Modul /Thema	Funktion	Beschreibung
Allgemeines	Grundfunktionalität	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. • Reporting Funktionen: ◦ Einheitliche Regelwerk-Reports über alle unterstützten Firewall-Module ▪ aktuell ▪ historisch (zu einem beliebigen Zeitpunkt in der Vergangenheit) ▪ aufgelöst (alle verwendete Gruppen) ▪ technisch (ohne Objektnamen, nur die technischen IP-Adressen und Service-Daten) ▪ ungenutzte Regeln (aktuell nur Check Point) ◦ 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: ◦ Komplett anpassbares Workflow Modul zur Beantragung von Änderungen am Firewall-Regelwerk ◦ Integriertes Ticket System ◦ Inklusive Genehmigung, Implementierung, Review ◦ Integration sowohl des Rezertifizierungs- als auch des „ungenutzte Regeln“ Reportings zur automatischen Beantragung von Regellöschungen ◦ API Schnittstelle zur Integration in ein Enterprise Ticket System wie ServiceNow • Re-Zertifizierung ◦ 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. • Compliance Matrix ◦ Prüfung von (beantragten) Regeln gegen eine vom Unternehmen definierbare IP-basierte Zonenmatrix

		• Offene Schnittstellen, Integration und Automatisierung ◦ Da alle Daten mittels der beiden integrierten APIs abgefragt werden können, haben Sie maximale Flexibilität in der Automation. ◦ Bestehende (ldap-basierte) Verzeichnisdienste können zur Nutzersteuerung integriert werden.
	Derzeit verfügbar für folgende Betriebssysteme	• Ubuntu >=18.04 LTS; empfohlene Plattform: Ubuntu 22.04 LTS Server • Debian >=10; empfohlene Plattform: Debian 11 Server)
	Weitere Systemvoraussetzungen	Siehe Dokument „Firewall Orchestrator Systemvoraussetzungen“ unter ***https://fwo.cactus.de/dokumente/***
	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 Wartungsdiensteister oder Anspruch auf Schadensersatz.
	Download	Firewall Orchestrator kann kostenfrei unter ***https://github.com/CactuseSecurity/firewall-orchestrator*** heruntergeladen werden.
Architektur	Kommunikationsbedarf	Applikationszugriffe: • Anwender → Frontend: 443/tcp • Produkt-intern: ◦ 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 Betriebssystem-Basis: • alle Module ausgehend ◦ → NTP-Server: 123/udp ◦ debian/ubuntu Update Server • Installation/Upgrade (ansible host)Installations-System → Internet-Proxy: proxy-Port (oder direkter Internet-Zugriff

	Vorhandene Module	• Importmodul
		
		• Frontend
		  ◦ Reporting
		  ◦ Report Scheduling
		  ◦ Report Archivierung
		  ◦ Rezertifizierung
		  ◦ Workflow – Beantragung von Firewall-Änderungen
		
		• Backend
		  ◦ GraphQL API
		  ◦ Datenbank
		  ◦ interner LDAP-Server
		  ◦ Middleware Server (Authentisierung, Autorisierung, Scheduling)

	Architektur-varianten	• Separierung der folgenden Module auf unterschiedliche Systeme z.B. zur Lastverteilung ist möglich:
		  ◦ Frontend
		  ◦ Backend
		  ◦ Importer
		
		• Der Aufbau mehrerer Instanzen der folgenden Module ist möglich:
		  ◦ 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	Mandanten-fähigkeit	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: • LDAP • Active Directory

	Role Based Access Control (RBAC)	Folgende Rollen dienen zur Zugriffssteuerung (sowohl Frontend als auch API): • 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 • requester: Beantragung von Änderungen • approver: Prüfung und Genehmigung von Änderungsanträgen • implementer: Umsetzung beantragter Änderungen
Frontend	Sprachvarianten	Die Oberfläche (Frontend) ist aktuell in den folgenden Sprachen (individuell je User einstellbar) vorhanden: • Deutsch • Englisch
	Report Formate	• PDF • HTML • JSON
Importer	Unterstützte Firewall-Produkte	• 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 Zugriff auf FortiGates • FortiManager 6ff – https API access inklusive AutoDiscovery aller aktiven 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 Limitierungen	Nicht unterstützte Feature	• Check Point Inline Layer: eingeschränkte (Reporting-)Funktionalität