

Innominate **mGuard** Firmware – Major Release 7

Das Embedded Secure Linux System für alle mGuard Appliances

Das Innominate mGuard System: Sicherheit für industrielle Netzwerke

Die Innominate mGuard Firmware ist das gemeinsame Herzstück aller mGuard Network Security Appliances. Das nunmehr in Major Release 7 vorliegende System

Details sorgen dafür, dass die Komplexität der Operation „Industrial Network Security“ effizient beherrschbar und für die Anwender ein problemloses „Plug & Protect“-Erlebnis bleibt.

Mehr Plattformen und noch mehr Geschwindigkeit

Mit mGuard 7 tragen Innominate konsequente Entwicklungsanstrengungen für Portierbarkeit und Multi-Plattform Support Früchte: die Firmware ist jetzt für ARM, x86 und PowerPC Architekturen verfügbar, was die mGuard Technologie zu einer zukunfts-sicheren Investition und attraktiven Option für Embedded Security OEM-Lösungen macht. Bereits bestens bekannt für die erstklassige Performance ihrer primären Sicherheitsfunktionen wurde sie weiterer Optimierung mit Beschleunigung vieler Hilfsfunktionen unterzogen, welche Sie mGuard Appliances schneller denn je flashen, ausrollen, booten und rekonfigurieren lassen.

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 erforderliches 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.



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 Innominate Device Manager, und viele ausgeklügelte

Highlights

- Top Performance, bootet und konfiguriert sich schneller denn je
- Stateful Packet Inspection (SPI) Firewall
- Routing mit NAT und 1:1 NAT
- Virtual Private Networks (IPsec VPNs) mit vollem PKI Support und optionaler Tunnelung durch TCP und Web Proxy Server
- Quality of Service (QoS)
- Optionale Integritätsüberwachung von Windows Dateifreigaben auf Infektionen durch Schadsoftware
- Plug & Protect: optimale Netzwerkintegration durch flexible Betriebsmodi
- Parallele oder Failover-Kommunikation über Ethernet und serielle Wählverbindung
- Extrem flexible und beschleunigte Flash- und Rollout-Prozedur auf Basis von DHCP und TFTP
- Konfiguration und Management zentral über Innominate Device Manager oder lokal über WebGUI und Command Line Interface
- Jetzt mit Multi-Plattform Support für ARM, x86 und PowerPC Architekturen

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 gruppen-spezifischen Vorlage dynamisch zusätzliche Firewall-Regeln für autorisierte Anwender aktiviert.

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 Funktion.

Virtual Private Networks (VPNs)

Die mGuard Firmware erlaubt den Aufbau von VPN-Verbindungen 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 oder einen elektrischen Schaltkontakt (de-)aktiviert werden – ideal für die Aus- oder Nachrüstung von Maschinen und Anlagen zur sicheren Fernwartung über Internet.

Public Key Infrastrukturen (PKIs)

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)

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 schadhafte Paketen eines Netzwerkangriffs gestört werden. QoS ist damit z. B. interessant für den Schutz überlastungsgefährdeter Steuerungen und für das Bandbreiten-Management im Teleservice, etwa bei Nutzung verzögerungsempfindlicher Protokolle wie Voice over IP (VoIP).

Integritätsüberwachung zum Schutz gegen Schadsoftware

Industrielle Automatisierungskomponenten mit Microsoft Windows Betriebssystemen sind heute weit verbreitet und wie ihre Pendanten 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) Protokoll technisch nicht möglich. Mit mGuard 7 stellt Innominat deshalb das neue CIFS Integrity Monitoring als innovative, industrietaugliche Lösung für dieses Problem vor. Sie umfasst den CIFS Antivirus Scan Connector, mit dem zum Datenaustausch genutzte Netzwerkordner regelmäßig von Ihrem bevorzugten externen Virenschanner 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 paten-

tierten 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 mGuard für eine Netzwerk-trennung von internem und externem Netz mit frei definierbaren zusätzlichen Routen. Besondere Router-Modi sind PPPoE (DSL Router) und der „Modem“-Modus, mit dem mGuard über ein analoges Modem oder einen ISDN Terminal Adapter als serieller Router über Wählleitungen fungiert. Wählverbindungen 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.

Geräte-Management

mGuard unterstützt ein zentrales Geräte-Management durch den Innominat Device Manager (IDM) mit seinen „Push“ und „Pull“ Verfahren. Vom IDM erzeugte Konfigurationen können von mGuard Systemen zeitgesteuert oder beim Booten automatisch per Configuration Pull von einem sicheren Web Server geladen 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, auf dem auch der Configuration Push vom IDM zu mGuard Appliances basiert. Administrative Zugriffe sind über Firewall-Regeln und Authentisierung geschützt und werden auch über VPN-Verbindungen zum jeweiligen mGuard unterstützt. In Verbindung mit IDM werden fünf Benutzerrollen 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.

