

Systemanforderungen Firewall Orchestrator v6.x

Hardware-Anforderungen

Sowohl physikalische als auch virtuelle Systeme werden unterstützt.

Minimal/Test-Installationen

- 20 GB HDD
- 8 GB RAM
- 1 CPU

Standard Produktiv-Installationen (<=1000 aktive Firewall-Regeln)

- 200 GB SSD
- 16 GB RAM
- 4 CPUs

Enterprise Produktiv-Installationen (>1000 aktive Firewall-Regeln)

- 800 GB SSD
- 32 GB RAM
- 8 CPUs

Software-Anforderungen

Unterstützte Betriebssysteme:

- Ubuntu >=18.04 (nur LTS-Versionen)
- Debian >=10

Anforderungen Netzwerkanbindung

- Zum Software-Download während der Installation oder beim Upgrade:
 - Direkte Internetverbindung mit den Protokollen http und https.oder http(s)-Proxy-basierte Internetverbindung
 - Bei vorhandener Sicherheitsfilterung (Proxy) muss für Installation- und Upgrade das Herunterladen aller notwendiger Quell-Pakete (Betriebssystempakete, Basiskomponenten) möglich sein. Liste der Domains, die erreicht werden müssen:
 - ubuntu.com
 - canonical.com
 - github.com
 - githubusercontent.com
 - docker.com
 - docker.io
 - hasura.io
 - ansible.com
 - postgresql.org
 - microsoft.com
 - nuget.org

- `visualstudio.com`
- Bei vorhandenem Wartungsvertrag muss der Remote-Zugriff per ssh auf alle Systeme unter Wartung für Cactus eSecurity Support-Mitarbeiter möglich sein. Der ssh-Zugriff muss mit Berechtigungen erfolgen, die zum vollen Betrieb der zu wartenden Software befähigt. Der ssh-Zugriff kann entweder direkt oder per OpenVPN, Wireguard oder IPSEC-VPN erfolgen.