

## SICHERHEIT

## Firewall to Go: Ein Blick auf die neueste mGuard-Firewall-Generation

Mit der Vorstellung des mGuard hatte die Innominat AG damals eine kleine Revolution ausgelöst. Firewalls waren auf einmal nicht mehr groß und sperrig und fürchterlich kompliziert zu bedienen. Das damals revolutionäre Gerät war klein und leicht, ideal für den Gebrauch am Notebook unterwegs und im Extremfall völlig ohne Konfiguration in Betrieb zu nehmen brachte es doch Sicherheit.

Trotz des Erfolges hat der Hersteller sich nicht auf den Lorbeeren ausgeruht und nur noch Detailverbesserungen vorgenommen. So wurde vor kurzem eine PCI-Variante des mGuard veröffentlicht, die zwar nicht mehr so klein ist, aber durch die Verwendung von Standard-Bauteilen preiswerter produziert werden kann. Diese Variante ist dennoch genauso einfach zu verwenden wie das Original.

### Variantenreich

Neben dem Formfaktor wurde auch der Funktionsausstattung einiges an Aufmerksamkeit geschenkt. Es stehen nun insgesamt drei Softwareausstattungen zur Verfügung, die sich nach außen vor allem in der Anzahl der VPN-Kanäle unterscheiden. Während die Professional-Variante mit nur zwei VPN-Tunneln als Device für Endgeräte spezialisiert ist, stehen mit der Enter-

prise-(10 VPN)/XL(250 VPN)Variante Geräte zur Verfügung, die auch als zentraler Firewall Router dienen können. Da es sich bei der Anzahl der Tunnel im Wesentlichen um Lizenz-Einschränkungen handelt, lassen sich die Professional-Produkte auf die jeweils höhere Stufe upgraden. Der mGuard Enterprise XL enthält aber für höheren Datendurchsatz einen schnelleren Prozessor und mehr Speicher, sodass hier kein Upgrade möglich ist.

Werfen wir vor allem einen Blick auf den neuen mGuard PCI. Dieser bietet zwei 10/100-BaseTX-Netzwerkanschlüsse für den Datenverkehr an. Diese können in zwei unterschiedlichen Betriebsmodi betrieben werden. In der Werkseinstellung befindet sich die PCI-Karte im Power-Over-PCI-Modus. Das heißt, der PCI-Anschluss dient lediglich der Stromversorgung der Karte. Der mGuard PCI wird entsprechend genutzt, wie der externe mGuard. Es ist also im Rechner eine weitere Netzwerkkarte vorzusehen. Diese wird per Patch-Kabel am LAN-Anschluss des mGuard angeschlossen. Eine weitere Kabelverbindung dient dem WAN-Anschluss. Der Vorteil dieser Lösung ist, dass die Karte ohne einen Treiber, der lediglich für Linux und Windows 2000/XP zur Verfügung steht, betrieben werden kann. Die Steuerung erfolgt wie beim Standard-mGuard über eine gesicherte Netzwerk-Verbindung. Der mGuard PCI kann aber auch als einzige Netzwerkkarte am Rechner/Server betrieben werden, der Netzwerkverkehr setzt dann die Installation eines Treibers voraus. Trotzdem werden internes und externes Netzwerk getrennt – dies geschieht dann direkt auf der Karte.

### Netzwerk-Optionen

Gegenüber den vorangegangenen Versionen hat der Hersteller in einigen wesentlichen Punkten die Netzwerkoptio-

nen ausgebaut. Der Internet-Zugang kann, wie bisher, über ein internes Netzwerk bzw. separaten Router erfolgen, es besteht aber auch die Möglichkeit, per PPPoE oder PPTP eine direkte Internetverbindung herzustellen.

Bei der Einsatzplanung für die Geräte sind die zwei zur Verfügung stehenden Modi unbedingt zu beachten: der Stealth- und der konventionelle Modus. Im Stealth-Modus fügt sich der mGuard völlig transparent in vorhandene Netzwerkstrukturen ein. So lässt er sich optimal mit tragbaren Devices nutzen, da bei einem Anschluss in fremde Netzwerke keine Konfiguration notwendig ist. Aber auch komplexe Netze, bei denen lediglich wenige Außenstellen per VPN abgesichert werden müssen, lassen sich so aufrüsten, ohne an den vorhandenen Einstellungen Änderungen vorzunehmen. Besonders hilfreich ist dies bei der schwierig zu handhabenden dynamischen Adressverteilung.

Stichwort „Stealth“: Stealth-Mode-Firewalls sind auf einer Bridge implementiert und gestatten das Filtern des Datenverkehrs, ohne eine entsprechende Unterteilung in Teilnetze vornehmen zu müssen. Diese Devices sind im Sinne der Netzwerktopologie transparent.

Im standardmäßigen Netzwerkverkehr versteht sich der mGuard auf alle notwendigen Maßnahmen: Er unterstützt DHCP als Client und Server, bietet DNS Caching und die Unterstützung für dynamische DNS-Vergaben über verschiedenen Dienste, inklusive dem Angebot von Innominat. Verschiedene Konfigurationsprofile erleichtern den Einsatz an unterschiedlichen Rechnern, bzw. in unterschiedlichen Netzwerken. Die Enterprise-Editionen unterstützen darüber hinaus externe Protokollaufzeichnungen, die eine Überwachung von zentraler Stelle erleichtern.



Abb. 1: In den erweiterten Einstellungen zur Firewall sichert der Anwender die Qualität der Dienste.

