

Informationsblatt

Modul Collax Net Security

Netzwerkinfrastruktur und Netzwerksicherheit

Netzwerk

Das Modul Collax Net Security vereint alle wichtigen Sicherheitsfunktionen und Netzwerkfunktionalitäten, die von einem Gateway erwartet werden können. Gerade am Gateway sind ausgefeilte Routing-Mechanismen, hohe Sicherheitsstandards und moderne Fernzugriffsmethoden gefordert. Aber auch innerhalb des Netzwerks steigen die Anforderungen, sowie neue Technologien wie Voice over IP (VoIP) stellen höhere Anforderungen an die Netzwerkinfrastruktur.

Sicherheit

Eine weitere entscheidene Säule für Ihr Netzwerk sind die im Modul Collax Net Security eingebauten Sicherheitsmechanismen. Viele sind unsichtbar und verhindern im Hintergrund Angriffsversuche und schützen vor unberechtigten Zugriffen. Eine voll ausgestattete Firewall erlaubt die aktive Sicherung Ihres Netzes. Die Administration über die innovative Firewall-Matrix geht nicht nur leicht von der Hand, sie reduziert auch das Risiko von gefährlichen Fehlkonfigurationen auf ein Minimum. Abgerundet wird das umfassende Sicherheitspaket durch das führende Intrusion Detection und Prevention System ‚snort‘. Auch hier sorgt die einfache Konfiguration für eine effektive Justierung der Filter gegen Eindringversuche in Ihr Netzwerk.

Die Features

Netzwerk

Um die Verfügbarkeit des Internet-Zugangs zu erhöhen, können für den Ernstfall alternative Netzwerkverbindungen angelegt werden. Eine zusätzliche **ISDN**-Verbindung, wird automatisch aktiviert, sobald die **DSL**-Hauptverbindung nicht mehr verfügbar ist. Durch das Collax **Link-Fail-Over**-Konzept bleiben Internet- oder generell Netzwerkverbindungen automatisch aufrecht erhalten. Auch **VPN**-Tunnel, **Router**-oder **Analog-Modem**-Verbindungen können ausfallsicher aufgebaut werden.

Für komplexere Netzwerkstrukturen stehen zusätzlich zu **Masquerading** bzw. **NAT** die Funktionen **Source-** und **Destination-NAT**, sowie **Source-** und **Destination-Netmap** zur Verfügung. Diese Funktionen bieten die erforderliche Flexibilität, um komplexe Netzwerkadress-Übersetzungen einfach abzubilden.

Für die Internet-Anbindung und die Verbindung zwischen Standorten stehen alle gängigen Zugangsarten stehen für eine Netzwerkanbindung zur Verfügung: **Analog-Modem**, **Router**, **ISDN**, **DSL** via **PPPoE** und **PPTP** oder **IP-Tunnel (GRE)**.

Durch den **Link Aktivitätsfilter** für dynamische Verbindungen mit Analog-Modem-, ISDN- und DSL-Zugängen werden Verbindungskosten reduziert. Ungewollter Internet-Traffic wird dadurch ausgefiltert und verhindert. Die **automatische Trennung** sorgt ebenso für eine Kostenreduzierung bei nach Zeit abgerechneten Internet-Tarifen.

Routing

Die Einrichtung einer **DMZ** mit mehreren unabhängigen Netzwerken kann sehr einfach durch erweiterte Routing-Funktionalität eingerichtet werden. Einzelne Dienste oder IP-Adressen können über **NAT** und **Netmap** auch via **Proxy-ARP** und **Port Forwarding** sicher weitergeleitet werden.

Mit dem **Bandbreiten-Management** oder auch **Traffic Shaping** lassen sich Bandbreiten von Verbindungen mittels **HTB** oder **HFSC** garantieren und priorisieren.

Mit **HFSC** ist es möglich die Übertragung innerhalb einer bestimmten Zeitspanne (Latency) zu garantieren. Gerade für VoIP-Anwendungen ist die entscheidend.

Umfangreiche **Statistik und Auswertemöglichkeiten** für die Auslastung der Verbindungen und Netzwerkschnittstellen stehen bereit.

Hardware-nahe Funktionen wie **Bridging, Bonding** (nach IEEE 802.3ad) und **tagged VLAN** (nach IEEE 802.1q) sind Komponenten des Collax Platform Servers.

Firewall

Die im Modul Collax Net Security enthaltenen Firewall kann den gesamten Verkehr mit der modernen **Stateful Inspection Technologie** filtern. Durch dieses Verfahren werden die Berechtigungen für eine Verbindung definiert und alle Datenpakete werden einer Verbindung zugeordnet. Pakete ohne eine solche Zuordnung werden verworfen, auch wenn der Dienst die Berechtigung hätte.

Die innovative **Firewall-Matrix** bietet den vollständigen Überblick über alle Regeln. Versteckte implizite Regeln, und nicht korrekt angeordnete Regeln, mit der Gefahr einen ungewollten Zugang in das Firmennetz zu öffnen, werden mit der **Firewall-Matrix** verhindert.

Alle Sicherheitskonzepte, die ein unterschiedliches Regelwerk für **mehrere unabhängige Netze** vorschreiben, können realisiert werden. Insbesondere wird die Einrichtung einer **DMZ** unterstützt.

Die Firewall lässt sich für **alle Dienste** (Ports) und eine **beliebige Zahl an Netzen** vollständig und **frei konfigurieren**. Alle gängigen Netzwerk-Dienste sind vorkonfiguriert. Zusätzliche Individuelle **Dienste** lassen sich bequem .

Zur korrekten Behandlung von Protokollen, die einen dynamischen Port aushandeln, stehen für **SIP, FTP, IRC, PPTP** und **TFTP** die **Layer-7-Protokollunterstützung** zur Verfügung.

