Collax Security Gateway

Complete threat protection system Security out-of-the-box

Highlights

- All technologies combined into one security solution (UTM)
- Based on leading security technologies
- Multi-level Firewall that combines stateful and application firewalling, user rights and operating system identification
- Protection from P2P or IM application threats
- High flexibility: User rights can be location-dependant or independent as required
- Simple and Standardized user interface
- Simple and rapid configuration with wizards
- SSL-VPN and IPSec VPN capabilities
- Highly precise multi-level Spam filter
- Gateway virus scanner for E-Mail, Web traffic and file transfer
- Integration into LDAP, Active Directory and NT Domain Controllers
- Hourly updates of virus signatures
- Continuous update service for all security components
- Investment protection with Update and Upgrade services

IT security is not a new topic and to protect your business against threats coming from the Internet everyone knows that they, typically, need at least: Anti-Virus, Anti-Spam, Firewall and various network security/control systems.

The **Collax Security Gateway** is a Unified Threat Management (UTM) solution that bring together all of the above and much more to actively protect your business, all in one complete out-of-the-box package (either appliance of software).

Apart from Anti-Virus, Anti-Spam capabilities the **Collax Security Gateway** contains complete web surfing security for your staff; advanced networking features that both maintain the integrity of your network and optimize it too; both IPSec and SSL VPN technology; a state-of-the-art firewalling solution and a full intrusion detection and prevention solution to finish off this total gateway security solution.

Protection at the highest level: Multi-level Firewall

The **Collax Multi-Level Firewall** component takes firewalling to a new level. It uses a unique method of securing users, networks, their traffic and the applications therein. Traditional firewalls only check for IP address and port. The **Collax Multi-Level Firewall** checks the IP address and ports, but also identifies the actual user, the application and the operating system being used.

Example: Allow “User A”, using “App. B”, on “OS C” to access “Server D” from the internal LAN.

Such rules are more secure, more relevant and more pertinent to business requirements. One last benefit is that rules can be user based and location independent. What would normally take many rules can now be done with a single rule in the **Collax Security Gateway**.

The right tool for the right job: VPN

There are two main forms of VPN (Virtual Private Network) technology: IPSec and SSL-VPN. The **Collax Security Gateway** comes with both!

VPNs are used to secure/encrypt communications between a remote location and your company network. Once connected the user experience is as if they were on your local network. The situation usually determines which kind of VPN should be used. If you wish to securely link two locations (e.g. branch offices) it is best to use IPSec based VPNs. If you wish to connect a mobile device or remote user then the SSL VPN would be a preferred solution.

The SSL-VPN is a clientless VPN solution where the user simply connects, with a browser, to a published internet location. They then simply authenticate and are then granted limited or general access depending on their rights.

Technical Highlights

Multi-Level Firewall
Firewall rules based in user, application, Operating system | Stateful Inspection | VOIP Support (SIP, RTP) | Connection Tracking | Malformed/Unclean Packet Filter | Denial of Service Protection | graphical network matrix

VPN
IPSec (X.509 or PSK) | PPTP | L2TP | DynVPN | CA for PKI | VPN Assistant | Certificate and CRL Management | SSLVPN

Filtering
Virus protection for E-Mail and Web | Web blocker URL Filtering | Black/ Whitelist URL Filtering | AntiPhishing | Keyword content Filtering | Active content filter | extended email filters | Application Proxy HTTP, SMTP, DNS, NTP, SOCKS

Spam
Live Spam Protection | Email Greylisting | Razor Check | Reputation Filter | SPF Check | definable Black/ Whitelists | more trainable Bayes Filter | DNS Blacklists | Image and PDF filter | Tarpit emulation

IDS/IPS
Intrusion Detection | Intrusion Prevention | dynamic Blocking | powerful proactive protection | stand alone IDS also in the stealth mode

Networking
Link/Interface Failover | Time-scheduled restarts of connections | Traffic Shaping | tagged VLAN | DMZ support | Bridging | NAT/Masquerading/Port Forwarding | MAC address monitoring

Server management
Central Group administration | Network and Host management | Remote administration HTTPS | Update management for system, Virus, Spam and URL filter | Active Directory, NT Domain or NTLM | LDAP, LDAP-Proxy, LDAP-Replik or Kerberos | Administration delegation | integrated backup | USV Support

Security through simple and clear configuration

A security solution is only as good as the rules it is given. One incorrect rule or oversight and your security become ineffective or even useless.

The **Collax Security Gateway** firewall uses a new concept in Firewall administration called the Firewall Matrix. The Firewall Matrix is an interactive graphical representation of your rules. In a glance you can see the rules and how they affect all your networks.

The Firewall Matrix results in rapid rule building, clearer understanding of rules and less chance of errors and security holes.

The other components of the **Collax Security Gateway** are either driven though wizards or direct configuration. The result is a flexible but clear solution that inherently reduces errors and vulnerabilities.

Finally the **Collax Security Gateway** is kept up-to-date with a single click download mechanism, while the engine, Virus and Spam rules are automatically updates on an hourly basis.

Transparent and secure: The firewall configuration in the graphical matrix is easy and clear to configure. The firewall always makes the right and most secure decision.Our Collax Security Gateway is also available as an appliance (total package of hard- and software).

System Requirements

- Intel Pentium or compatible
- Bootable CD-ROM drive
- Hard drive: 8 GB
- 2 network interfaces
- User memory: 512 MB
- For installation: VGA graphic card (only while installation)

You can find a complete hardware compatibility list on: www.collax.com.

Also the Collax Security Gateway can be purchased as a hardware appliance. Please contact Collax for more details.

You have more questions? Feel free to contact us at:

Collax GmbH
Gutenbergstraße 1
85737 Ismaning Germany
Telephone: +49 (0) 89-99 01 57-0
Fax: +49 (0) 89-99 01 57-11
0800 4265529 (Free in Germany)
www.collax.com sales@collax.com