

Der Body-Guard für Ihr Unternehmens-Netzwerk

Jeder kennt sie: Hacker-Attacken, Trojaner, Würmer, Viren, Massenwerbe-Mails (Spam) und Trickbetrügereien (Phishing) aus dem Internet.

Alles Plagegeister, die nicht nur die Sicherheit ihres IT-Netzwerkes bedrohen, sondern auch Ihr Unternehmen selbst. Sie löschen Dateien, zum Teil ganze Festplatten. Sie lassen Serverdienste abstürzen und kapern den ganzen Server, um von dort aus Angriffe auf andere Rechner zu starten oder den Server als Spamschleuder zu missbrauchen.

Wie viel beruhigter würden Sie schlafen, wenn sie wüssten, dass ein zuverlässiger Body-Guard den Eingang zu Ihrem Unternehmens-Netzwerk bewacht? Und allen schädlichen Plagegeister schon am Eingangstor zu Ihrer Firmen-IT den Eintritt verweigert?

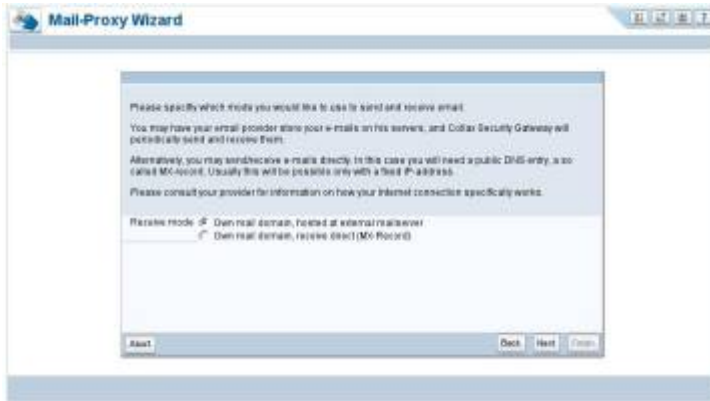
Das fundierte technologische Know-how von Collax im Bereich Sicherheit garantiert schon seit Jahren sichere IT-Netzwerke. Das Collax Security Gateway ist eine Lösung für das umfassende, so genannte Unified-Threat-Management (UTM) – ein Sicherheitspaket, das mit der besten auf dem Markt verfügbaren Linux und Open Source Software Ihr gesamtes Netzwerk gegen alle Bedrohungen aus dem Internet schützt.



Simply Linux - Startklar mit wenigen Mausklicks

Damit Sie mit dem Collax Security Gateway sofort allen Angriffen aus dem Internet trotzen können, haben wir die Konfiguration sehr einfach gestaltet. Nicht die Intelligenz der Hacker, sondern ungewollte Hintertürchen in der Konfiguration öffnen ungebetenen Gästen meist den Zugang zum Firmen-Netzwerk.

Dank der von Collax entwickelten Firewall-Matrix lassen sich solche Konfigurationsfehler auf ein Minimum reduzieren. Die Bedienung des Collax Security Gateways über Kontextmenüs und Icons ermöglicht außerdem eine schnelle und benutzerfreundliche Konfiguration. Assistenten unterstützen Sie Schritt für Schritt bei der Einrichtung der Sicherheits-Lösung. Diese kleinen Helfer ermöglichen es sogar Netzwerk-Laien, die Grundeinstellungen für die Nutzung des Internets, Intranets, VPNs, Web-Proxys etc. vorzunehmen.



Mit wenigen Mausklicks haben Sie auf diese Weise die Konfiguration der Sicherheitslösung vorgenommen – und das alles ohne Linux Know-how oder fundierte Netzwerk- Kenntnisse.

Und auch die Wartung des Collax Security Gateway ist absolut einfach – klicken Sie mit der Maus auf den Knopf „Update“ und schon werden die Updates und Patches vom Collax Update-Sever herunter geladen und Sie sind wieder gegen alle Angriffe gewappnet.

Sicherheit von Collax – Simply no limits!

Das Collax Security Gateway können Sie ohne jegliches Linux Know-how bedienen. Durch eine eigens entwickelte, anwenderfreundliche Benutzeroberfläche setzen wir unser Credo ‚Simply Linux‘ um. Unter dieser Oberfläche arbeiten die von uns sorgfältig ausgewählten und getesteten „Best-of-breed“ Linux und Open Source Komponenten. So ist es für Sie möglich, die Power von Linux und Open Source auch ohne Linux Know-how zu nutzen.

Die Vorteile einer Unified Threat Management-Lösung

Der Vorteile einer Unified Threat Management-Lösung liegt auf der Hand.

