SAFE for decision makers

Purpose

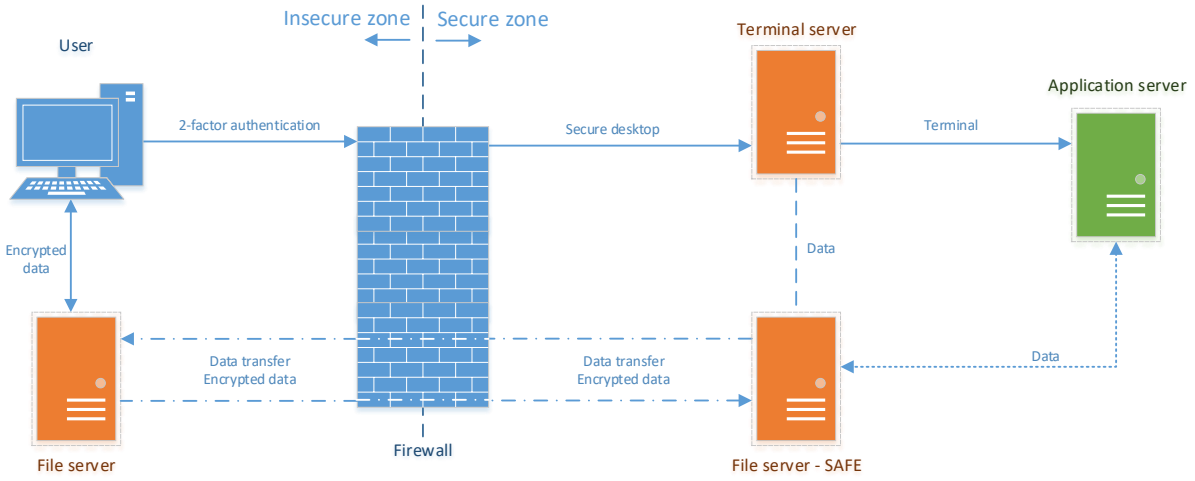
At the IT-department at the University of Bergen, we have developed a solution for secure processing of sensitive personal data in research, SAFE.

SAFE is based on “Norwegian Code of conduct for information security in the health and care sector” (Normen) and ensures confidentiality, integrity, and availability are preserved when processing sensitive personal date

Through SAFE, the IT-department offers a service where employees, students and external partners get access to dedicated resources for processing of sensitive personal data.

Principle

Access to SAFE can be described using the following graphic:



Access to SAFE

The users connects to the secure desktop from his/her own computer using a VPN client, which supports 2-factor authentication. In addition to a username and password, the user will have to supply a one-time code received on his/her phone, either as a text message or in an app. Following a successful login, the user will connect to the secure desktop using remote desktop software.

The secure desktop is a session on a terminal server, hardened according to guidelines provided by “Norwegian Data Inspectorate” (Datatilsynet). Measures include no cut-and-paste, no printing, and no mapping of folders. Users in the same projects share a terminal server.

The data are located on a network share, available from the secure desktop. The project manager controls access to files and folders through an access document.

If a project requires Linux resources, a dedicated Linux application server is provided. The users access the Linux server using Putty or X2Go.

Getting started with SAFE

A project manager asks for a new SAFE project using our ticketing system (https://bs.uib.no). The SAFE team will set up a terminal server based on the information from the project manager and install relevant software. A suitable data share is set up with security settings provided by the project manager. At this point, the project manager will have access and can start transferring data to SAFE.

The access document is only available for the project manager and contains authoritative information on all users in the project, including name, user-id, cell phone number, and access level. To initiate a change in access, the project manager updates the access document and creates an issue in our ticketing system.

Access to SAFE requires a University of Bergen computer account. However, each department have approvers who can create external accounts for partners if needed.

Transfer of data

Data can be imported to the secure desktop by placing files in an import folder available to computers in the UoB network. The files will be transferred to the secure desktop within 5 minutes.

Data can be exported from the secure desktop by placing files in an export folder available from the secure desktop. The files will be transferred to a folder available to computers on the UoB network within 5 minutes.

The project manager for each project controls which users can export files, but all users within a project can import files.

When users copy data from the secure desktop, a copy of the data is made in a folder accessible only to the project manager. In addition, a file containing the time stamps is updated. Before transferred, files are also encrypted (AES-256). The password needed to open the file on the outside is kept in the export folder available from the secure desktop.

Infrastructure

SAFE is based on a virtualization platform from VMware. Hardware in SAFE is redundant for the most parts. Backups of data shares are encrypted before leaving SAFE.

Maintenance of SAFE

In order to support SAFE, some users from the IT department have access to the management zone. From the management zone, maintenance tasks related to physical hardware can performed.

SAFE is relying on some basic network services in the UoB network, like DNS, DHCP, AD and Puppet. Servers in SAFE are patched simultaneously with other servers maintained by the IT-department every third Saturday of each month. Exceptions can be made upon request.

Client management

The IT-department is offering management of clients, both Windows, Mac and Linux. Users who have computers not managed by the IT-department are expected to comply with the guidelines outlined in Appendix 1 “SAFE E - Contract with external users.docx”.

Training

A training course is available from *Mitt UiB* (https://mitt.uib.no) providing potential users with a basic description of SAFE as well as detailed procedures on how to connect to SAFE. The training course requires a UoB account. Some files with similar content are available from https://it.uib.no/SAFE.

Appendix 1:

UNIVERSITETET I BERGEN
IT-avdelingen

Agreement between University of Bergen and <name of partner> at <name of institution>.

Secure solution for sensitive data (SAFE)

Minimum Security Standards for computers connecting to SAFE.

We expect the following to be true when connecting to SAFE from a computer not maintained by the University of Bergen, IT-department:

1. An individual computer (not shared)
2. A supported operating system with the latest patch level
3. Current anti-virus and anti-malware software installed
4. Personal firewall turned on
5. Login account without elevated privileges
6. Lock-screen policy enabled
7. Complex password
8. No unencrypted authentication
9. No unnecessary services running

Expected behavior:

1. SAFE system is used only for the purpose for which it is intended
2. Ensure sensitive data extracted from SAFE is encrypted whenever computer is connected to the Internet.
3. Report any security incidents

The University of Bergen IT-department reserves the right to block access to SAFE from computers, which do not comply with the above guidelines.

_____

Signature partner