Module/Topic	Function	Description
General	Base Functionality	Provides unified access to all of your firewall configurations via a single web frontend. For system providers with complex customer firewall environments there is a built-in multi-tenant functionality, allowing granular access for each customer. • Reporting functionality: ◦ Normalized rule report across all supported firewall modules ▪ current ▪ historic ◦ Normalized change report across all firewall modules ◦ Compliance reporting (customizable, e.g. show all rules with any objects) ◦ Statistics report shows the number of existing rules and objects per firewall management/gateway ◦ Reports can be scheduled and exported into various report formats • Re-certification functionality: ◦ allows certain users (those with role recertifier) to analyse existing rules and either re-certify or request deletion of rules ◦ re-certification time interval configurable ◦ re-certification workflow customizable to your needs • Open access, integration and automation ◦ All data is accessible via APIs to give you maximum flexibility ◦ Integrate your existing (ldap-based) directory service for access handling
	Currently available for the following operating systems	• Ubuntu >=18.04 (LTS only, recommended platform: Ubuntu 20.04 LTS Server) • Debian >=10
	Additional system requirements	See document „Firewall Orchestrator system requirements“
	License	Firewall Orchestrator is provided according to Apache 2 license (***https://www.apache.org/licenses/LICENSE-2.0.html***) without warranty or liability.
	Download	Firewall Orchestrator can be downloaded free of charge at ***https://github.com/CactuseSecurity/firewall-orches-***

		***trator*.**

Architecture	Communication requirements	Application access:
		• End user → Frontend: 443/tcp
		• FWO internally:
		  ◦ Frontend → Backend: API access9443/tcp
		  ◦ Importer → Backend: API access 9443/tcp, DB access 5432/tcp
		  ◦ Importer → Firewall-Systeme: Import 22/tcp (SSH), 443/tcp (API)
		  ◦ Backend → LDAP/AD: 636/tcp (ldaps)
		• Access from 3rd party systems → Firewall Orchestrator API: 9443/tcp
		
		Operating system:
		• all modules outgoing
		  ◦ → NTP-Server: 123/udp
		  ◦ debian/ubuntu Update Server http/https
		• Installation/Upgrade (ansible host) Installations-System → Internet-Proxy: proxy-Port - or direct Internet access via http(s)

	Available Modules	• Import module
		
		• Frontend
		  ◦ Reporting
		  ◦ Report Scheduling
		  ◦ Report Archivierung
		  ◦ re-certification
		
		• Backend
		  ◦ GraphQL API
		  ◦ Database
		  ◦ internal LDAP-Server
		  ◦ Middleware Server

	Architecture variants	• Separation of the following modules on different systems, e.g. for load-balanancing purposes is possible:
		  ◦ Frontend
		  ◦ Backend

		◦ Importer • Setting up multiple instances of the following modules (e.g. one per tenant or for complying with access restrictions) is possible: ◦ Frontend ◦ Importer
Backend APIs	API Integration	• Firewall Orchestrator GraphQL API allows for automated access to all firewall data • User Management API for automated user and RBAC handling
User management	Multi-tenant support	Firewall Orchestrator supports separating data for multiple tenants either on a firewall management or gateway level.
	Integration of external directory services	The following external enterprise directory services can be used by Firewall Orchestrator: • LDAP • Active Directory
	Role Based Access Control (RBAC)	The following pre-defined roles exist within the product to control data access (in addition to tenant-separation) at the front end and API access layer: • reporter: report generation on a per-tenant-level • reporter-viewall: unlimited report generation across all firewall systems • importer: internal technical role for firewall configuration import into Firewall Orchestrator • dbbackup: internal technical role for backing up all data • auditor: Frontend user role for full read-only access • fw-admin: role for firewall admins • admin: Super user full read/write access • recertifier: role for users with firewall rule re-certification rights
Frontend	Language support	The web front end is currently available in the following languages (individually adjustable per user): • German • English
	Report formats	• PDF

		• HTML • JSON
Importer	Supported firewall products	• Check Point R5x/R6x/R7x - ssh access to management server (SmartCenter) • Check Point R8x - https API access to SmartCenter • Check Point R8x - https API access to MDS (Multi Domain Server) • Fortinet 5.0 - 6.4 • Barracuda Firewall Control Center Vx - ssh access to firewall gateway directly • phion netfence 3.x - ssh access to firewall gateway directly • JUNOS 10 - 17 - ssh access to firewall gateway directly • Netscreen 5.x/6.x - ssh access to firewall gateway directly