

Innominate

mGuard smart

Die einzigartige Sicherheitskomplettlösung für die Absicherung geschäftskritischer Kommunikation



Erhältlich ist der mGuard smart in den Leistungsklassen

- mGuard smart/266
- mGuard smart/533
- mGuard smart/266 VPN
- mGuard smart/533 VPN

Der mGuard smart ist derzeit das kleinste Security Device mit einem derart extrem hohen Grad an Sicherheit und Leistung. Er ist überall schnell und einfach integrierbar, ohne Veränderungen an den Rechnersystemen, unabhängig von Prozessortechnologien und Betriebssystemen.



Grundlegende Funktionen

Die „device attached security“-Lösung mGuard von Innominate vereint alle Funktionen, um IP-Verbindungen zuverlässig abzusichern:

- VPN (optional) für sichere Datenübertragung über öffentliche Netze (hardwarebasierte DES-, 3DES- und AES-Verschlüsselung, IPsec-Protokoll).
- Konfigurierbare Firewall schützt vor unberechtigten Zugriffen von „außen“. Die Stateful Inspection Firewall untersucht Datenpakete anhand der Ursprungs- und Zieladresse und blockiert unerwünschten Datenverkehr auch von „innen“.
- Benutzer-Firewall regelt den Zugriff auf interne oder externe Ressourcen über mGuard Anmeldung und zentralen RADIUS Server.
- Integrierter Anti-Virus-Schutz (optional) mit Unterstützung für die Protokolle HTTP, FTP, SMTP und POP3. Die Virenprüfung erfolgt bereits außerhalb des Computersystems. Also: mehr Sicherheit für den Rechner – die volle Leistung für die Anwendungen.

Neuartig und unvergleichbar: die wirtschaftliche Sicherheitslösung für die Industrie

Herkömmliche Sicherheitskonzepte, sowohl hardware- als auch softwarebasiert, erfordern immer eine aufwendige Implementierung mit Veränderungen an den Rechnerkonfigurationen. Doch in vielen Bereichen können Systeme nicht ohne weiteres verändert werden. In der Industrie beispielsweise gelten für Produktionssysteme strenge Sicherheitsauflagen und im medizintechnischen Bereich sind Validierungsprozesse gesetzlich vorgeschrieben. Jede Systemveränderung erfordert zusätzlichen Aufwand, der hohe Kosten verursacht.

Zudem gibt es Bereiche, die auf die Zuverlässigkeit älterer Prozessortechnologien bauen oder proprietäre Plattformen nutzen. Für zusätzliche Sicherheitstechnologien fehlt es hier oft an der Performance, an der Verfügbarkeit von Treibern oder an der Softwareunterstützung.

Die sichere Lösung für Büro und Produktions-Backoffice

Gängige Gateway Appliances sichern in der Regel ganze Netzwerke oder Netzwerksegmente mit einem einheitlichen Sicherheitsstandard und nur gegen Gefahren von „außen“. Ein unternehmenskritischer Server oder das Notebook eines Vorstands erfordern aber Sicherheitslevel, die weit höher liegen. Und: Unterschiedliche Systeme erfordern unterschiedliche Level. Mit herkömmlichen Gateways ist das kaum zu machen.

Dazu kommen die vielfältigen Gefahren von „innen“: Beispielsweise durch den Einsatz von Notebooks, Datenträgern oder die Nutzung privater E-Mail-Accounts wird oft ein „Malicious Code“ unwissentlich

eingeschleppt und verbreitet. Anti-Viren-Software hilft da nur bedingt, weil sie auf dem Betriebssystem aufsetzt. Die Sicherheitslücken bei dem in Büros meistens genutzten Betriebssystem Windows sind bekannt. Da ist auch die beste Anti-Viren-Software machtlos. Abgesehen davon gibt es auch im Office-Umfeld Systeme, welche die Installation zusätzlicher Software ausschließen, wie beispielsweise SAP/R3-Server.