In einem einzigen Produkt sind die besten auf dem Markt verfügbaren („Best-of-breed“) Software-Komponenten gegen Bedrohungen aus dem Internet wie Hacker-Attacken, Viren, Würmer, Trojaner, Spam, Phishing, Spyware etc. enthalten. Sie alle sind auf einer Hardware-Plattform verfügbar und über eine einheitliche Benutzeroberfläche zu bedienen.

All-in-one UTM-Lösungen sind deshalb kostengünstiger als herkömmliche Sicherheits-Lösungen, einfacher zu installieren und zu verwalten und können darüber hinaus schneller an neu auftauchende Sicherheitsbedrohungen angepasst werden.

Unified Threat Management (UTM) von Collax

Als UTM-Lösung übernimmt das Collax Security Gateway Web-, E-Mail und Netzwerk-Sicherheit. Alle Funktionalitäten sind dabei auf einer Verwaltungsplattform verfügbar. Der Vorteil: Anwendungsflexibilität, denn Sie können entweder alle im Collax Security Gateway enthaltenen Sicherheitsdienste nutzen oder das Produkt für eine spezielle Aufgabe einsetzen. Darüber hinaus überwacht das Collax Security Gateway mit einem Traffic Management, bestehend aus Traffic Shaping, Link Fail-over und MultiWAN, den gesamten Datenverkehr.

10 gute Gründe für das Collax Security Gateway

1. Schützt als All-in-one Lösung vor allen Bedrohungen aus dem Internet
2. Sicherheit auf Linux und Open Source Basis
3. Ohne Linux Know-how bedienbar
4. Einheitliche einfache Benutzeroberfläche
5. Schnelle und effiziente Konfiguration durch Assistenten
6. Stündliche Aktualisierung der Virensignaturen
7. Ein Update für alle Sicherheitsdienste
8. Integriert sich in alle bestehenden Netze
9. Kostentransparenz durch Subscription
10. Investitionsschutz (Update- und Upgrade-Service)

Was ist eine Unified Threat Management-Lösung?

Den Begriff Unified Threat Management (UTM) hat Charles Kolodgy von der International Data Corporation (IDC) 2004 geprägt. Die Idee: Eine einzige, so genannte All-in-one Sicherheits-Lösung, die das Firmen-Netzwerk gegen alle Bedrohungen aus dem Internet schützt. Die rudimentärste Form einer Unified Threat Management-Lösung beinhaltet eine Firewall, VPN, IDP und eine Anti-Virus-Lösung.

Unified Threat Management im Detail

Firewall:

- Stateful Packet Filtering
- VPN Verbindungen (IPSec / L2TP / PPTP)
- Malformed/Unclean Packet Filter
- Denial-of-Service Protection
- SIP und RTP Support

IDS/IPS

- Intrusion Detection
- Intrusion Prevention
- Dynamic Blocking
- Powerful, proactive Protection
- Standalone IDS Fähigkeit im Stealth Mode

Filtering:

- Viren-Schutz Mail und Web
- Web-Blocker URL Filtering
- Black/Whitelist URL Filtering
- Anti-Phishing
- Keyword Content Filtering
- Active Content Filter
- Live Spam-Protection
- E-Mail Greylisting
- Extended Mail Filter
- Application Proxy HTTP, SMTP, DNS, NTP, SOCKS
- NTLM support für HTTP-Proxy

Managing & Configuration Setup

- Einfaches Setup Management
- VPN Wizard
- Graphisches Real-Time Monitoring
- Sicheres, flexibles Logging, Benachrichtigungen und Reporting
- Umfangreiche Statistiken
- Diagnose Tools
- Sichere Fernwartung per https
- Authentifizierung per ADS, PDC, NTLM, LDAP, Kerberos
- Firewall-Matrix
- Datensicherung und Wiederherstellung
- Zertifikats Verwaltung X.509 (inkl. CRL)
- Live-Log Views
- Online Software Updates für das System, Virus-, Spam-, Url-Filter
- Zentrale Benutzer- und Gruppenverwaltung
- Delegierbare Administration
- Netzwerk und Host Management
- Flexibles Konfigurations-Management
- USV Unterstützung

Networking:

- Internet-Zugang per Ethernet, DSL, ISDN, Kabel- und analog Modem
- Multi-WAN (redundanter Internet-Zugang)
- Link/Interface Failover
- Zeitgesteuerter Verbindungsaufbau für dynamische Verbindungen
- Traffic Shaping
- SIP Protocol Support
- DMZ Support
- tagged VLAN
- Bridging
- NAT/Masquerading/Port-Fowarding
- MAC-Adressen Überwachung