datenblatt

mGuard
firmware

Major Release 8 –
Die Security Software für alle mGuard Appliances

Die Innominate *mGuard Firmware* ist das gemeinsame Herzstück aller mGuard Network Security Appliances. Das nunmehr in Major Release 8 vorliegende System setzt Markt- und Kundenanforderungen an die Sicherheit vernetzter industrieller Systeme in innovativer und dennoch ausgereifter Weise mit robusten Funktionen für die Praxis um. Eingesetzt auf den für verschiedene Umgebungen optimierten Bauformen von mGuard Appliances bringt es autonomen, maßgeschneiderten Schutz dezentral zu den Systemen, die ihn brauchen: in der Fertigungs- und Prozessindustrie, in der Infrastruktur für Transport und Versorgung und in die Produkte des Maschinen- und Anlagenbaus. Eine zentrale Geräte-Management-Komponente, der mGuard Device Manager, und viele ausgeklügelte Details sorgen dafür, dass die „Industrial Network Security“ effizient beherrschbar und für die Anwender ein problemloses „Plug-n-Protect“-Erlebnis bleibt.

Globale Konnektivität

In Verbindung mit mGuard 3G Geräten und den unterstützten Mobilfunk-Standards UMTS/HSPA und CDMA sind der Konnektivität keine Grenzen mehr gesetzt. Maschinen und Anlagen können auch dort angebunden werden, wo dies bisher nicht oder nur eingeschränkt möglich war. Durch ausgeklügelte Funktionen wie WAN-Redundanz und SIM-Failover wird eine Datenübertragung selbst bei Ausfall der Hauptverbindung gewährleistet.

Sichere Fernwartung leicht gemacht mit VPNs und der mGuard Secure Cloud

Die *mGuard Firmware* erlaubt den Aufbau von VPN-Verbindungen (Virtual Private Networks) nach dem offenen und weltweit bewährten Internet Standard IPsec in jedem Netzwerk-Modus und zu jedem mGuard Interface. Wo verfügbar, unterstützt sie Hardware-beschleunigte Verschlüsselung für einen maximalen VPN-Datendurchsatz. IKE Fragmentation Support sorgt dafür, dass die Verbindungen auch über Strecken mit UDP Fragmentverlusten zuverlässig zustande kommen. Und für Szenarien mit restriktivem Internet-Zugang können mGuard VPN-Verbindungen sogar über beliebige TCP Ports und Web Proxy Server mit Authentisierung getunnelt werden. Als weitere Besonderheit lassen sich dedizierte Firewall-Regeln innerhalb jedes VPN-Tunnels anwenden, um dessen jeweiligen Verkehr zu filtern. VPN-Verbindungen können wahlweise über eine Software-Schnittstelle, einen elektrischen Schaltkontakt oder per SMS (de-)aktiviert werden. Ideal für die Aus- oder Nachrüstung von Maschinen und Anlagen zur sicheren Fernwartung über Internet. Durch die Anbindung an eine mGuard Secure Cloud wird Fernwartung jetzt noch einfacher. Die mGuard Secure Cloud bietet Betreibern und Maschinen- und Anlagenbauunternehmen eine perfekt auf die *mGuard Firmware* abgestimmte schlüsselfertige VPN-Komplettlösung.

Stateful Packet Inspection Firewall

Ein- und ausgehende Datenpakete können in beiden Richtungen, d.h. vom externen Netz ins geschützte interne und umgekehrt anhand von Regeln gefiltert werden. Basierend auf Protokollen, Quelladressen und -ports sowie Zieladressen und -ports kann die Netzwerkkommunikation gezielt auf ein definiertes, produktiv erforder-

liches Maß beschränkt werden. Dabei werden Antwortpakete zu bestehenden erlaubten Verbindungen durch Connection Tracking erkannt und zugelassen (Stateful Inspection Prinzip). Firewall-Regeln können in hierarchischen Regelsätzen strukturiert werden, was die Konfiguration für gleichartige Protokoll-Gruppen zwischen verschiedenen Subnetzen sehr erleichtert. Zudem ist es mit der mGuard Conditional Firewall Funktionalität möglich, Regelsätze über konfigurierbare Schaltereignisse zu (de-)aktivieren. Dadurch können dynamisch differenzierte Regelwerke für verschiedene Betriebszustände, wie zum Beispiel Produktiv- und Wartungsbetrieb, einfach realisiert werden.

