

## „Das Ziel ist der Weg“

Mario Eichelberger T: 030 96 20 54 95 www.SCS-Concept.de  
 Rotkamp 39 F: 030 96 20 44 12 info@SCS-Concept.de  
 13053 Berlin

# Collax Security Gateway

Der Rund-um-Schutz  
Security "out of a box"

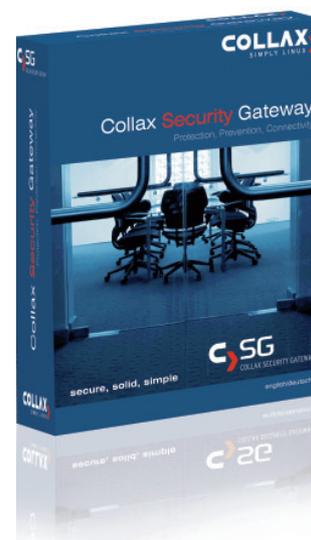
## Highlights

- › Alle Technologien zur Gefahrenabwehr zusammengefasst (UTM)
- › Basierend auf führender Sicherheitstechnologie
- › Multi-Level Firewall: Kombiniert Stateful und Application Firewall
- › Firewall-Rechte nach Applikation, Benutzer und Betriebssystem
- › Schutz vor Exploits durch P2P- oder IM-Anwendungen
- › Hohe Flexibilität: Benutzerrechte können sowohl standortabhängig als auch unabhängig sein.
- › Einheitliche, einfache Benutzeroberfläche
- › Schnelle und einfache Konfiguration mithilfe von Assistenten
- › SSL-VPN und IPSec VPN sinnvoll kombiniert
- › Hocheffektive mehrstufige Spam-Erkennung
- › Gateway-Virens Scanner für Mail, Webtraffic und Filetransfer
- › Integrierbar in LDAP, Active Directory Und NT Domain Controller
- › Stündliche Aktualisierungen der Virensignaturen
- › Kontinuierlicher Update-Service für alle Sicherheitsdienste
- › Investitionsschutz durch Update- und Upgrade-Service

Die Unified Threat Management (UTM)-Lösung, schützt Ihr Netzwerk vor allen Gefahren aus dem Internet. Die Schutzmechanismen beginnen bei sehr wirkungsvollen Anti-Spam- und Anti-Virus-Verfahren des E-Mail Verkehrs. Spam, Viren und Trojaner haben keine Chance! Einbruchversuche in Ihr Netzwerk erkennt das System durch Intrusion Detection/Prevention und vereitelt diese. Darüber hinaus stellt das System Ihren Außendienstmitarbeitern oder anderen Niederlassungen mittels Virtual-Private-Networking sichere Zugangsmöglichkeiten zu Ihrem Netzwerk zur Verfügung. Unter anderem mittels IPSEC oder dem „client-lose“ SSL. Mit der neuartigen, mehrstufigen Firewall sind Sie in der Lage Applikationen den Zugang zu gewissen Netzen oder dem Internet zu verbieten – abhängig von Benutzern oder Benutzergruppen.

### Schutz auf höchster Ebene: Multi-Level Firewall

Mit der Multi-Level Firewall ist es erstmals möglich, PC's nicht nur über IP-Adressen in die Firewall-Regeln einzubinden, sondern dies in Abhängigkeit von Benutzern, Betriebssystemen aber auch Anwendungen (z.B. Skype) zu filtern. Somit werden nicht nur Sicherheit und Kontrolle im Unternehmensnetzwerk verbessert, sondern Sicherheitsbestimmungen können sehr viel zielgerichteter und schneller umgesetzt werden. Ein Umgehen der bisherigen Firewall-Regeln durch das „Missbrauchen“ von Port 80 (http) oder das zufällige Wechseln von Ports zur Datenübertragung wird durch die Multi-Level Firewall zuverlässig blockiert. Ein großer Vorteil ergibt sich zudem aus der vom Standort unabhängigen Anwendung des Regelwerks und der Unterstützung des Terminal-Servers. Hierbei können für jeden Benutzer desselben Systems unterschiedliche Firewall-Regeln angewendet werden.



### Der richtige Fernzugang für jeden Zweck

Das **Collax Security Gateway** stellt neben anderen, die beiden wichtigsten VPN- Technologien IPSec- und SSL-VPN zur Verfügung. Dadurch können Unternehmen beide Technologien, je nach Anwendung, auf einem einzelnen Gateway nutzen. IPSec-VPN kommt für die Standortvernetzung oder für „Power-User“ zum Einsatz, die einen netzwerkweiten Zugang benötigen. Für die Anbindung von mobilen Geräten, Außendienstmitarbeitern oder Heimarbeitsplätzen ist die installationsfreie und clientlose Nutzung von SSL-VPN optimal.



