

Modul /Thema	Funktion	Beschreibung
Allgemeines	Grundfunktionalität	<p>Firewall Orchestrator gibt Ihnen einen einheitlichen Zugriff auf Ihre Firewall-Konfigurationen mittels eines Standard-Web-Frontends. Für Systemhäuser mit komplexen Kunden-Firewall-Umgebungen bietet Firewall Orchestrator eine integrierte Mandantenfunktionalität, die jedem Kunden einen granularen Zugriff auf seine Daten ermöglicht.</p> <ul style="list-style-type: none"> • Reporting Funktionen: <ul style="list-style-type: none"> ◦ Einheitliche Regelwerk-Reports über alle unterstützten Firewall-Module <ul style="list-style-type: none"> ▪ aktuell ▪ historisch (zu einem beliebigen Zeitpunkt in der Vergangenheit) ▪ aufgelöst (alle verwendete Gruppen) ▪ technisch (ohne Objektamen, nur die technischen IP-Adressen und Service-Daten) ◦ Einheitliche Änderungs-Reports über alle unterstützten Firewall-Module ◦ Compliance Reporting (individuell anpassbar, z.B. Auflistung aller Regeln mit Any-Objekten) ◦ Statistik-Report listet die Anzahl der Regeln und Objekte je Firewall-Management bzw. Gateway ◦ Reports können zu beliebigen Zeitpunkten automatisch generiert und in unterschiedlichen Formaten exportiert werden. • Workflow Modul: <ul style="list-style-type: none"> ◦ Komplet anpassbares Workflow Modul zur Beantragung von Änderungen am Firewall-Regelwerk ◦ Integriertes Ticket System ◦ Inklusive Genehmigung, Implementierung, Review ◦ API Schnittstelle zur Integration in ein Enterprise Ticket System wie ServiceNow • Re-Zertifizierung <ul style="list-style-type: none"> ◦ erlaubt es berechtigten Nutzern regelmäßig all existierenden Regeln zu sichten und entweder zu re-zertifizieren oder einen Lösch-Antrag zu stellen. ◦ Re-Zertifizierungsintervall ist konfigurierbar ◦ Der Re-Zertifizierungsworkflow kann nach Ihren Bedürfnissen angepasst werden. • Offene Schnittstellen, Integration und Automatisierung <ul style="list-style-type: none"> ◦ Da alle Daten mittels der beiden integrierten APIs abgefragt werden können, haben Sie maximale Flexibilität in der Automation. ◦ Bestehende (Idap-basierte) Verzeichnisdienste können zur Nutzersteuerung integriert werden.
	Derzeit verfügbar für folgende Betriebssysteme-	<ul style="list-style-type: none"> • Ubuntu >=18.04 LTS; empfohlene Plattform: Ubuntu 20.04 LTS Server • Debian >=10; empfohlene Plattform: Debian 11 Server)

Datenblatt Firewall Orchestrator v6

	me	
	Weitere Systemvoraussetzungen	Siehe Dokument „Firewall Orchestrator Systemvoraussetzungen“ unter https://fwo.cactus.de/wp-content/uploads/2021/07/fwo-systemanforderungen-v5.pdf
	Lizenz	Firewall Orchestrator wird gemäß der Apache 2 Lizenz (https://www.apache.org/licenses/LICENSE-2.0.html) bereitgestellt. Somit besteht keinerlei Gewährleistung oder Haftung des Wartungsdienstleister oder Anspruch auf Schadensersatz.
	Download	Firewall Orchestrator kann kostenfrei unter https://github.com/CactuseSecurity/firewall-orchestrator heruntergeladen werden.
Architektur	Kommunikationsbedarf	<p>Applikationszugriffe:</p> <ul style="list-style-type: none"> • Anwender → Frontend: 443/tcp • Produkt-intern: <ul style="list-style-type: none"> ◦ Frontend → Backend: API-Zugriff 9443/tcp, 8888/tcp ◦ Importer → Backend: API-Zugriff 9443/tcp, 8888/tcp, DB-Zugriff 5432/tcp ◦ Importer → Firewall-Systeme: Import 22/tcp (SSH), 443/tcp (API) ◦ Backend → LDAP/AD: 636/tcp (ldaps) • Zugriff Dritt-Systeme → Firewall Orchestrator API: 9443/tcp, 8888/tcp <p>Betriebssystem-Basis:</p> <ul style="list-style-type: none"> • alle Module ausgehend <ul style="list-style-type: none"> ◦ → NTP-Server: 123/udp ◦ debian/ubuntu Update Server • Installation/Upgrade (ansible host)Installations-System → Internet-Proxy: proxy-Port (oder direkter Internet-Zugriff)
	Vorhandene Module	<ul style="list-style-type: none"> • Importmodul • Frontend <ul style="list-style-type: none"> ◦ Reporting ◦ Report Scheduling ◦ Report Archivierung