User Firewall

Bestimmte Netzwerkzugriffe sollen oftmals nicht pauschal, sondern nur für autorisierte Benutzer oder Gruppen freigegeben werden. Wenn diese mit dynamischen IP-Adressen oder von wechselnden Geräten aus arbeiten, lässt sich dies über statische Firewall-Regeln nicht mehr abbilden. Die mGuard Lösung: eine User Firewall, die nach lokaler oder RADIUS-basierter Authentisierung anhand einer benutzer- oder gruppenspezifischen Vorlage dynamisch zusätzliche Firewall-Regeln für autorisierte Anwender aktiviert. Diese Funktion steht auch innerhalb von VPN-Verbindungen zur Verfügung.

Routing mit NAT und 1:1 NAT

Die Strukturierung komplexer Produktionsabläufe in vernetzte, weitgehend eigenständige Zellen ist sehr üblich. Dabei ist es für die Effizienz bei Engineering, Dokumentation und Betrieb dieser Zellen oder Maschinen von Vorteil, den IP-basierten Teil ihrer internen Netze gleichförmig, d. h. mit Vergabe identischer Adressen in allen Maschinen eines Typs zu gestalten. Wird jegliche Kommunikation aus den internen Zellnetzen heraus initiiert, können auch mehrere dieser identischen Maschinen durch einfache NAT-Router mit Maskierung an das Produktionsnetz eines Betreibers angeschlossen werden. Wenn jedoch Verbindungen auch von einem übergeordneten Netzwerk zu einzelnen Zellknoten initiiert werden sollen, reicht dies nicht aus, da die Zellknoten damit von außen nicht adressierbar sind. Benötigt wird dann ein Router, der interne Maschinennetze durch 1:1-Network-Address-Translation ganz oder selektiv auf jeweils eindeutige, virtuelle externe Netze (anderweitig nicht genutzte Subnetze des übergeordneten Netzwerks) abbilden kann. Die *mGuard Firmware* leistet daher neben reinem NAT-Routing auch diese 1:1-NAT-Routing-Funktionen.

OPC Inspector

Während sich OPC-Datenverkehr durch konventionelle Firewalls nicht sinnvoll absichern lässt, bietet der mGuard OPC Inspector hierfür eine Lösung. Durch die Deep Packet Inspection von OPC-Datenpaketen können diese durch den mGuard präzise gefiltert werden. Dabei wird das Stateful Inspection Prinzip auch auf OPC-Daten angewandt. Mittels Firewall-Regeln können OPC-Verbindungen zwischen einzelnen Netzwerkteilnehmern erlaubt oder untersagt werden. Im OPC-Protokoll ausgehandelte Portänderungen werden durch die Firewall erkannt und dynamisch erlaubt. Dabei prüft die Firewall, dass ein durch OPC geöffneter Port innerhalb eines Timeouts benutzt wird und der über diesen abgewickelte Datenverkehr dem OPC-Protokoll entspricht. Mit dem OPC Inspector wird zudem sogar NAT des OPC-Datenverkehrs ermöglicht. Selbstverständlich unterstützt der OPC Inspector ebenso eine OPC-Kommunikation über VPN.

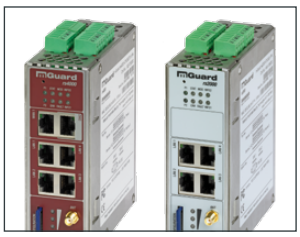
Public Key Infrastrukturen (PKIs)

Die *mGuard Firmware* zeichnet sich durch eine vollständige Unterstützung von Public-Key-Infrastrukturen aus. Es können Zertifikate zur Nutzung auf einem Gerät bzw. von vertrauenswürdigen Gegenstellen sowie von signierenden Certificate Authorities (CAs) verwaltet und zur Authentisierung verwendet werden. Certificate Revocation Lists (CRLs) können berücksichtigt und die zeitliche Gültigkeit von Zertifikaten und CRLs überprüft werden.

Quality of Service (QoS)

Die QoS-Funktionalität der *mGuard Firmware* erlaubt, die Paketraten bzw. Bandbreiten des Datenverkehrs durch eine mGuard Appliance auf ein Maß zu beschränken, das die an der Kommunikation beteiligten Verbindungswege und Komponenten übertragen und zuverlässig verarbeiten können. Sie sorgt bei Überschreitung von Schwellwerten für geeignete Priorisierung der Datenpakete und garantierten Mindestdurchsatz für definierte Protokolle, damit zeitkritische Verbindungen nicht von weniger wichtigen Daten oder gar vorsätzlich schadhaften Paketen eines Netzwerkangriffs gestört werden. QoS ist damit zum Beispiel interessant für den Schutz überlastungsgefährdeter Steuerungen und für das Bandbreiten-Management im Teleservice, etwa bei Nutzung verzögerungsempfindlicher Protokolle wie Voice over IP (VoIP).

