

System Requirements Firewall Orchestrator

Hardware Requirements

Both physical and virtual systems are supported

For minimal (test) installations

- 20 GB HDD
- 8 GB RAM
- 1 CPU

For standard production installations (<1000 rules)

- 200 GB SSD
- 16 GB RAM
- 4 CPUs

For large production installations (>1000 rules)

- 800 GB SSD
- 32 GB RAM
- 8 CPUs

Software Requirements

Supported operating systems:

- Ubuntu >=20.04 (LTS only)
- Debian >=11 (stable and testing)

Requirements Network Connection

- For software download during installation and upgrade:
 - Either direct Internet connection via http or https or http(s) proxy-based Internet connection.
 - In case of a security filtered Internet access, download of all required packages (operating system and base components) for installation and upgrade must be possible. List of domains that must be reachable:
 - cactus.de (only for downloading test data)
 - ubuntu.com
 - canonical.com
 - github.com
 - githubusercontent.com
 - docker.com
 - cloudflare.docker.com
 - docker.io
 - hasura.io
 - postgresql.org
 - microsoft.com

- nuget.org
 - googlechromelabs.github.io
 - storage.googleapis.com
 - pypi.org
 - pythonhosted.org (and sub-domains)
 - snapcraft.io
 - snapcraftcontent.com (and sub-domains)
 - visualstudio.com
- In case of an existing support contract, remote access via ssh to all firewall or-
chestrator systems must be possible for Cactus eSecurity support personnel.
Ssh access must use permissions which allow for the complete administration of
the software components that need to be supported. Ssh access can be one of the
following: either direct or based on OpenVPN, Wireguard or IPsec.