Collax Security Gateway

Profischutz für Ihr Netzwerk

Informationssicherheit für Ihr Next-Generation-Netzwerk

Das Collax Security Gateway ist eine Unified-Threat-Management-Lösung (UTM). Es fasst alle Sicherheitsfunktionen in einem Produkt zusammen. Dabei schützt es gleichermaßen die Anwendenden, ihr Netzwerk und ihre Server vor Bedrohungen aus dem Internet.

Sicheres und produktives Arbeiten im Netz

Dank hierarchisch aufgebauter Filter wird Ihr Unternehmen zuverlässig vor Spam und Viren geschützt. Und das effizient. Auch die Nutzung des Internets kann mit dieser Lösung einfach und schnell abgesichert werden. So können Webseiten entweder komplett gesperrt oder die Zugriffsrechte nach Benutzenden oder Zeitplänen eingeschränkt werden. Downloads aus dem Internet können mit diesem Collax Security Gateway einfach und sicher begrenzt werden, um potentielle Gefahren zu minimieren. Die Möglichkeit zum Schutz des verschlüsselten Datenverkehrs (SSL-Interception) rundet das Sicherheitskonzept ab.

Next-Generation-Firewall

Das Collax Security Gateway verfügt über eine komplett ausgestattete Stateful Inspection Firewall. Die Firewall-Regeln lassen sich, dank Gruppierungen, grafischer Darstellung und Suchfunktionen, effizient administrieren. Eine Ländersperre kann Zugriffe aus unerwünschten Ländern verhindern.

Anbindung von Filialen und externen Mitarbeitenden

Um Filialen und mobile Mitarbeitende sicher an das eigene Firmennetz anzuschließen, kann VPN (Virtual Private Networking) als Kommunikationskanal verwendet werden. Neben dem VPN nach dem IPsec-Standard und per WireGuard zur Netzwerkanbindung, stellt das Collax Security Gateway auch SSL-VPN zur Verfügung. WireGuard und IPsec-VPN sind die erste Wahl bei der sicheren Standortvernetzung.

Für granulare Zugangsberechtigungen von Benutzenden bietet Collax als Lösung SSL-VPN, was ohne zusätzliche Installation und plattformunabhängig einen gesicherten Zugang für die Anwendenden bereitstellt.

Optimale Nutzung der Netzwerke

Mit dem Collax Security Gateway bieten wir Ihnen unterschiedliche Methoden der optimalen Netzwerknutzung an. So bietet der Brute-Force-Schutz Möglichkeiten für die Angriffserkennung bzw. -abwehr. Moderne Netzwerktechniken wie Link-Failover und Traffic Shaping stellen sicher, dass Ihre Anwendungen auch unter hoher Netzwerkbelastung optimal genutzt werden können. Das Policy Routing teilt dabei den Datenverkehr nach Ihren Wünschen optimal auf die vorhandene Infrastruktur auf. Vom Unternehmens-Wiki bis zu einem ERP können Anwendungen für Ihre Mitarbeitenden zugänglich gemacht werden.

Vorteile

- Zuverlässiger Unternehmensschutz durch gehärtetes Firewall-System
- Abgesicherter Web-Zugriff für Anwendende
- Saubere E-Mail-Postfächer durch E-Mail-Spamfilter
- Inklusive Virenfilter für E-Mail und Web-Traffic
- Bequemer, sicherer Fernzugriff
- Optimierte Traffic Policies für Netzwerkverkehr
- Effiziente Wartung und Überwachung für Administrierende
- Moderne GUI

Systemvoraussetzungen

Mindestanforderungen:

- 64Bit X86-Prozessor
- USB-Stick oder CD-/DVD-ROM-Laufwerk, bootfähig
- Festplatte ab 16 GB, mit V72 30 GB
- Min. 2x 1GB Netzwerkschnittstellen
- RAM min. 1024 MB
- Nur für die Installation: VGA-fähige Grafikkarte

Collax GmbH · Tel: +49 (0) 761 - 55 72 10-0 · info@collax.com · www.collax.com

Technische Details

Stateful Inspection Firewall
Stateful Inspection Paketfilter · Application Layer Firewall · Application Proxy für SMTP · DNS · NTP · VoIP-Support (SIP, RTP) · Connection Tracking · Denial-of-Service Protection · grafisches Regelmanagement · Schutz vor Brute Force Attacken · Ländersperre

VPN
VPN für Mobilgeräte - Android, iOS, Windows · IPSec mit X.509 Zertifikaten mit IKEv1 und IKEv2 · WireGuard (Netz-zu-Netz) · L2TP · VPN Wizard · Große Interoperabilität · Zertifikatsverwaltung und CRL-Management · CA für PKI · SSL-VPN · DynVPN · Proposal nach BSI-Empfehlung

