

Module/Topic	Function	Description
General	Base Functionality	<p>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.</p> <ul style="list-style-type: none"> • Reporting functionality: <ul style="list-style-type: none"> ◦ Normalized rule report across all supported firewall modules <ul style="list-style-type: none"> ▪ current ▪ historic ▪ resolved (without any object groups) ▪ technical (without object groups or names, just plain IP addresses and service information) ▪ unused rules (currently for Check Point systems only) ◦ 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 • Workflow module: <ul style="list-style-type: none"> ◦ Fully customizable workflow module for requesting firewall rulebase changes ◦ integrated ticketing system ◦ Included workflow steps for approving, implementing and reviewing changes ◦ Integration of recertification module as well as unused rules reporting to automatically create rule deletion requests ◦ Provides API for integration with enterprise ticketing systems like ServiceNow • Re-certification functionality: <ul style="list-style-type: none"> ◦ 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 • Compliance Matrix <ul style="list-style-type: none"> ◦ Verify (requested) rules against a self-configurable ip-based zone matrix • Open access, integration and automation <ul style="list-style-type: none"> ◦ All data is accessible via APIs to give you maximum flexibility

Data Sheet Firewall Orchestrator v7

		<ul style="list-style-type: none"> ◦ Integrate your existing (ldap-based) directory service for access handling
	Currently available for the following operating systems	<ul style="list-style-type: none"> • Ubuntu >=18.04 (LTS only, recommended platform: Ubuntu 22.04 LTS Server) • Debian (stable and testing) >=10 (recommended platform Debian 11)
	Additional system requirements	See https://fwo.cactus.de/en/dokumente/
	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-orchestrator .
Architecture	Communication requirements	<p>Application access:</p> <ul style="list-style-type: none"> • End user → Frontend: 443/tcp • FWO internally: <ul style="list-style-type: none"> ◦ Frontend → Backend: API access 9443/tcp, 8888/tcp ◦ Importer → Backend: API access 9443/tcp, 8888/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, 8888/tcp <p>Operating system:</p> <ul style="list-style-type: none"> • all modules outgoing <ul style="list-style-type: none"> ◦ → 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	<ul style="list-style-type: none"> • Import module • Frontend <ul style="list-style-type: none"> ◦ Reporting

Data Sheet Firewall Orchestrator v7

		<ul style="list-style-type: none"> ○ Report Scheduling ○ Report Archivierung ○ re-certification of rules ○ workflow module for requesting firewall changes <ul style="list-style-type: none"> • Backend <ul style="list-style-type: none"> ○ GraphQL API ○ Database ○ internal LDAP-Server ○ Middleware Server
	Architecture variants	<ul style="list-style-type: none"> • Separation of the following modules on different systems, e.g. for load-balanancing purposes is possible: <ul style="list-style-type: none"> ○ Frontend ○ Backend ○ Importer • Setting up multiple instances of the following modules (e.g. one per tenant or for complying with access restrictions) is possible: <ul style="list-style-type: none"> ○ Frontend ○ Importer
Backend APIs	API Integration	<ul style="list-style-type: none"> • 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	<p>The following external enterprise directory services can be used by Firewall Orchestrator:</p> <ul style="list-style-type: none"> • LDAP • Active Directory
	Role Based Access Control (RBAC)	<p>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:</p> <ul style="list-style-type: none"> • reporter: report generation on a per-tenant-level

Data Sheet Firewall Orchestrator v7

		<ul style="list-style-type: none"> reporter-viewall: unlimited report generation across all firewall systems 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 requester: Request changes to firewall configuration approver: check and approve requests implementer: manually implement requested changes
Frontend	Language support	<p>The web front end is currently available in the following languages (individually adjustable per user):</p> <ul style="list-style-type: none"> German English
	Report formats	<ul style="list-style-type: none"> PDF HTML JSON
Importer	Supported firewall products	<ul style="list-style-type: none"> Azure Firewall via REST API Check Point R8x - https API access to SmartCenter Check Point R8x - https API access to MDS (Multi Domain Server) Cisco Firepower Management Center 7ff FortiGate 6ff – REST API access FortiManager 6ff - https API access including AutoDiscovery of all active Domains/Devices Barracuda Firewall Control Center Vx - ssh access to firewall gateway directly JUNOS 10ff - ssh access to firewall gateway directly Netscreen 5.x/6.x - ssh access to firewall gateway directly
Importer Limitations	Unsupported Features	<ul style="list-style-type: none"> Check Point Inline Layer: limited (reporting) functionality