Product Information

Logical Segmentation – ZoneZero® SDA

Generic

safe-t

High Level Use Case

The logical segmentation use case discusses the deployment of ZoneZero® SDA in order to perform logical segmentation between two networks. For example, a sensitive and non-sensitive network or IT and OT network

Target Market/Customers

- Industrial companies
- Medical companies
- Energy companies
- Government agencies
- Federal agencies
- Military organizations
- Regulated organizations
- Organizations looking to do micro-segmentation

The Challenge

There are many different organizations (industrial, medical, government, energy, military, etc.) that are required by regulation to segment between different networks, could be sensitive and non-sensitive networks or IT and OT networks, or between user networks and IT networks.

Today such segmentation is either achieved by complex firewalling or the deployment of physical data diodes. In both cases the solution is not 100% suitable and is quite costly.

- **Segmentation using firewalling** – this approach requires complex design and manual configuration. Which increases the overall IT OPEX due to spend on man hours. In addition, it is not true segmentation, as you have open firewall ports between the segments
- **Segmentation using physical data diodes** – this approach has many deficiencies including: (1) very high IT CAPEX costs as the solution is physical; (2) increased IT OPEX costs as it requires development of customized data transmitters and receivers in order to accommodate customer applications; (3) long rollout times; (4) the solution is only suitable for physically connected network segments and does not support geographically separated locations

The Need

There is a need then for a solution which will allow segmenting networks regardless of their physical location (same datacenter or different datacenters), in a fast and easy manner, and that does not require any modification of an application.

Such a solution should adhere to micro-segmentation concepts, such as defined by Forrester, which has introduced to the world a new paradigm for network designs, called the Zero Trust Network. This paradigm has been widely adopted by leading enterprise organizations and security and networking vendors alike. By establishing Zero Trust boundaries that effectively compartmentalize different segments of the network, you can protect critical intellectual property from unauthorized applications or users, reduce the exposure of vulnerable systems, and prevent the lateral movement of malware throughout your network.

ZoneZero® SDA Solution

Safe-T's ZoneZero® SDA is built on-top of Safe-T's unique dual-server patented technology, that removes the need to open any ports within a firewall while allowing secure application access between networks (through the firewall) on an outbound firewall rule.

Located in the organization's DMZ (on-premise or cloud), the role of the Access Gateway is to act as a front-end to all services/applications published to the Internet. It operates without the need to open any ports within the internal firewall, therefore ensuring that only legitimate session data can pass through into the internal network. What's more, the Access Gateway performs TCP offloading, allowing it to support any TCP based application without the need to perform SSL decryption.

The role of the Access Controller it to pull the session data into the internal network from the Access Gateway, and only if the session is legitimate, perform layer 7 proxy functionality (SSL offloading, URL rewrite, etc) and pass it to the destination application server.

Safe-T's ZoneZero® SDA removes the need to open any ports within the network firewall, for traffic flowing between two network segment and between an internal network or other micro-segments. This is achieved while allowing secured access through the firewall.

Safe-T's ZoneZero® SDA is a perfect fit to complement and enhance the Zero Trust Network segmentation paradigm, further improving and securing it. This is done without changing existing infrastructure or applications and thus removing the need to use a physical data diode.

Safe-T revolutionizes the Zero Trust Network design. By deploying Safe-T as a central technology in the core network segment, organizations gain the ability to not only keep sensitive segments separate and small, but also to ensure that only outbound communication takes place, thus enhancing the security of the model.

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

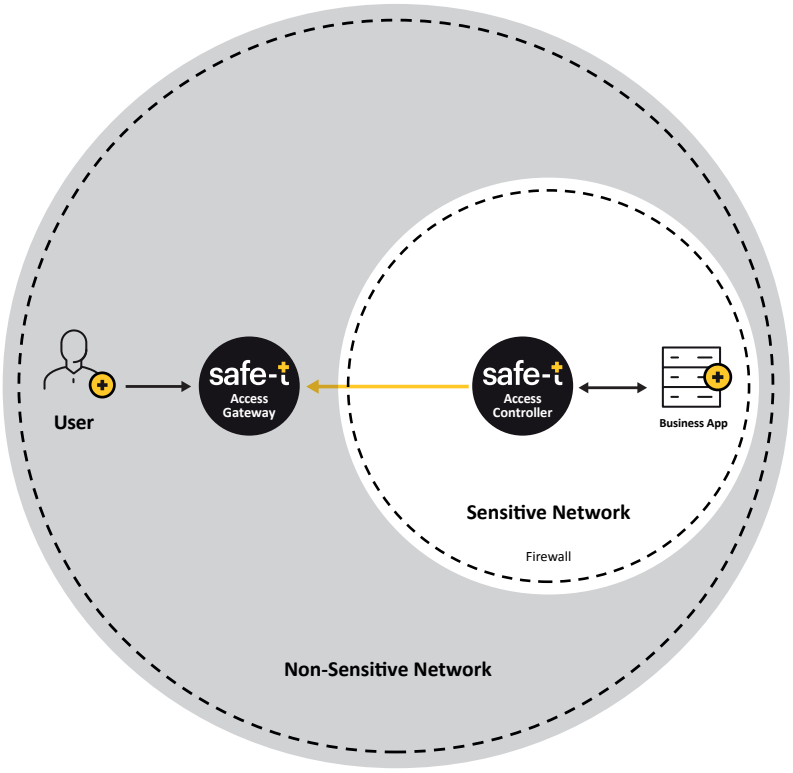
Singapore
Tel : (65) 6296 4268
Email : sales@version-2.com.sg

Product Information

Logical Segmentation – ZoneZero® SDA

Generic

safe-t



Features & Benefits Include:

- Logically segment networks
- Protect networks from attacks
- Enhance Zero Trust Network security
- Improve data security by closing incoming firewall ports
- Improve MCAP segmentation
- Remove the need for physical segmentation solution
- Connect remote located networks and same location networks
- Support humans, application, and connected devices

Frequently Asked Questions (FAQ)

- **Is your solution software based or hardware based?**
  Our solution is software based
- **Does your solution require special networking configuration?**
  No, our solution is transparent to the network
- **Does your solution require modifications to applications?**
  No, our solution does not require any changes to applications
- **Can you Safe-T ZoneZero® SDA replace a physical data diode?**
  Yes, our solution can replace a physical data diode for network segmentation
- **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® SDA supports passing traffic to any TCP based application
- **Which types of users does your solution support?**
  Safe-T ZoneZero® SDA 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

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