoneZero SDP supports passing traffic to any TCP based application
- + **Which types of users does your solution support?**
Safe-T ZoneZero SDP supports traffic from human users, applications, and connected devices
- + **Can your solution be used to connect networks located in separate physical locations?**
Yes, our solutions can be used to connect networks located in separate physical locations, cloud networks to datacenter networks, etc