Contents

Introduction ................................................................. 3
The Safe-T Solution ........................................................ 3
How It Works .................................................................. 3
Capabilities .................................................................... 4
Benefits ........................................................................... 5
Feature List ...................................................................... 5
Access Component .......................................................... 5
Introduction

Recent years have shown an ever-growing increase in cloud adoption by organizations, both regulated and non-regulated. Cloud adoption has many aspects, whether it’s using SaaS solutions, outsourcing MSSP services or hosting previously on-premises located servers in the cloud.

In this paper we will focus on the last use case, where an organization is migrating servers who were previously located on-premises to a public cloud (Azure, AWS, etc). Moving application tiers to the cloud, requires rearchitecting the network and application, for example, if previously all application tiers were located on-premises, now you need to connect a cloud based application tier to application tiers located on-premises.

Such a move creates a few challenges, such as:
• Incoming holes in the organization’s Firewall for cloud traffic
• Requires a VPN or secure connection to connect between Cloud and organization premises
• Hacking the cloud allows revealing the customer’s internal network IP
• Potentially placing an authentication component in the cloud

The Safe-T Solution

Safe-T® Software Defined Access provides a method for enterprises to convert their complex DMZ and perimeter architecture to light perimeter layer hosted in the cloud, while increasing network and application security.

By deploying Safe-T in a hybrid cloud and on-premises deployment, organizations can benefit from a cloud based perimeter and DMZ segment which can augment and simplify their local enterprise DMZ and allow pushing their perimeter farther away from their on-premises data center. In addition, the solution, allows securely connecting cloud-based application tiers (e.g. web frontend) with on-premises application tiers (e.g. backend or DB) without the need to open the organization’s firewall to the cloud, or deploying a VPN between the cloud and premises.

Using this architecture, all the organization’s services are published from the cloud using an Access Gateway located within the cloud and an Access Controller which is located on-premises.
How It Works

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

- **Cloud tier** – includes an Access Gateway which is in the public cloud after the cloud located front-end server

- **On-premises tier** - includes an Access Controller which connects to the on-premise back-end applications

*Figure 1 - Safe-T Secure Hybrid Cloud Access*
The flow of the solution is as follows:

1. User browses to Cloud service

2. Cloud Application/front-end server authenticates user and connects to Access Gateway

3. Access Controller pulls in the user’s request from the Access Gateway and passes it to backend application (L7 Proxy can be added)

4. Backend App/DB provides data the Access Controller which pushes it to the Access Gateway

5. Access Gateway pushes the data to the Cloud App

Capabilities
Deploying Software Defined Access for Secure Hybrid Cloud Access provides the following capabilities:

- Ability to run in any cloud environment
- Hybrid cloud and on-premise deployment
- Enterprise 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 cloud
- Front-end all enterprise public facing applications from cloud
- Support a variety of applications – HTTP/S, SMTP, SFTP, SSH, APIs, RDH5, WebDAV
- Robust multi factor authentication options
- Remove the need for VPN connectivity between cloud and on-premises
- Full redundancy by utilizing multiple cloud locations
- Integration with leading security solutions
Benefits

The benefits of such a hybrid cloud and on-premises deployment include:

- Reduce the risk of application and networks based attacks
- Improve data center security by reducing organization’s attack surface
- Mask the true location of the organization’s data center
- No need to open the enterprise firewall for cloud traffic
- Simple and easy migration to the cloud
- No cloud to premises VPN overhead
- Block network access, allow application access
- End-to-end monitoring of file access flow
- No direct access to the enterprise from the Internet

Feature List

Access Component

<table>
<thead>
<tr>
<th>Feature</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Level Features</strong></td>
<td></td>
</tr>
<tr>
<td><strong>High Availability (HA)</strong></td>
<td>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.</td>
</tr>
<tr>
<td>Ability to perform high availability/clustering mode in the same data center and between data centers</td>
<td></td>
</tr>
</tbody>
</table>
## Feature List

### Access Component

<table>
<thead>
<tr>
<th>Feature</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Level Features</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Disaster Recovery</strong></td>
<td>Safe-T Secure Application Access solution can be setup in a disaster recovery architecture using an external load balancer or application delivery controller</td>
</tr>
<tr>
<td><strong>Deployment</strong></td>
<td>On-premises or Hybrid-cloud</td>
</tr>
<tr>
<td><strong>Access Features</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Patented Reverse-Access technology</strong></td>
<td>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)</td>
</tr>
<tr>
<td><strong>Requires opening firewall ports</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Support any TCP based application / service</strong></td>
<td>Safe-T Secure Application Access solution supports any TCP based application / service, applying reverse-access to it</td>
</tr>
<tr>
<td><strong>Logical Network Segmentation</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>HTTPS Proxy</strong></td>
<td>Safe-T Secure Application Access solution supports HTTP/S based applications / services</td>
</tr>
<tr>
<td><strong>WebDAV Support</strong></td>
<td>Safe-T Secure Application Access solution supports WebDAV based file access</td>
</tr>
</tbody>
</table>
## Feature List

Access Component

<table>
<thead>
<tr>
<th>Feature</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Features</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SSL Off-loading</strong></td>
<td>Safe-T Secure Application Access solution support terminating SSL client connections destined to an application / service</td>
</tr>
</tbody>
</table>
| **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 Secure Application Access 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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management and Operation</strong></td>
<td></td>
</tr>
<tr>
<td>Using a Web for full management</td>
<td>Yes</td>
</tr>
<tr>
<td>System logs</td>
<td>Yes</td>
</tr>
<tr>
<td>External Provisioning</td>
<td>Yes, via TCP API for reverse-access rules</td>
</tr>
</tbody>
</table>

© 2018 Safe-T Data Ltd. All Rights Reserved. Safe-T and all other Safe-T product and service names are registered trademarks of Safe-T Data in the U.S. and other countries. All other trademarks and names are the property of their respective owners.