SAFE-T

Keeping Data in the Right Hands

Secure Application Access

Product Brief

Contents

Introduction

As the world becomes much more digital and global, organizations are opening up their network and internal applications to the outside world (e.g. employees, customers, business partners, 3rd party vendors, mobile, IOT), much more than in the past.
But while the amount of external parties is ever growing and evolving, the common methods of providing external parties access, have stayed the same - S/FTP access, VPN and SSL VPN access, reverse-proxy access, RDP, etc. And they all have one common flaw, they provide access before the authenticate, essentially exposing your services to both trusted and untrusted entities.
In addition to the above, the common access options, have benefits but also major faults:

- **S/FTP -** File servers are simple to deploy and use by either internal or external users, and are usually placed in the DMZ (on-premises or in the cloud) for easy access.
  However, this methodology is inviting hackers to easily attack such as service, using it as a jump point to the network via the open firewall port or steal its SSL keys and certificates.
- **VPN / SSL VPN -** VPNs offer high security by utilizing certificates or other authentication mechanisms. However, they pose various challenges when used by external parties – they are complicated to manage due to certificates distribution to partners, they store SSL certificates in the DMZ, they open ports in the firewall, and they provide network access.
- **Reverse Proxy access -** everse-proxies are the simplest means of allowing external parties to access internal applications, they are simple to deploy and they offer a wide range of security options. However they pose quite serious security concerns - hackers can easily "see" and attack them using various SSL/SSH based attacks or OS based vulnerabilities, they store SSL keys in the DMZ (on-premises or in the cloud) unprotected, they require opening ports in the firewall, and more.
- **RDP (Remote Desktop) -** remote desktop access is used to allow remote/external access to a specific machine within the network. This access can be granted to organization employees or 3rd party partners, however in most cases the basic requirement is the use of a VPN connection over which the RDP protocol will flow. This results in the VPN deployment challenges discussed above.

The Safe-T Solution

Safe-T Software Defined Access introduces an evolution in the way organizations grant secure external access to their services.
Built on Safe-T's Software Defined Perimeter technology and Integrated Data Security Platform, it offers true secure and transparent access for all entities to internal applications and data.
By deploying Safe-T's Software Defined Perimeter architecture organizations can now design and deploy the On-Demand Perimeter. The On-Demand perimeter creates access rules for authenticated users into applications and data, in a fully automated and dynamic fashion.

How It Works

As can be seen in figure 1 below, the Safe-T Secure Application Access solution is composed of three access servers. The solution is deployed in multiple tiers within the organization and cloud:

- Cloud tier – includes the Authentication Gateway which is deployed with the cloud (Amazon, Azure, etc)
- DMZ tier – includes the Access Gateway
- Lan tier - includes the Access Controller which connects to the organization's backend applications, storages and authentication services (AD, IAM, etc).

