SafeViewer

software united by NOVENTIQ Global expertise, local outcomes

Installation Abstract

In light of a successful installation of Safe Viewer (hereonto known as “System”), please find all necessary details and procedures regarding an implementation process. In fact, the system is devided into two logically separated and independent components - backend and frontend. When it comes to a database, the system uses MySQL DB server which is, by default, located at the same virtual machine as the backend server. The DB server itself can be, of course, moved to a different virtual machine, if that better suits client’s will.

The system uses standard web communication protocols (HTTP, WebSocket), therefore, it is necessary to provide adequate network configuration / security policies in order for the platform to work properly and meet expected results.

An installation process itself can be placed either remotely or in physically in person, according to a client’s decision / agreement. The process is started and led by dedicated proprietary automation scripts. The scripts are unique for each installation and no sensitive / client-related information is shared, by any means, among installation attempts.

System requirements

	BACKEND	FRONTEND
OS	Linux Ubuntu 22.04 LTS	Linux Ubuntu 22.04 LTS
CPU	~ 2Ghz (4-8 core)	~ 2Ghz (4-8 core)
RAM	4-8 GB	4 GB
SSD	128 GB	25 GB
SSD1	As needed	/
FS2	separate ext 4 virtual drive	/

Network Configuration

	BACKEND	FRONTEND
Incoming	TCP: 80,443,10791	TCP: 80,443,10791
Outgoing	No restriction	No restriction

The system can be accessed and maintained through either a VPN connection, if exists, and further through a locally available SSH port. In such a case, no ports have to be exposed publicly. The other option is to provide a direct remote access through the Internet via SSH (ex: 10791) and further NAT it to a desired port (ex. public: 10791/TCP -> private: 10791/TCP).

There is a need for 2 publicly reachable IP addresses, thus the same number of sub-domains, in a case of a direct access. However, WAF (Web application firewall) can also become a solution in this scenario. In fact, with WAF having the role in the play, the number of IP addresses used reduces to only 1, potentially offering a better foundation for client's needs.

An important point to mention in that virtual servers have no need to be locally visible (backend and frontend). Have in mind that, if a previously mentioned DB server is located at a separate server, then a visibility between those virtual assets is required.

It is necessary to create appropriate DNS entries to suit for address resolution needs. Records should be of an A type, and their number corresponds to the number of issued IP addresses or WAF nodes. SSL certificates are to be automatically generated (Let's Encrypt) by the system itself, if not otherwise done. If routed through WAF, HTTPS is going to be terminated at the firewall, and traffic forwarded to the endpoint nodes through HTTP protocol.

A Web proxy is not required, yet the system supports it, and can be realized upon client's needs. When it comes to NAT, it is enough to allow a standard Web allowance policy (refer to 'Network configuration' table above).

The installation is expected to be completed within 24 hours. This timeframe also includes testing and making sure that every aspect of the process went along properly. After the successful installation, we provide support for license activation and a further guidance, if needed.
Although all main topics of the installation procedure are covered above, please be free to contact us as a need appears.