## SICHERHEIT

Fortsetzung von Seite 14

Im VPN-Modus bewältigt der mGuard einen Datendurchsatz von 35 MBit/s bei Professional und Enterprise, die Enterprise XL schafft durch die bessere Hardwareausstattung den doppelten Durchsatz, die maximale Anzahl der Tunnel beträgt 2, 10, bzw. 250 Stück. Abgesichert werden die IPsec-Kanäle, die wahlweise im Tunnel- oder Transport-Modus arbeiten, über 3DES- oder AES-Verschlüsselung, unterstützt von X.509-Zertifikaten, oder PSK zur Authentifizierung, für die Datenintegrität sorgen wahlweise MD5 oder SHA-1. Das IPsec Layer 2 Tunneling Protocol steht nur für die Enterprise-Varianten zur Verfügung. Praktischerweise profitieren auch die VPN-Kanäle von der dynDNS-Unterstützung.

### Firewalling und Antivirus

Wie bei den meisten Firewalls sperrt der mGuard im Auslieferungszustand sämtlichen eingehenden Datenverkehr und erlaubt ausschließlich ausgehenden Datenverkehr. Somit ist er gut für den schnellen, mobilen Einsatz zwischendurch gerüstet. Bei Gebrauch innerhalb eines Firmennetzes gelten jedoch andere Regeln, sodass der Anwender hier entsprechende Regelwerke erstellen muss, da im einfachsten Fall das Firmennetz ja als nicht vertrauenswürdige Netz gilt. Daher muss der Anwender, sofern er den ausgehenden Verkehr einschränken will, darauf achten, dass Dienste, wie z.B. die Druckdienste, freigegeben werden. Eine Stateful Inspection sorgt nach korrekter Konfiguration für sicheren Netzwerkzugang. Außerdem lässt sich die Anzahl gleichzeitiger Verbindungen, neuer ein- und ausgehender Verbindungen und neuer ein- und ausgehender „Ping“-Anfragen beschränken, um vor derartigen Attacken geschützt zu sein.

Im Firewall-Bereich bestehen keine Unterschiede zwischen den verschie-

denen Geräte-Varianten, sodass alle den gleichen Schutz bieten.

Zusätzlich zur Firewall lässt sich beim mGuard auch ein Virusschutz installieren. Zum Einsatz kommt dabei die bekannte Kaspersky Embedded Anti Virus Protection. Diese scannt den Datenverkehr auf HTTP-, POP3- und SMTP-Protokollen. Regelmäßige, automatische Online-Updates gehören zum Schutz dazu. Eine Besonderheit ergibt sich durch die kompakte Bauform des mGuard. Diese bietet relativ wenig Speicherplatz, sodass eine Überprüfung von großen Dateien, die auf Viren gefiltert werden sollen, nur schwer möglich ist. Eine Kontrolle der Dateigröße ermöglicht zwei Varianten, entweder Blockade der entsprechenden Datei, bei gleichzeitiger Warnung an den Anwender, oder ein ungeprüftes Passieren betroffener Dateien.

### Systemmanagement

Die Verwaltung der mGuard Devices erfolgt über verschiedene Wege. Die meistgenutzte Variante dürfte wohl der Zugang über den gesicherten HTTP-Zugang sein. Die umfangreichen Einstelloptionen des mGuard werden im Frontend sehr übersichtlich dargestellt. Zusätzliche Hilfe erhält der Anwender durch die ausführlich geratene Dokumentation, die nicht nur die pure Funktion der möglichen Einträge erläutert, sondern auch eine Reihe praktischer Hinweise zur Konfiguration bietet. Eine weitere, wenn auch nicht wirklich komfortable Verwaltung kann der Anwender über einen SSH-Zugang per Kommandozeile initiieren. Als weitere Option steht bei den Enterprise-Varianten eine Steuerung über SNMP (Simple Network Management Protocol) zur Verfügung.

Der Hersteller bietet darüber hinaus noch den Innominate Security Configuration Manager an. Dabei handelt es sich um eine Sammlung

von drei Tools, mit denen sich mehrere mGuards und auch Devices von einigen Fremdherstellern zentral überwachen lassen. Der Hersteller weist ausdrücklich darauf hin, dass diese Lösung nur für größere Stückzahlen an Endgeräten interessant ist, da eine Konfiguration ansonsten über Webbrowser einfacher und auch günstiger ist. Mittels grafischer Darstellung des Netzwerkes lassen sich Firewall-Regeln teilautomatisch generieren und per Knopfdruck auf die verschiedenen Firewalls übertragen. Über diese Darstellung behält der Administrator auch stets einen Überblick über sein Netzwerk, sodass Lücken im Netz besser erkannt werden.

### Fazit

Der mGuard eignet sich für Sicherheitsfälle, bei denen größere Lösungen den Overkill bedeuten würden. Besonders in Umgebungen, in denen der Stealth-Modus zum Einsatz kommen kann, bietet das kleine Gerät unschätzbare Service-Vorteile. Im praktischen Einsatz bei der Gefahrenabwehr verhält sich das Gerät so wie man es erwartet, Port-Scans zeigten keine offenen Stellen, auch gegen DoS- und Flood-Attacken setzt sich das Gerät zur Wehr. Zudem gibt es wenige Daten über sich selbst preis, was Angriffe erschwert. Die zwei unterschiedlichen Bauformen des mGuard dienen dabei unterschiedlichen Szenarien. Die PCI-Variante ist ca. 100 Euro preiswerter als die externen Varianten und bietet sich so als günstige Alternative für den Einbau in einzelne Workstations oder Server an. Der OriginalmGuard, im extrem kleinen, externen Gehäuse eignet sich praktisch ideal für die temporäre Integration von Laptops in bestehende Netze.

Andreas Reitmaier

→ [www.innominate.com](http://www.innominate.com)