Schnell installiert: das plattformunabhängige Sicherheitskonzept

Die mGuard Lösung vereint die Vorteile hardware- und softwarebasierter Sicherheitskonzepte in einer Komponente. Alle Sicherheitsfunktionen sind auf der eigenständigen, völlig unabhängig arbeitenden mGuard Plattform integriert. Deshalb muss das geschützte Rechnersystem nicht umkonfiguriert werden und es müssen weder Treiber noch zusätzliche Software installiert werden.

Unangreifbar durch den Innominate Stealth Mode

Die „device attached security“-Systeme mGuard von Innominate verfügen über eine besondere Funktion, den Stealth Mode. Sie arbeiten dabei absolut transparent und benötigen nicht einmal eine eigene IP-Adresse. Stattdessen nutzen sie dieselbe IP wie der zu schützende Rechner und sind dadurch für einen Angreifer nicht zu erkennen und deshalb auch nicht angreifbar.

Maximaler Datendurchsatz für VPN und Firewall

Die Basis der integrierten Sicherheitslösung ist das Embedded Linux auf dem Netzwerkprozessor mit XScale-Kern von Intel (IXP 42x): mit bis zu 533 MHz Prozessorleistung, 64 MByte SDRAM Arbeitsspeicher und 16 MByte Flash-Speicher. Im Prozessor gibt es fest verdrahtete Befehle für die Verschlüsselungsverfahren DES, 3DES und AES. Das garantiert den überragenden Durchsatz bei Firewall (bis zu 99 Mbit/s) und VPN (bis zu 70 Mbit/s).

Innominate Device Manager

Mit dem Innominate Device Manager (IDM) können große Populationen von mehreren tausend mGuard Appliances effizient konfiguriert werden. Der Roll-Out von vielen gleichartig konfigurierten Geräten ist durch den Template-basierten Ansatz des IDM schnell und komfortabel durchführbar.

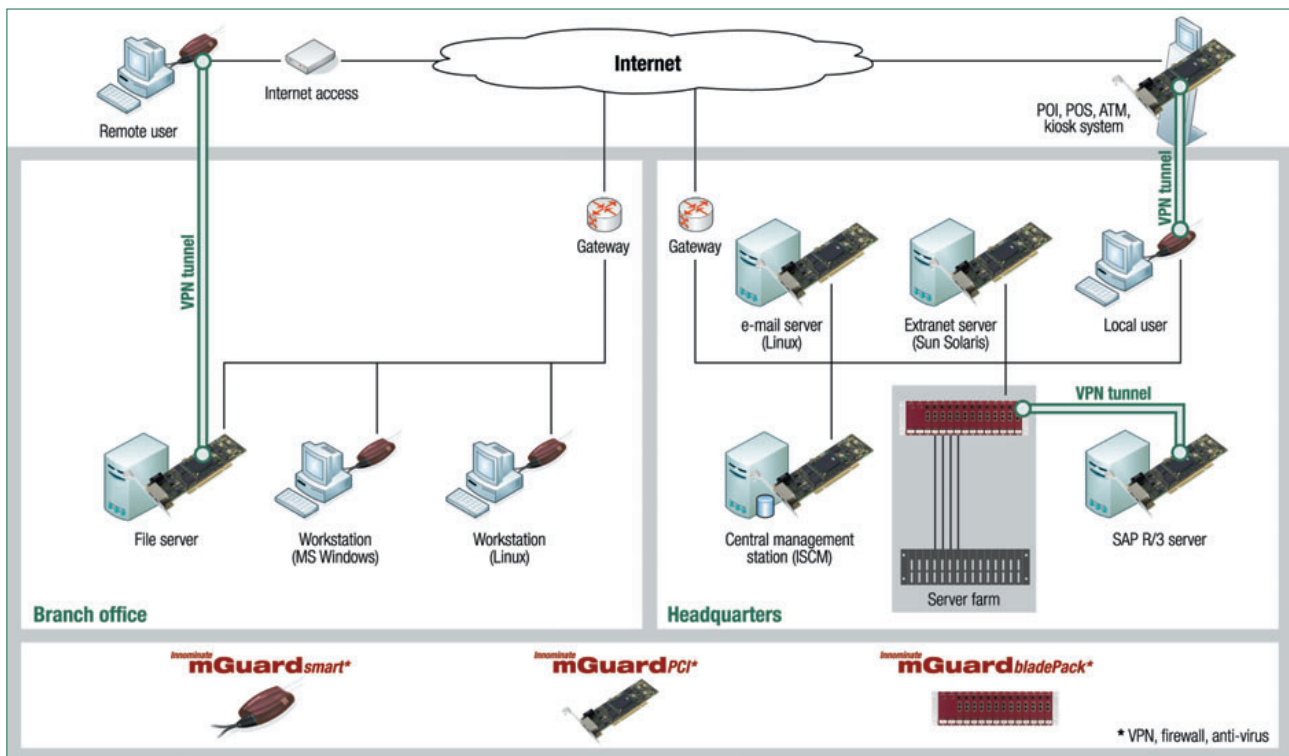
Für ein intuitives Monitoring und Logging kommunizieren die mGuards mit allen handelsüblichen SNMP-Systemen. Die volle grafische Einbindung wird zum Beispiel in der Industrial HiVision Management Plattform der Firma Hirschmann angeboten.

