PHOENIX CONTACT
INSPIRING INNOVATIONS

FAQ

mGuard IT-related FAQs

1. **What type of security / network protection does the mGuard product line offer?**
   The mGuard offers a wide array of network security including:
   - *Stateful inspection firewall*
   - *Traffic rate limiting for DoS/DDoS protection*
   - *Patented "Stealth Mode" technology to provide "bump-in-the-wire" security without the need to reconfigure the protected devices or network topology*
   - *CIFS Integrity Monitoring and AV Extender technology (license 2701083 required) to ensure the integrity of end devices and provide an additional layer of anti-malware protection*
   - *IPSec VPN for authentication, encryption, and integrity of data flowing across an untrusted network*
   - *A User Firewall requiring authentication into the mGuard via local user/password or RADIUS id; ideal for solutions where users or assets have dynamic IP addresses.*
   - *On-demand initiation of specific firewall rule sets via hardware contact closure. Ideal for tying rulesets to physical events.*
   - *Local and remote (i.e. syslog) logging support*

2. **What network layers or traffic types can the mGuard firewall filter on?**
   The mGuard is capable of filtering on Layer 2 through Layer 4. More specifically individual MAC addresses or MAC ranges (e.g. wildcards such as allowing only 00:a0:45:xx:xx:xx), Ethertype, Source and Destination IP, TCP, UDP, GRE, ICMP and Source and Destination Port.

3. **Does the mGuard have "Layer 7" or Deep Packet Inspection capabilities?**
   The mGuard currently supports Layer 7 support for OPC Classic traffic, ensuring only valid OPC traffic is traversing port 135 and dynamically opening firewall ports as called for by the Client/Server communication. This feature requires an additional license (2702191). Future plans include support for Modbus/TCP and Ethernet/IP DPI support.

4. **How are the mGuard variants different than traditional enterprise appliances (e.g. Cisco, SonicWall, etc)?**
   The FL, TC and GT mGuard variants encompass features traditionally seen only in enterprise router and security appliances in an industrially rugged form factor suitable for control cabinet, plant floor and field deployment. This ruggedization includes:
   - *a wide operating temperature range starting at -20 to +60C (-4 to +140F) and extending as high as -40 to +70C (-40 to 158F)*
   - *high levels of resistance to RF, EMI and other electric "noise" commonly found in a factory or production environment*
   - *DIN-rail mounting and DC power*
   - *Approvals such as UL Class 1 Div 2, ATEX, GL, DNV, etc.*

5. **What routing capabilities does the mGuard product line offer?**
   The mGuard supports both static and dynamic routing. It can be configured for 1:1 NAT (Network Address Translation), Masquerading (aka N:1 NAT) of both incoming or outgoing traffic, and Port Forwarding (aka PAT). Additionally the mGuard is capable of supporting multiple IP addresses/networks on each of its interface to more easily allow mixed network support.

6. **Can the mGuard share dynamic routing information with my enterprise routers?**
   Yes, beginning with firmware 8.3 the mGuard natively supports OSPF (Open Shortest Path First).

7. **Does the mGuard support redundancy?**
   Yes, the mGuard supports VRRP (Virtual Router Redundancy Protocol). This allows it to function in active/standby configuration with its partner and allow for graceful failover of the state of existing firewall connections, routing/NAT traffic, and VPN connections. This redundancy capability requires an additional license (2701356 for Firewall/Routing and 2702244 for Firewall/Routing/VPN)

8. **What are the mGuard VPN capabilities?**
   The mGuard supports standard IPSec VPN connectivity that is compatible with a number of enterprise solutions such as Cisco ASA, SonicWall, etc. X.509 certificate and Pre-Shared Keys are supported for authentication, encryption algorithm supports from DES up to AES-256, all common DH and PFS schemes are supported as well.

FAQ

9. **Will users be able to use the VPN to access the enterprise network?**
   No, the VPN only allows access to the Local Area network or the DMZ network (RS4004 and TC4000 devices); VPN traffic cannot "bounce back" out the WAN port to the enterprise network

10. **Is there an easy way for them to activate/deactivate VPN tunnels?**
    With the FL mGuard, it is possible to enable and disable the tunnel with a contact closure on the mGuard hardware. Make sure you request the special feature configured for this case.

11. **Can I restrict what type of traffic is allowed through the VPN?**
    Yes, the traffic flowing through the VPN can be filtered on any combination of traffic type, source IP, destination IP, source port and destination port. Additionally the "User Firewall" functionality can be extended to VPN traffic, forcing a user to Authenticate to the mGuard or RADIUS server to allow traffic to pass through to the LAN network.