Optimierter Update-Prozess

Geräte mit Verbindung zu einem Firmware Update Web Server können „auf Knopfdruck“ automatisch auf das aktuellste Patch oder Minor Release bzw. das nächste Major Release der mGuard Firmware aktualisiert werden. Bei diesen inkrementellen Updates, die ohne Beeinträchtigung im laufenden Betrieb vorgenommen werden können und nach Möglichkeit auch keinen Neustart des Geräts erfordern, bleibt die jeweilige Geräte-Konfiguration erhalten. Nachträglich für optionale Features eingespielte Lizenzen werden auf den Geräten persistiert und stehen damit auch nach einem kompletten Flashen mit einer anderen Firmware Version sofort wieder zur Verfügung. Proxy Server einschließlich Authentisierung werden für den Firmware Download wie auch für den oben genannten Configuration Pull unterstützt.

Netzwerk Management Unterstützung

mGuard unterstützt SNMP v1/v2/v3 mit entsprechenden MIBs für Queries und Traps für wichtige Ereignisse, z. B. Link Up/Down oder VPN Status-Änderungen. System- und Firewall/VPN-Ereignisse können lokal oder auf einem Remote Syslog Server geloggt werden. Die Systemzeit kann über NTP mit einer zentralen Zeitquelle synchronisiert werden. Ferner wird das Discovery Protokoll LLDP zur automatischen Erkennung von Geräten im Netz unterstützt.

Kategorien / Leistungsmerkmale	Standard-Ausstattung (*) und Option	Neu in mGuard Version
Unterstützte Netzwerk-Modi		
Stealth, Multi-Stealth, Router, PPPoE, PPTP; statische IP o. DHCP Client	•	
Modem (externes und internes)	•	5.0/5.1
Sekundäres externes Interface (seriell)	•	6.0
Network Services		
DHCP 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
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 Innominate Device Manager	•	5.0/6.0
Administration über VPN	•	6.0
Remote Syslog Logging	•	
Firewall		
Stateful Inspection Firewall	•	
Benutzer-Lizenzen (Knoten)	unbeschränkt	
NAT, 1:1 NAT	•	
Port Forwarding	•	
MAC-Filtering	•	
Firewall-Regeln in VPN-Verbindungen	•	
User Firewall	•	
Hierarchische Regelsätze	•	
IP Spoofing Protection	•	
Konfigurierbare SYN Flood und DoS Protection (gegen Denial of Service)	•	
Virtual Private Networks (IPsec VPNs)		
	Lizenz oder Bundle erforderlich	
Max. Anzahl gleichzeitig aktiver VPN Tunnel (abhängig von Gerätetyp und /oder Software-Lizenz)	10/250/1.000	7.0
Verschlüsselungsalgorithmen: DES, 3DES, AES-128/-192/-256, Null	•	
Hardware-beschleunigte Verschlüsselung	•	
IPsec Modes: ESP Tunnel/ESP Transport; IPsec NAT-Traversal	•	
IPsec Tunnelung durch TCP und Web Proxy Server mit Authentisierung	•	6.1
Authentisierung: X.509v3 Zertifikate mit RSA oder PSK	•	
PKI Support: Zertifikatsverwaltung, CA-Zertifikate, CRLs	•	5.0/6.0
Datenintegrität: MD5, SHA-1	•	
Internet Key Exchange (IKE): Quick Mode, Main Mode, PFS	•	
IKE Fragmentation Support	•	5.1
IPsec L2TP Server	•	
Dead Peer Detection (RFC 3706)	•	
DynDNS Support für VPNs	•	
VPN Verbindungen zu jedem mGuard Interface	•	6.0
VPN in jedem Netzwerk Modus inkl. Single und Multi Stealth Mode	•	6.0
1:1 NAT in VPNs (Local und Remote Network)	•	
NAT Maskierung in VPNs (Local Network)	•	6.1
(De-)Aktivieren von VPN Tunneln über HTTPS	•	
(De-)Aktivieren von VPN Tunneln über elektrischen Signalkontakt	•	5.1/6.0
SNMP Traps für VPN-Ereignisse (Tunnel Up/Down)	•	5.1
Erweiterte VPN-Diagnose und Statusabfragen über CGI	•	6.1
Integritätsüberwachung / Schutz vor Schadsoftware		
CIFS Integrity Monitoring, bestehend aus CIFS Antivirus Scan Connector und CIFS Integrity Checking für Windows Dateifreigaben	Option	7.0

Hardware-Plattform Support

Die mGuard 7 Firmware ist für die Prozessorarchitekturen

- ARM,
 - x86
 - und PowerPC
- verfügbar, und unterstützt die folgenden mGuard Security Appliances:
- mGuard blade
 - mGuard centerport
 - mGuard delta
 - mGuard industrial RS (Analog/ISDN)
 - mGuard PCI
 - mGuard smart
 - EAGLE mGuard.