Auf einen Blick

- Mehr CPU-Leistung und höherer Datendurchsatz bei VPN und Firewall.
- Keine Konfigurationsänderungen, keine Installation von Treibern oder zusätzlicher Software.
- Eigenständig und unabhängig von Prozessor-technologien oder Betriebssystemversionen.
- Transparenter Innominate Stealth Mode.
- Plattformübergreifendes Security Management mit dem Innominate Security Configuration Manager (optional).
- Konfiguration mit dem Innominate Device Manager (IDM).
- Integrierte, leistungsfähige Anti-Virus-Lösung (optional).
- Benutzer-Firewall für personenbezogene Zugriffsregel (RADIUS Server).
- Virtuelle Adressierung (1:1 NAT) im VPN Tunnel zur Vermeidung von Adresskonflikten.

Die typischen Einsatzgebiete der mGuard Technologie

- Zusätzliche Sicherungen an neuralgischen Punkten im unternehmensweiten Netzwerk.
- Individuelle Absicherung unternehmenskritischer Systeme.
- Wirtschaftlich vertretbare Sicherheitslösungen für Systeme, die nicht „State of the Art“ sind.
- Kontrollierter Remote-Zugriff auf bestimmte Systeme für Mitarbeiter und externe Dienstleister.
- Kostengünstige, jederzeit verfügbare, sichere Verbindungen zu externen Teilnetzen und Remote-Arbeitsplätzen.



