Product Information

Secure Remote Access – ZoneZero® VPN

Generic

safe-t

High Level Use Case

This is a general use case that describes secure remote access with Safe-T ZoneZero® VPN module, that allows the organization to meet Zero Trust methodology requirements without any compromise or any architectural changes in the organization

Target Market/Customers

- Small-medium to large businesses – all Verticals
- Enterprise customers – all verticals

The Challenge

A Virtual Private Network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their client devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management (and the risks) of the private network. Most external users will use a form of remote access technology, which provides the ability for an organization's users to access its non- public computing resources from external locations other than the organization's facilities. However, there are many issues with current VPN's:

- On-going Zero-days vulnerabilities detection and disclosure in most leading VPN's vendors infrastructure
- Architectural issues – "win one – win them all"
- Lateral movement (network access vs. service Access)
- Lack of an integral MFA (2FA in best case) support

The Need

In the world of digital transformation there is a growing need for remote secure access. Almost any company needs to provide remote users – remote employees, contractors, 3rd party vendors, supply chain partners and even corporate employees that are simply out of the office - with access to corporate resources. When providing remote access, one should consider Zero Trust values. ZTNA (Zero Trust Network Access) is designed to help organizations adopt more effective security, based on the "never trust, always verify" principle. This is generally achieved by:

- Separating control plain and data plain
- Continuous & improved authentication
- Application layer access & control using least privilege strategy

ZoneZero® VPN Solution

Safe-T's ZoneZero® VPN revolutionizes secure access by providing true separation of the data plane and control plane, application layer policy monitoring & enforcement, and MFA integration to any application or service. All this is done on top of the existing infrastructure. 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). Seamlessly providing ZTNA features to existing VPN infrastructures.

The ZoneZero® VPN Flow

The following describes the process flow of an access request with ZoneZero® VPN:

1. A user requires access to a destination on-premise service or application
2. The user runs a VPN client and connects to the organizational VPN using natively supported authentication
3. The user is assigned a private IP address by the VPN service and forwards all the network traffic to **ZoneZero® Access Gateway**
4. The **ZoneZero® Access Controller** receives the user information from the VPN server and connects to Active Directory to pull the user's information and mobile number
5. The **ZoneZero® Access Controller** sends an additional factor of authentication using an external REST API (such as Telegram)
6. Only when the user responds to the MFA request his network packets are accepted by **Access Gateway** and relayed to the relevant application or service on the backend of the network

Version 2 | 第二
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

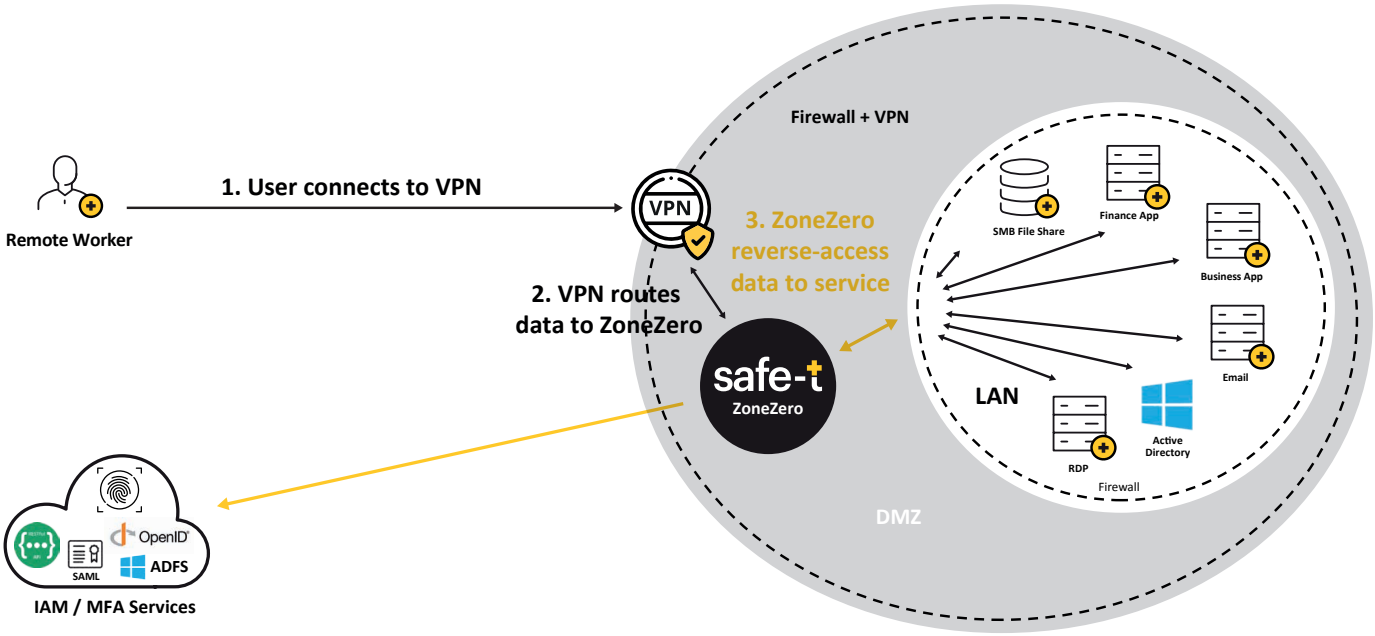
Singapore
Tel : (65) 6296 4268
Email : sales@version-2.com.sg

Product Information

Secure Remote Access – ZoneZero® VPN

Generic

safe-t



Features & Benefits Include:

- Seamless implementation
- Integration of MFA to any VPN – Tunnel/TLS
- Application layer access policies
- Continuous authentication
- Deliver ZTNA features to VPN infrastructure
- Vendor agnostic
- No UX interference
- Optimize cost of deployment and ownership

Frequently Asked Questions (FAQ)

- **How Safe-T can complement VPN with MFA?**
  VPN access schemes and non-web applications (such as SMB, SHH, SFTP, and more) are still a vital part of the organization's environment. Since SDP/MFA solutions are generally not compatible with this existing environment, organizations tend to see ZTNA as something that will require them to embark on a long journey to replace existing infrastructures with SDP solutions. As a result, the huge potential of ZTNA is unfulfilled and the adoption rate of ZTNA remains low
- **Do we have basic logging functions which are included in the core package?**
  Our end user logs, will describe to the organization, who is successfully or failed to login to the system, which granted access that specific user gain, username, time, date, and log out
- **Can SSL VPN meet the Zero Trust needs?**
  VPN and SSL VPN have the same methodology of access, the only main difference between them, is "how" to access. In addition to that, with SSL VPN the organization still are missing the capabilities of Zero Trust (authenticated before access, missing the Safe-T unique Reverse Access technology patent to prevent inbound port) and with Safe-T the organization gain support for vertical access, such as application, API, and IOT devices

Version 2 | 版一
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