Über den **ICMP-Filter** lässt sich das Verhalten auf „ping“-Anfragen regeln. Zum Schutz vor gefälschten Adressen wird eine „**Spoof Protection**“ eingesetzt.

Ein **Auswertungs-Tool, regelmäßige Berichte und das Ereignislog** sorgen für den Durchblick über die aktuelle Situation der Firewall und im lokalen Netz.

IPsec-VPN

Die wichtigste Anwendung für **IPsec VPN** ist die **Standortvernetzung**. Aber auch für Heimarbeitsplätze oder den so genannten Power Usern ist IPsec VPN ideal geeignet.

Alle wichtigen Verschlüsselungsalgorithmen (**3DES, AES, DES, Blowfish, Serpent, Twofish, CAST**) und Hash-Algorithmen (**MD5, SHA, SHA2**) sorgen für Kompatibilität zu IPsec-Gegenstellen.

Der **Verbindungs-Failover** sorgt für die Aufrechterhaltung von unternehmenskritischen VPN-Standortverbindungen.

Realisieren Sie eine **PKI** (Public Key Infrastructure), indem Sie Ihre Zertifikate selber generieren und Sie diese mit Hilfe der **CA** (CA: Certification Authority) verwalten. Bauen Sie auf die sichere Authentifizierung und Verschlüsselung mit Zertifikaten nach dem **X.509 Standard** ohne teure Zertifikate einkaufen zu müssen. Zertifikate können vorzeitig für ungültig erklärt werden (**Certificate Revokation List, CRL**).

Mit einem Pre-Shared Key (**PSK**) wird ein gemeinsames Passwort auf beiden Systemen zur synchronen und einfachen Authentifizierung zum Aufbau von Ipsec-Tunnel verwendet.

Mithilfe von **NAT-T** können, speziell für mobile Benutzer die GPRS oder UMTS einsetzen, VPN-Verbindungen aus lokalen Netzwerken realisiert werden. Standorte, die über keine feste IP-Adresse verfügen, können über **DynDNS** angebunden werden

IPsec VPN-Verbindungen können im **Transport Mode** und im **Tunnel Mode** eingerichtet werden.

Die Zahl der einsetzbaren **VPN-Tunnel** ist **unlimitiert**. Die einzige Beschränkung stellt die vorgegebene Bandbreite der Internet-Verbindung dar.

Das Betriebssystem Windows erlaubt es VPN-Verbindungen ohne zusätzliche Software mit wenigen Schritten per **PPTP** (Point-to-Point Tunneling Protocol) oder **L2TP** (Layer 2 Tunneling Protocol) einzurichten. L2TP ist dabei die neuere, sicherere Variante, die auf IPsec basiert und in Verbindung mit dem Betriebssystem Windows verwendet werden sollte.

SSL-VPN

SSL-VPN unterstützt den sicheren Zugriff auf **Web-Anwendungen**, wie Outlook Web Access, egal von welchem Standort der Person. Alternativ wird diese Funktion auch als **Reverse Proxy** bezeichnet. Selbst unverschlüsselte Web-Anwendungen werden mit SSL-VPN automatisch durch Verschlüsselung geschützt. Die Zugriffssteuerung von Benutzer auf Anwendung im Collax Gruppenmanagement gewährt eine flexible Anpassung an Unternehmensstrukturen.

Durch die Einrichtung von **S-Tunnel** können beliebige Protokolle verschlüsselt durch eine Firewall gereicht werden. Damit können Anwendungen von Arbeitsstationen außerhalb des Unternehmens mit einem Klick per **verschlüsselter Verbindung** mit dem Unternehmen kommunizieren. Das Berechtigungs-Management von Collax garantiert auch hier eine flexible Anpassung an die Unternehmensstruktur.

Terminal-Server-Sitzungen auf Server oder Arbeitsplatzrechner können direkt im Browser gestartet werden. Unterstützung stehen für **RDP** und **VNC** zur Verfügung. Für die Nutzung von RDP oder VNC ist keine Software-Installation notwendig, **Browser-Applets** übernehmen die Client-Funktion. Alternativ lassen sich auch lokal installierte, native Clients benutzen. Die **Berechtigungen** können **je Zielrechner** und **je Benutzer** unabhängig gesetzt werden.

Einbruchserkennung

Das **Intrusion Detection und Prevention System (IDP)** überprüft den Datenstrom auf bekannte Angriffsmethoden und unterbindet gegebenenfalls den Zugriff. Das auf *snort* basierende IDP mit **4.000 Regeln**, eingeteilt in **46 Kategorien**, sorgt für einen umfassenden Schutz vor bekannten Angriffen auf Ihr Netzwerk.

Das IDP kann in drei Betriebsarten eingesetzt werden. Als **Host-basiertes Intrusion Detection System (IDS)** beobachtet es den durchfließenden Datenstrom und alarmiert bei erkannten Angriffen. Es kann auch parallel zum Datenstrom platziert werden, so dass es nur passiv die Daten beobachtet und bei Ereignissen Alarm schlägt – **Netzwerk-basiertes IDS**. Die dritte Betriebsart ist wird als **Intrusion Prevention System (IPS)** bezeichnet. Hierbei wird der durchgeleitete Datenstrom überwacht. Im Gegensatz zum Host-basierten IDS wird aber nicht nur alarmiert sondern die angreifende **Verbindung** zusätzlich **blockiert**.

Um die Einbruchserkennung **im Netzwerk unsichtbar** zu betreiben kann der **Stealth-Modus** aktiviert werden.

Weitere Informationen unter www.collax.com



Kontaktieren Sie unsere Vertriebsmitarbeiter

E-Mail: sales@collax.com

Telefon: +49 (0) 89 990 1570