„Das Ziel ist der Weg“

Mario Eichelberger T: 030 96 20 54 95 www.SCS-Concept.de  
Rotkamp 39 F: 030 96 20 44 12 info@SCS-Concept.de  
13053 Berlin

**Technische Highlights**

**Multi-Level-Firewall**

Firewall-Rechte nach Benutzer, Applikation, Betriebssystem | Stateful Inspection | VOIP-Support (SIP, RTP) | Connection Tracking | Malformed/Unclean Packet Filter | Denial-of-Service Protection | grafische Netzwerkmatrix

**VPN**

IPSec mit X.509 oder PSK | PPTP | L2TP | DynVPN | CA für PKI | VPN Assistent | Zertifikatsverwaltung und CRL-Management | SSL-VPN

**Filtering**

Viren-Schutz für E-Mail und Web | Web-Blocker URL-Filtering | Black-/Whitelist URL-Filtering | Anti-Phishing | Keyword Content Filtering | Active Content Filter | extended E-Mail-Filter | Application Proxy HTTP, SMTP, DNS, NTP, SOCKS

**Spam**

Live Spam Protection | E-Mail-Greylisting | Razor-Check | Reputation-Filter | SPF-Check | definierbare Black-/Whitelists | trainierbarer Bayes-Filter | DNS Blacklists | Image- und PDF-Filter | Teergruben-Emulation

**IDS/IPS**

Intrusion Detection | Intrusion Prevention | dynamic Blocking | powerfull, proactive Protection | stand-alone IDS-Fähigkeit im Stealth-Modus

**Networking**

Link/Interface-Failover | zeitgesteuerter Restart dynamischer Verbindungen | Traffic Shaping | tagged VLAN | DMZ Support | Bridging | NAT/Masquerading/Port-Forwarding | MAC-Adressenüberwachung

**Einfache Konfiguration**

Zentrale Benutzer- und Gruppenverwaltung | Netzwerk- und Hostmanagement | Fernadministration HTTPS | Update-Management für System, Virus-, Spam- und URL-Filter | Active Directory, NT-Domäne oder NTLM | LDAP, LDAP-Proxy, LDAP-Replik oder Kerberos | delegierbare Administration | integrierte Datensicherung | USV-Unterstützung

**Noch sicherer durch einfache Konfiguration**

Eine Firewall kann nur so gut arbeiten, wie sie selbst konfiguriert ist. Denn durch fehlerhafte Anwendung erhalten Hacker möglicherweise einen Zugang in Ihr Netzwerk. Dank der von Collax eingesetzten Firewall-Matrix reduzieren sich solche Konfigurationsfehler auf ein Minimum. Die Konfiguration ist schnell durchgeführt, denn Assistenten unterstützen Sie Schritt für Schritt bei der Einrichtung Ihrer Sicherheitslösung. Die Wartung dieses Systems ist ebenfalls denkbar einfach. Mit einem Mausklick laden Sie alle Aktualisierungen vom Collax Update Server herunter. Selbstverständlich werden die Virensignaturen automatisch stündlich aktualisiert. Das **Collax Security Gateway** ist Ihr Spezialist für das Unified Threat Management, also eine umfassende Lösung zum Schutz gegen alle externen Gefahren. Ihre E-Mails werden auf Viren und Trojaner geprüft, die Zahl der Spam-Mails erheblich reduziert und der Zugang zu fremden Websites abgesichert.



Transparent und sicher: Die Firewall-Konfiguration in der grafischen Matrix ist einfach und übersichtlich konfigurierbar. Sie tut immer das Richtige und das Sichere. Der Collax Security Gateway steht auch als Appliance (Komplettsystem inkl. Hardware) zur Verfügung.

**Systemvoraussetzungen**

- Intel Pentium oder kompatibel
- Bootfähiges CD-ROM-Laufwerk
- Festplatte: 8 GB
- 2 Netzwerkschnittstellen
- Speicher: 512 MB
- VGA-fähige Grafikkarte (nur während der Installation)

Sie finden die aktuelle Hardware-Kompatibilitätsliste auf [www.collax.com](http://www.collax.com).

Das Collax Security Gateway kann auch als Appliance erworben werden. Für weitere Details kontaktieren Sie bitte das Collax Sales-Team.

„Das Ziel ist der Weg“

Mario Eichelberger T: 030 96 20 54 95 www.SCS-Concept.de  
Rotkamp 39 F: 030 96 20 44 12 info@SCS-Concept.de  
13053 Berlin

**Sie haben Fragen? Kontaktieren Sie uns gerne:**

SCS Concept  
Rotkamp 39  
13053 Berlin  
Telefon: +49 (0)30 96205497  
Fax: +49 (0)30 96204412  
([Office@SCS-Concept.de](mailto:Office@SCS-Concept.de))  
<http://SCS-Concept.de>