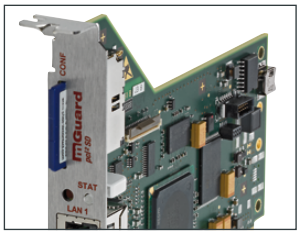
mGuard rs4000/rs2000



mGuard rs4000 3G/rs2000 3G

mGuard centerport²

mGuard delta²



mGuard pci²

mGuard smart²

Integritätsüberwachung zum Schutz gegen Schadsoftware

Industrielle Automatisierungskomponenten mit Microsoft Windows Betriebssystemen sind heute weit verbreitet und wie ihre Pendants in Büronetzen durch eine Fülle von Würmern, Viren und anderer Schadsoftware bedroht. Leider ist aber die lokale Installation von Antivirus-Software auf diesen industriellen Komponenten wegen Mangel an Hardware-Ressourcen und ungewissem Echtzeitverhalten meist ausgeschlossen. Und das Appliance-basierte Scannen von Netzwerkverkehr auf Viren ist für das wichtige und zum Zugriff auf Windows Dateifreigaben häufig genutzte Server Message Block (SMB) oder Common Internet File System (CIFS) protokolltechnisch nicht möglich.

Deshalb bietet die *mGuard Firmware* mit CIFS Integrity Monitoring eine innovative, industrietaugliche Lösung für dieses Problem. Sie umfasst den CIFS Antivirus Scan Connector, mit dem zum Datenaustausch genutzte Netzwerkordner regelmäßig von Ihrem bevorzugten externen Virenscanner analysiert werden können, und das konfigurierbare CIFS Integrity Checking, welches Dateisysteme auf unerwartete Modifikationen oder Hinzufügungen von Programmen, DLLs oder anderem ausführbaren Code überwacht. Letzteres basiert rein auf Berechnung von Hashcode-Signaturen und kommt ohne Virenmuster und deren ständige Aktualisierung aus. Entdeckte Integritätsverletzungen können dann einen Alarm per SNMP Trap oder E-Mail an den Administrator auslösen. All dies kann zwar nicht den Echtzeitschutz eines lokal installierten Scanners bieten, leistet aber das unter den gegebenen Umständen Bestmögliche: es lässt Infektionen nicht lange unentdeckt bleiben, riskiert nicht, kritische Kommunikation aufgrund von „False Positives" zu unterbrechen, und findet sogar Schäden von Zero Day Exploits, für die es noch gar keine Virenmuster gibt.

Flexible Netzwerkintegration

Die *mGuard Firmware* unterstützt den flexiblen Betrieb von mGuard Appliances in verschiedensten Netzwerk-Szenarien. Die Ethernet MAU-Konfiguration (10/100/1000 MBit/s, Half/Full Duplex) erfolgt dabei wahlweise automatisch oder manuell. Im patentierten Single Stealth Mode schützt das System transparent und ohne eigene IP-Adresse einen einzelnen Netzwerkknoten, im Multi Stealth Mode ebenfalls transparent, aber mit eigener Management-IP ein ganzes Subnetz. Im Router Mode sorgt der mGuard für eine Netzwerktrennung von internem und externem Netz mit frei definierbaren zusätzlichen Routen. Besondere Router-Modi sind PPPoE (DSL Router) und der Modem-Betrieb über ein integriertes Mobilfunk-Modul oder externes serielles Modem. Diese Modem-Verbindungen können auch parallel oder als Failover zum Ethernet-Betrieb genutzt werden. Die externe Netzwerk-Konfiguration kann über DHCP erfolgen und das mGuard System auch selbst als DHCP Server oder Relay agieren. Bei Verwendung dynamischer IPs ist die automatisch mögliche DynDNS-Registrierung nützlich. Noch flexibler einsetzbar sind mGuard Appliances mit eingebautem managed Switch. Diese bieten zudem eine DMZ (Demilitarisierte Zone), eine zusätzliche Netzwerkzone mit eigenem Regelwerk für Routing und Firewall.