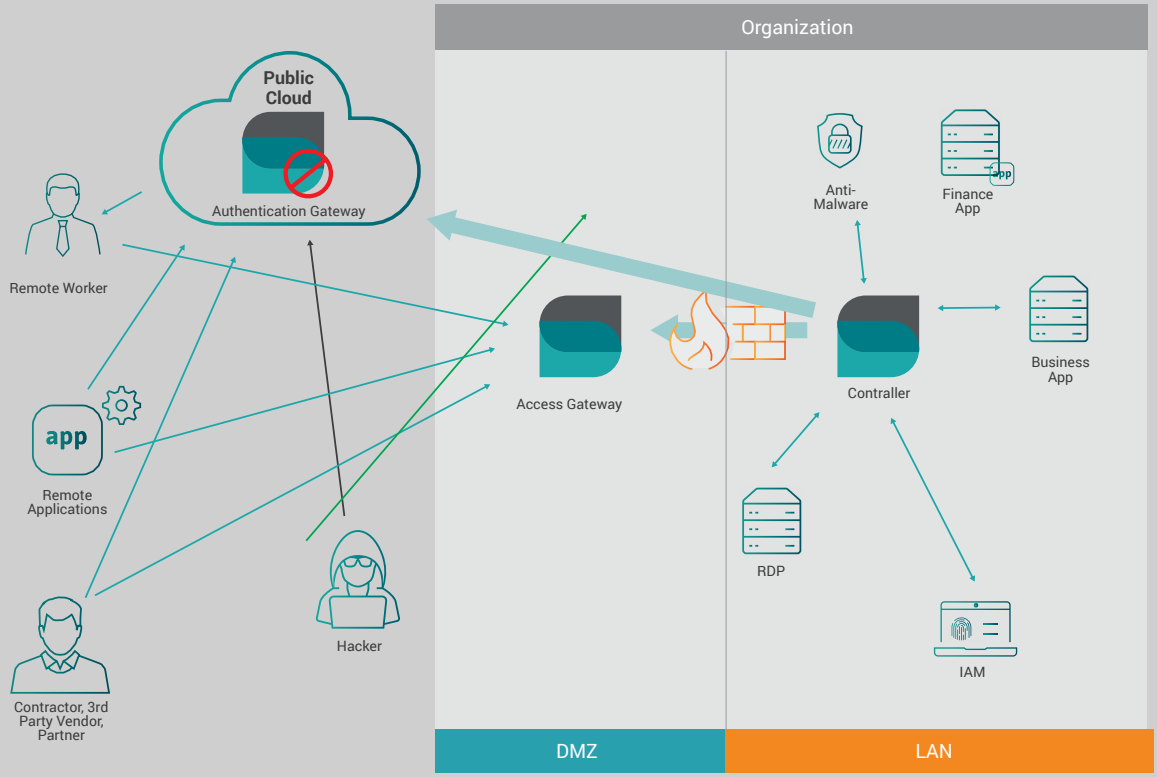

Figure 1 - Safe-T Secure Application Access

The flow of the solution is as follows:

1. User logs into dedicated authentication portal published by the **Authentication Gateway**
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 - 3rd party IAM/IDP solutions, POST based login, Microsoft Active Directory, SAML, OTP, etc
4. Once the user is authenticated, the **Access Controller** instructs the **Authentication Gateway** which applications to display to the user, and instructs the **Access Gateway** to provide (reverse) access to the specific user to allowed applications
5. The user selects the application which should be accessed
6. The user is redirected to the application's published IP address
7. The user accesses the newly published service
8. Once the user disconnects from the service, the **Access Controller** instructs the **Access Gateway** to block access to the specific user to the specific application

Capabilities

Deploying Software Defined Access for secure application access provides the following capabilities:

- Firewall is constantly in deny-all state, no open ports required for access
- Bi-directional traffic is handled on outbound connections from the LAN to the outside world
- Support a variety of applications – HTTP/S, SMTP, SFTP, APIs, RDP, RDH5, WebDAV
- Allow client-less access to applications and data
- Robust multi factor authentication options
- Remove the need for VPN access
- Perform SSL decryption in a secure zone
- Scan any incoming traffic for attacks
- Hide DMZ components which can be hacked and utilized to access the network
- Provide only direct application/service access, blocking network access

Benefits

The benefits of providing application access via Safe-T's Anonymous Application Access:

- **Authenticate before providing access**
- **Hide services from unauthorized users**
- **Reduce attack surface by closing incoming firewall ports**
- **Client-less application access**
- **Minimize risk of network DDoS and application level attacks**
- **Control user access and usage**
- **End-to-end monitoring of application access flow**

Feature List

Access Component

Feature	Comments
System Level Features	
High availability (HA) **Ability to perform high availability/clustering mode in the same data center and between data centers**	Safe-T Secure Application Access solution can be setup in HA using an external load balancer or application delivery controller. In addition, a single Access Controller can operate with multiple Access Gateways and Authentication Gateways.

Feature List

Access Component

Feature	Comments
System Level Features	
Disaster recovery **Ability to failover to another data center in the event of application unavailability or site disasters**	Safe-T Secure Application Access solution can be setup in a disaster recovery architecture using an external load balancer or application delivery controller
Deployment	On-premises or Hybrid-cloud
Access Features	
Patented Reverse-Access technology	Safe-T's reverse-access technology is patent protected. The Reverse-access technology is a dual node technology, which removes the need to open any ports within a firewall, while allowing secured application access between networks (through the firewall)
Requires opening firewall ports	No
Support any TCP based application / service	Safe-T Secure Application Access solution supports any TCP based application / service, applying reverse-access to it
Logical Network Segmentation	Logically segment the network, deploying a Zero Trust model, to reduce the risk of cyber-attacks from reaching internal network segments, or laterally moving throughout your network
HTTPS Proxy	Safe-T Secure Application Access solution supports HTTP/S based applications / services
WebDAV Support	Safe-T Secure Application Access solution supports WebDAV based file access

Feature List

Access Component

Feature	Comments
Access Features	
SSL Off-loading	Safe-T Secure Application Access solution support terminating SSL client connections destined to an application / service
Multi-factor authentication	Safe-T Secure Application Access solution supports authenticating and authorizing users with multi-factor identity management tools before service requests to back-end applications can take place. • Authentication via the organization's LDAP or Active Directory systems, • Authentication using OTP as 2nd factor for NTLM or Kerberos • Integration with 3rd party authentication solutions • NoPost authentication based on emails • SSO support
Client-less and VPN-less application access	Safe-T Secure Application Access solution does not require any client application to be installed on the end-user's machine
Dynamic URL rewriting supporting multi-domain applications	Safe-T SDA supports the following rewriting options: • Rewriting the destination hostname to defined subdomain • Prepending the virtual directory • Rewriting both (http / https) protocol to https or http
Per User Group Access Policies	Yes
Time/Date Based Access Policies	Yes

Feature List

Access Component

Feature	Comments
Management and Operation	
Using a Web for full management	Yes
System logs	Yes
External Provisioning	Yes, via TCP API for reverse-access rules