Hardware-Leistungsmerkmale	mGuard smart/266 mGuard smart/533	mGuard smart/266 VPN mGuard smart/533 VPN
CPU	Intel IXP 42x mit 266/533 MHz	Intel IXP 42x mit 266/533 MHz
RAM / Flash	64 MB SDRAM / 16 MB Flash	64 MB SDRAM / 16 MB Flash
1 LAN / 1 WAN port	Ethernet IEEE 802.3 10 / 100 BaseTX, RJ45, Full Duplex, Auto-MDIX	Ethernet IEEE 802.3 10 / 100 BaseTX, RJ45, Full Duplex, Auto-MDIX
MAU-Management	•	•
Internet		
Internetunterstützung	PPPoE, PPTP, Static IP, DHCP-Client, Stealth/Multi-Stealth	PPPoE, PPTP, Static IP, DHCP-Client, Stealth/Multi-Stealth
Network Services		
DHCP Support	Server oder Relay Agent	Server oder Relay Agent
DNS-Cache/Dyn. DNS	•/•	•/•
NTP Client	•	•
LLDP (Link Layer Discovery Protocol)	•	•
VLAN (802.1Q)	•	•
Internet Updates	•	•
Remote Syslog Logging	•	•
Anwenderbasierte Konfigurationsprofile	•	•
Sprachen	Deutsch, Englisch und Japanisch	Deutsch, Englisch und Japanisch
Virtual Private Network		
VPN-Datendurchsatz (3DES) 266/533	-	35/70 Mbit/s
Max. Anzahl an VPN-Tunneln	-	10
Verschlüsselungsverfahren	-	DES, 3DES, AES-128, -192, -256
Hardwarebasierte Verschlüsselung	-	•
IPsec-Modus	-	ESP-Tunnel / ESP-Transport
Authentifizierung	-	X.509v3 Zertifikate mit RSA oder PreShared Keys (PSK)
Datenintegrität	-	MD5, SHA-1
Internet Key Exchange (IKE)	-	Quick mode, Main mode, PFS
IPsec L2TP Server	-	•
VPN im Stealth Modus	-	•
1:1 NAT im VPN	-	•
IPsec NAT-Traversal	-	•
Dead Peer Detection (RFC 3706)	-	•
Dyn. DNS VPN-Support	-	•
Systemmanagement		
Webbasiertes Management (HTTPS)	•	•
Command Line Interface (SSH)	•	•
SNMP v1, v2, v3	•	•
Innominate Security Configuration Manager	optional	optional
Innominate Device Manager	optional	optional
Anti-Virus-Schutz*		
Integrierte Scan Engine	optional	optional
Prüft HTTP, FTP, POP3, SMTP, HTTP-Proxy	optional	optional
Block by File Size	optional	optional
Automatisierte Pattern File Updates	optional	optional

* Es wird empfohlen, den Anti-Virus-Schutz mit der 533 MHz CPU zu verwenden.

Technische Details	Firewall	mGuard Software-Optionen
Stromversorgung über USB Schnittstelle (5 V bei 500 mA); optional: ext. Stromadapter (110–230 V)	Firewall-Datendurchsatz 99 Mbit/s Anwenderlizenzen unbegrenzt	Innominate mGuard VPN-10 IPSec VPN Gateway, max. 10 VPN Tunnel
Betriebstemperatur 0 bis 40 °C	Stateful Inspection Firewall •	Innominate mGuard VPN-250
Relative Luftfeuchtigkeit 20 bis 90%, nicht kondensierend	NAT, 1:1 NAT •	IPSec VPN Gateway, max. 250 VPN Tunnel
Maße (B x H x T) 27 x 77 x 115 mm	Port-Weiterleitung •	Innominate mGuard Anti-Virus-50
Gewicht 158 g	MAC-Filtering •	50 Appliances, unbegrenzte Lizenz für CLAM AV™ Virus Pattern
	Firewall-Regeln in VPN-Verbindungen •	Innominate mGuard Anti-Virus-200
	IP Spoofing Protection •	200 Appliances, unbegrenzte Lizenz für CLAM AV™ Virus Pattern
	Syn Flood Protection •	Innominate mGuard Anti-Virus-1000
	Konfigurierbare DoS Protection •	1000 Appliances, unbegrenzte Lizenz für CLAM AV™ Virus Pattern
	Redundante Firewall (VRRP) optional	Innominate mGuard Redundant Firewall Option
		Erfordert zwei mGuard Security Appliances

Innominate mGuard ist ein eingetragenes Markenzeichen der Innominate Security Technologies AG. Für die mGuard Technologie sind mehrere nationale und internationale Patente angemeldet oder erteilt worden. Alle weiteren Warenzeichen, Marken und Namen sind Eigentum der entsprechenden Firmen. Änderungen von Produktspezifikationen, Fehler und Irrtümer vorbehalten. Stand 01.2007