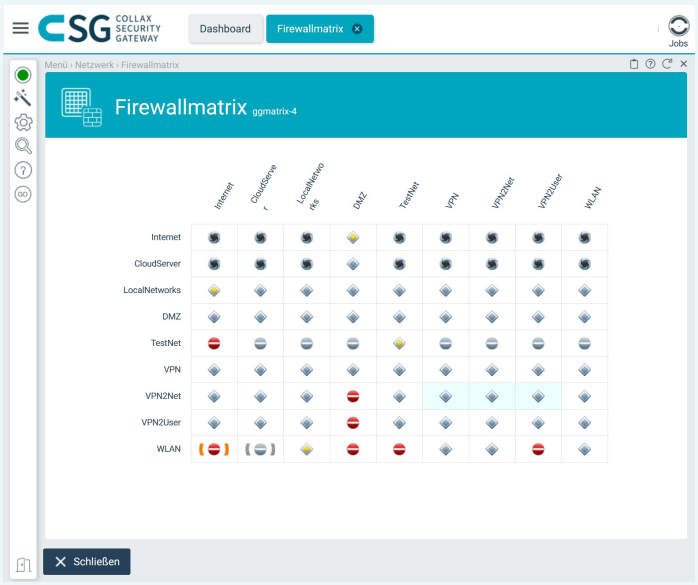
Web-Browsing Security
Application Proxy und Virenfilterung für Web Traffic · Web-Blocker URL-Filtering · Web Traffic SSL Interception · individuelle Black-, White-Listen · Active Content Filter · Anti-Phishing · Regelung nach Gruppen und Zeit für Application Proxy · Statistik und Berichte · benutzerbasierte Auswertung (optional)

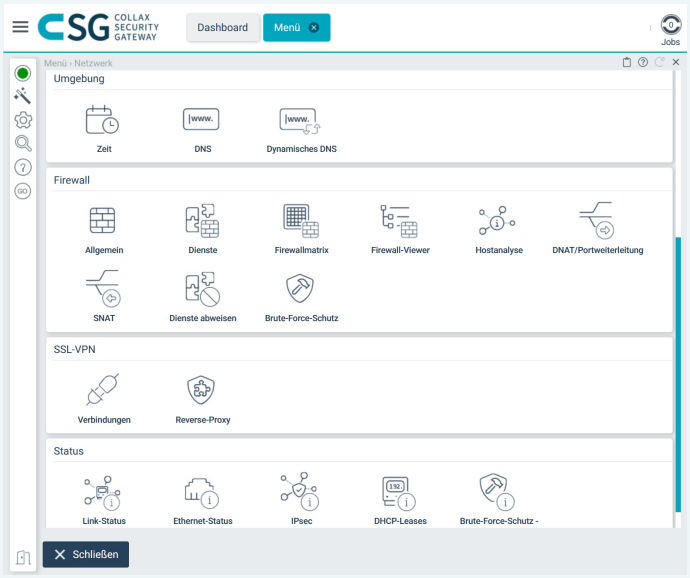
E-Mail Security
Live Spam Protection · E-Mail Greylisting · Cloud-basierter Razor-Check · Reputation-Filter · DNS-Cloud basierte DKIM und SPF-Checks · Realtime Blackhole List & DNS Blacklists · Individuelle Black- und White-Listen · Zero Day Protection (Heuristik) · Trainierbarer Bayes-Filter · DNS Blacklists · Image und PDF-Filter · Teergruben-Emulation · Header Filter und Anhangsfilter · ClamAV Virenschutz integriert.

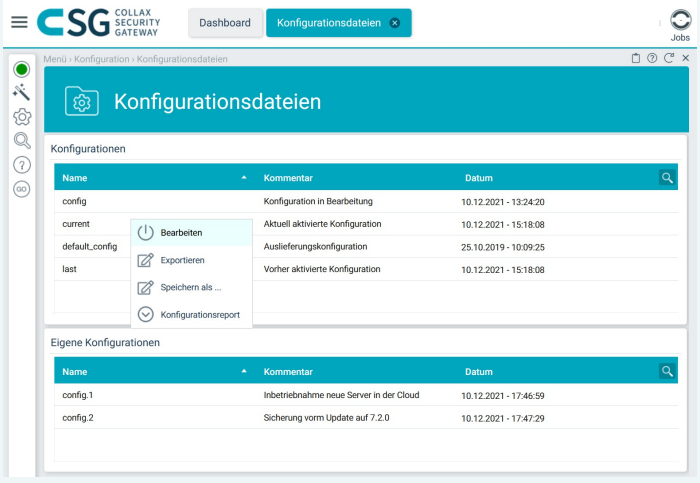
Networking
Link- und Interface Failover · Traffic Shaping · Policy Routing · Tagged VLAN · DMZ Support · Virtual Switching · Bridging · Performance und redundante Link aggregation/Teaming SNAT · DNAT · Masquerading · Port-Forwarding · MAC-Adressenüberwachung

Gehärtetes Betriebssystem – Effizientes Management
Deterministisches System · Binär-Dateien mit Exploit-Schutz · Passwortrichtlinien · Zentrale Benutzer- und Gruppen-verwaltung per LDAP · LDAP Proxy · LDAP-Replik oder Kerberos · Windows™ ActiveDirectory Integration · SSO · Fernadministration HTTPS · Update-Management für System-, Virus-, Spam- und URL-Filter · Delegierbare Administration · Integrierte Datensicherung · USV-Unterstützung

Mögliche Erweiterungen
Avira Antivir · Surf Protection powered by Cobion







Collax GmbH · Tel: +49 (0) 761 - 55 72 10-0 · info@collax.com · www.collax.com