Geräte-Management und dynamisches User Interface für einfache Konfiguration

mGuard unterstützt ein zentrales Geräte-Management durch den mGuard Device Manager (mdm) mit seinen „Push-und-Pull-Verfahren". Vom mdm erzeugte Konfigurationen können von mGuard Systemen zeitgesteuert oder beim Booten automatisch per Configuration Pull von einem sicheren Web Server geladenen und aktiviert werden. Auch Firmware-Updates und das Aufspielen von Lizenzen können so veranlasst werden. Bei Fehlern in der neuen Konfiguration kann ein automatischer Rollback den vorherigen Zustand und Zugriff auf das Gerät wiederherstellen.

Lokal können mGuard Systeme über ein sicheres Web Interface sowie ein sicheres Command Line Interface administriert werden. Durch das dynamische WebGUI sind mGuard Geräte dabei auch für ungeübte Nutzer leicht zu administrieren. Geänderte bzw. fehlerhafte Einstellungen werden farbig hervorgehoben und liefern dem Nutzer so jederzeit einen Überblick.

Administrative Zugriffe sind über Firewall-Regeln und Authentisierung geschützt und werden auch über VPN-Verbindungen zum jeweiligen mGuard unterstützt. In Verbindung mit mdm werden fünf Benutzer-Rollen mit abgestuften Rechten angeboten: Root, Admin, Netadmin, User und Audit. Konfigurationsprofile können als Sicherung oder Variante auf den Geräten gespeichert und wiederhergestellt bzw. heruntergeladen werden.

Ihre Vorteile

Sicherheit: Geben Sie Angreifern keine Chance! Die hochsicheren Komponenten der *mGuard Firmware* schützen die Kommunikationswege zu Ihren Systemen, Maschinen und Anlagen mit höchster Sicherheit vor Angriffen und lassen Sie beruhigt schlafen.

Plug-n-Protect: Vermeiden Sie langwierige Abstimmungen! Die *mGuard Firmware* bietet durch den patentierten mGuard Stealth Mode schnelle und rückwirkungsfreie Integration der Security Appliances. Diese verhalten sich dabei völlig transparent und verwenden die IP-und MAC-Adresse des zu schützenden Systems. Hierdurch sind sie für einen Angreifer nicht zu erkennen und somit auch nicht kompromittierbar.

Schnelligkeit: Erhöhen Sie Ihre Sicherheit ohne Verschlechterung der Antwortzeiten! Die hohen Durchsatzraten von Geräten mit *mGuard Firmware* ermöglichen Ihnen die schnelle und gleichzeitig sichere IP-Kommunikation mit allen Maschinen und Systemen.

Aktualität: Lassen Sie sich nicht abhängen! Neuen sicherheits- und marktgetriebenen Anforderungen können Sie schnell und einfach mit Hilfe von regelmäßigen Upgrades der *mGuard Firmware* begegnen.

Zeitersparnis: Erhöhen Sie Ihre Effizienz! Der optional erhältliche mGuard Device Manager erleichtert Ihnen das zentrale Management und den Vorlagen-basierten Roll-out sämtlicher mGuard Geräte.

mGuard Firmware	Standard-Ausstattung (•) Hardwareabhängig	Neu in mGuard Version
Unterstützte Netzwerk Modi		
Stealth, Multi-Stealth, Router, PPPoE, PPTP; statische IP o. DHCP Client	•	
Externes Modem	•	5.0/5.1
Sekundäres externes Interface (seriell)	Hardwareabhängig	6.0
Mobile Network Connection (GPRS/EDGE/UMTS/HSPA und CDMA)	Hardwareabhängig	8.0
Switch Unterstützung (managed/unmanaged)	Hardwareabhängig	8.0
Unterstützung DMZ (demilitarisierte Zone)	Hardwareabhängig	8.0
Netzwerk Services		
DHCP Server Support: Server oder Relay Agent	•	
DNS Cache und lokaler DNS Server	•	6.1
Dyn DNS	•	
NTP Client und Server	•	6.0
LLDP (Link Layer Discovery Protocol)	•	
VLAN (802.1Q)	•	
QoS (Quality of Service): Bandbreiten-Management und Priorisierung	•	5.0/5.1
GPS/GLONASS zur Positionsbestimmung und Zeitsynchronisation	Hardwareabhängig	8.0
COM Server nach RFC2217	Hardwareabhängig	8.0
System Management		
Beschleunigte Firmware-Flash-und-Rollout-Prozedur	•	7.0
Online Updates	•	
Benutzer-definierte Konfigurationsprofile und Custom Default Profile	•	6.0
Web-basiertes Management (HTTPS)	•	
Command Line Interface (SSH)	•	
SNMP v1, v2, v3	•	
Erweiterte Unterstützung für mGuard Device Manager	•	5.0/6.0
Administration über VPN	•	6.0
Remote Syslog Logging	•	
Eventgesteuerte E-Mail und SMS Versendung	Hardwareabhängig	8.0
Firewall		
Stateful Inspection Firewall	•	
Benutzer-Lizenzen (Knoten)	Unbeschränkt	
NAT, 1:1 NAT	•	
Port Forwarding	•	
MAC-Filtering	•	
Firewall-Regeln in VPN-Verbindungen	•	
User Firewall (neu: auch in VPN-Verbindungen)	•	8.1
(De-)Aktivieren von Firewall Regelsätzen über Signalkontakt	Hardwareabhängig	8.1
(De-)Aktivieren von Firewall Regelsätzen über CGI oder SMS	Hardwareabhängig	8.1
Hierarchische Regelsätze	•	
IP Spoofing Protection	•	
Konfigurierbare SYN Flood und DoS Protection (gegen Denial of Service)	•	

