SOLUTION BRIEF

Fortinet and Safe-T Data Security Solution

Executive Summary

As the world has become more digital and connected, organizations are increasingly opening their networks and internal applications to external or public audiences, such as employee devices, business partners, third-party vendors, mobile devices, and Internet-of-Things (IoT) devices. While this enhanced connectivity opens new business opportunities, connectivity comes at a cost. This comes at a time when 69% of breaches within the past year were perpetrated by outsiders.[1]

One reason why many organizations are vulnerable to attack is because they are relying on traditional cybersecurity methods. Perimeter networks that consist of demilitarized zone segments, and application access via IPsec, secure sockets layer (SSL) virtual private networks (VPNs) simply cannot keep pace.

The Fortinet and Safe-T Data partnership addresses these challenges, helping organizations create a secure and agile remote access solution based on zero-trust concepts. The joint solution establishes a best-of-breed zero-trust network access solution controlling user access and how access is granted to internal and cloud services.

Key Benefits

- Authenticates before providing access with FortiAuthenticator
- Easily integrates FortiAuthenticator to any application access flow
- Hides services from unauthorized users
- Reduces attack surface by closing incoming firewall ports
- Controls user access and network use
- End-to-end monitoring of application access flow

FORTINET Fabric-Ready

Joint Solution Description

This joint solution allows access to applications on a need-to-know basis only, while providing users with fast and seamless access to the resources they need. This results in a verify-first, access-second zero-trust approach across applications for enhanced security, greater understanding of network activity, and fewer frustrated users.

The Safe-T Software-Defined Perimeter controls the access to an organization's internal services, and uses FortiAuthenticator to authenticate users trying to access the services.

The joint solution can be deployed using either the on-premises Safe-T Software-Defined Perimeter deployment as depicted in Figure 1, or with the cloud-based Safe-T Software-Defined Perimeter service as depicted in Figure 2.

The Fortinet and Safe-T joint solution works as follows:

1. A user logs into the dedicated authentication portal published by an authentication gateway that is either deployed by the organization or from the Safe-T cloud service.
2. The user enters their 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 via FortiAuthenticator.

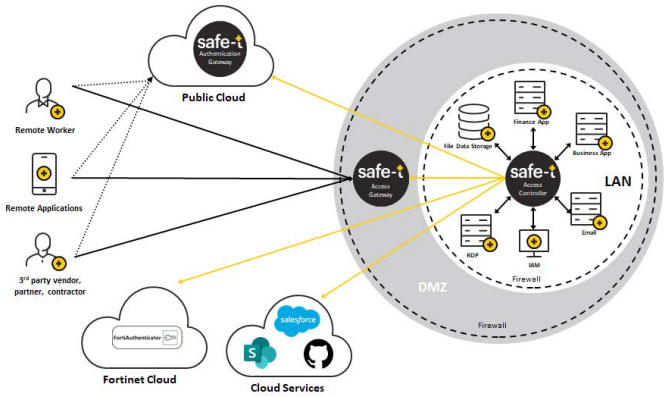

Figure 1: On-premises Safe-T Software-Defined Perimeter with FortiAuthenticator.

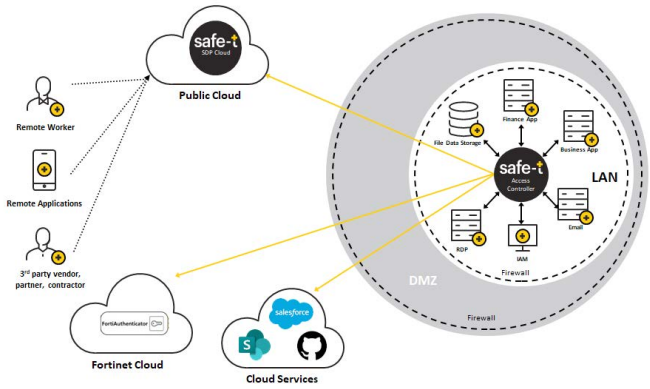

Figure 2: Cloud-based Safe-T Software-Defined Perimeter with FortiAuthenticator.

4. Once the user is verified by FortiAuthenticator, the access controller:
   - Instructs the authentication gateway which applications to display to the user
   - Instructs the access gateway to provide the user with reverse access to the allowed applications
5. The user selects the application that should be accessed.
6. The user accesses the newly published transmission control protocol (TCP)-based service via the access gateway.

Safe-T Software-Defined Perimeter

Safe-T Secure Application Access is an evolved approach to granting secure external access to services. Built on the Safe-T Software-Defined Perimeter technology and reverse-access patent, it offers secure and transparent access for all entities to internal applications and data.

Deploying the Safe-T Software-Defined Perimeter architecture allows organizations to design and deploy an on-demand perimeter. The on-demand perimeter creates automated, dynamic access rules for authenticated users accessing applications and data.

FortiAuthenticator strengthens enterprise security by simplifying and centralizing management. FortiAuthenticator identifies users, queries access permissions from third-party systems, and communicates this information to FortiGate next-generation firewalls to create identity-based policies. FortiAuthenticator provides key services in creating an effective security policy and strengthening security with user authentication.

Features

- Robust multi-factor authentication options with FortiAuthenticator
- No open ports are required to be configured for access
- Bi-directional traffic is handled on outbound connections from the LAN to the outside world
- Support any TCP-based application or protocol, including HTTP/S, SMTP, SFTP, APIs, RDP, WebDAV, SSH, or SAP
- Integrated user behavioral analysis
- Performs SSL decryption in a secure zone
- Provides only direct application/service access and blocks network access
- Removes the need for VPN access

About Safe-T

The Safe-T Group Ltd. provides zero-trust access solutions that mitigate attacks on business-critical services and sensitive data, while ensuring uninterrupted business continuity.

Safe-T cloud and on-premises solutions ensure that an organization's internal and external access use cases are secured according to the validate first, access later zero-trust philosophy. This means that verification is required from everyone trying to gain access to resources on the network or in the cloud.

With Safe-T patented reverse-access technology and proprietary routing technology, organizations of all size can secure their data, services, and networks against internal and external threats. For more information about Safe-T, visit www.safe-t.com.

[1] "2019 Data Breach Investigations Report," Verizon, 2019.

FORTINET®

www.fortinet.com

February 13, 2020 12:12 AM

587896-0-0-EN

D:\Fortinet\Solution Briefs\grey solution briefs\Safe-T\sb-FA-fortinet-and-safe-t-data-security-solution