Datenblatt Firewall Orchestrator v6

		<ul style="list-style-type: none"> ○ Rezertifizierung ○ Workflow – Beantragung von Firewall-Änderungen <ul style="list-style-type: none"> • Backend <ul style="list-style-type: none"> ○ GraphQL API ○ Datenbank ○ interner LDAP-Server ○ Middleware Server (Authentisierung, Autorisierung, Scheduling)
	Architekturvarianten	<ul style="list-style-type: none"> • Separierung der folgenden Module auf unterschiedliche Systeme z.B. zur Lastverteilung ist möglich: <ul style="list-style-type: none"> ○ Frontend ○ Backend ○ Importer • Der Aufbau mehrerer Instanzen der folgenden Module ist möglich: <ul style="list-style-type: none"> ○ Frontend ○ Importer (z. B. für sichere Netzwerkbereiche mit restriktiven Zugriffsregelungen)
Backend API	API Integration	Die Firewall Orchestrator GraphQL API dient dem automatisierten Zugriff auf die Firewall-Daten
Benutzer- verwaltung	Mandantenfähigkeit	Firewall Orchestrator unterstützt eine Mandantentrennung auf Firewall-Management- und Firewall-Gateway-Ebene.
	Integration Benutzer-Authentisierung	Folgende externe Enterprise Directory-Systeme können in Firewall Orchestrator integriert werden: <ul style="list-style-type: none"> • LDAP • Active Directory
	Role Based Access Control (RBAC)	Folgende Rollen dienen zur Zugriffssteuerung (sowohl Frontend als auch API): <ul style="list-style-type: none"> • reporter: Berechtigung zur mandantenbezogenen Report-Generierung • reporter-viewall: Berechtigung für unbeschränkte (mandantenübergreifende) Report-Generierung • auditor: Frontend-Benutzerberechtigung für vollen lesenden Zugriff • fw-admin: Berechtigungsrolle für Firewall-Administratoren • admin: Berechtigungsrolle für vollen administrativen Firewall Orchestrator Zugriff • recertifier: Berechtigungsrolle für Nutzer, die Firewall-Regeln rezertifizieren dürfen

Datenblatt Firewall Orchestrator v6

		<ul style="list-style-type: none"> • requester: Beantragung von Änderungen • approver: Prüfung und Genehmigung von Änderungsanträgen • implementer: Umsetzung beantragter Änderungen
Frontend	Sprachvarianten	<p>Die Oberfläche (Frontend) ist aktuell in den folgenden Sprachen (individuell je User einstellbar) vorhanden:</p> <ul style="list-style-type: none"> • Deutsch • Englisch
	Report Formate	<ul style="list-style-type: none"> • PDF • HTML • JSON
Importer	Unterstützte Firewall-Produkte	<ul style="list-style-type: none"> • 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) • Cisco Firepower Management Center 7ff • FortiGate 5ff – ssh access to FortiGate • FortiManager 6ff – https API access inklusive AutoDiscovery aller aktiven Domains/Devices • 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
Importer Limitierungen	Nicht unterstützte Feature	<ul style="list-style-type: none"> • Check Point Inline Layer (Roadmap 2023)