mGuard Firmware	Standard-Ausstattung (•) Hardwareabhängig	Neu in mGuard Version
Virtual Private Networks (IPsec VPNs)	Lizenz oder Bundle erforderlich	
Max. Anzahl gleichzeitig aktiver VPN Tunnel	Bis zu 3000	
Verschlüsselungsalgorithmen: DES, 3DES, AES-128/-192/-256	Hardwareabhängig	
Hardware-beschleunigte Verschlüsselung	•	
IPsec Modes: ESP Tunnel / ESP Transport; IPsec NAT-Traversal	•	
IPsec Tunnelung durch TCP und Web Proxy Server mit Authentisierung	•	
Authentisierung: X.509v3 Zertifikate mit RSA oder PSK	•	
PKI Support: Zertifikatsverwaltung, CA-Zertifikate, CRLs	•	
Datenintegrität: SHA-1 – SHA-512	•	
Internet Key Exchange (IKE): Quick Mode, Main Mode/Aggressive Mode, PFS	•	
IKE Fragmentation Support	•	
IPsec L2TP Server	•	
Dead Peer Detection (RFC 3706)	•	
DynDNS Support für VPNs	•	
VPN Verbindungen zu jedem mGuard Interface	•	
VPN in jedem Netzwerk Modus inkl. Single und Multi Stealth Mode	•	
1:1 NAT in VPNs (Local und Remote Network)	•	
NAT-Maskierung in VPNs (Local Network)	•	
(De-)Aktivieren von VPN Tunneln über HTTPS	•	
(De-)Aktivieren von VPN Tunneln über elektrischen Signalkontakt	Hardwareabhängig	
(De-)Aktivieren von VPN Tunneln über SMS	Hardwareabhängig	8.0
SNMP Traps für VPN-Ereignisse (Tunnel Up/Down)	•	
Erweiterte VPN-Diagnose und Statusabfragen über CGI	•	
	•	
Integritätsüberwachung/Schutz vor Schadsoftware	Lizenz erforderlich	7.0
CIFS Integrity Monitoring, bestehend aus CIFS Antivirus Scan Connector und CIFS Integrity Checking für Windows Dateifreigaben	Option	
Deep Packet Inspection für OPC	Lizenz erforderlich	8.1
mGuard OPC Inspector	Option	

Weitere Informationen zu den mGuard Produkten und der mGuard secure cloud finden Sie in den jeweiligen Datenblättern und auf **www.innominate.com.**

Innominate® und HyperSecured® sind eingetragene Markenzeichen der Innominate Security Technologies AG in den Ländern der Europäischen Union. mGuard® ist ein eingetragenes Markenzeichen der Innominate Security Technologies AG in den Ländern der Europäischen Union sowie den USA. Für bestimmte Technologien, welche in mGuard® Produkten Verwendung finden, sind in den Ländern der Europäischen Union, den USA und in Japan der Innominate Security Technologies AG Patente erteilt bzw. durch sie beantragt worden. Alle weiteren Warenzeichen, Marken und Namen sind Eigentum ihrer jeweiligen Inhaber. Weitere Informationen stehen unter www.innominate.de/trademarks zur Verfügung. Änderungen von Produktspezifikationen, Fehler und Irrtümer vorbehalten. Stand: Oktober 2014.

Innominate Security Technologies AG | Rudower Chaussee 13 | 12489 Berlin | Deutschland | Tel. +49 30 921028-0 | Fax +49 30 921028-020 | www.innominate.com