Monnit ALTA Ethernet Gateway 4 Security Brief

The Monnit ALTA® Ethernet Gateway 4 (EGW4) Ethernet network interface consists of the following:

1. Proprietary Operating System
2. WIZnet Hardwired TCP/IP Stack
3. Configurable Socket Interfaces
4. Application-specific Security

All of these modules were selected and designed to meet requirements for IoT Security in today's world.

Proprietary Operating System (OS)

The EGW4 is a purpose-built embedded gateway with a proprietary operating system and static file system. There is no mechanism supported to add programs or viruses to this device.

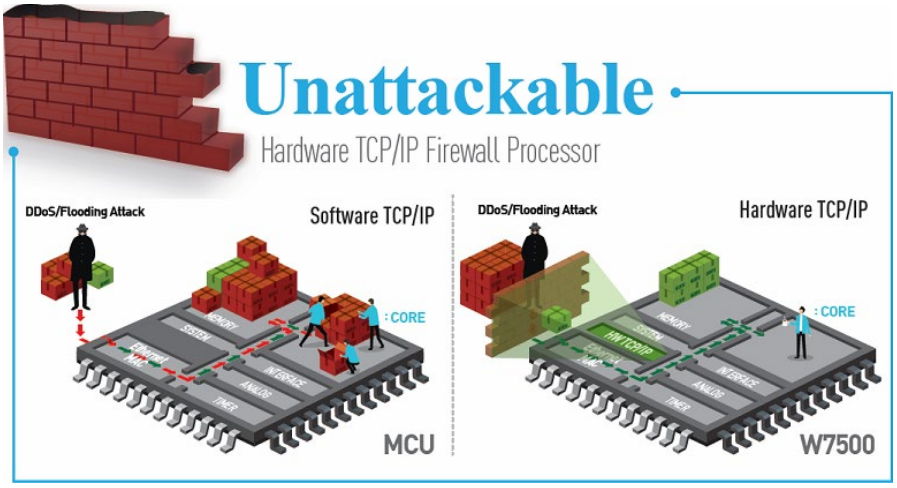
Potential points of attack:

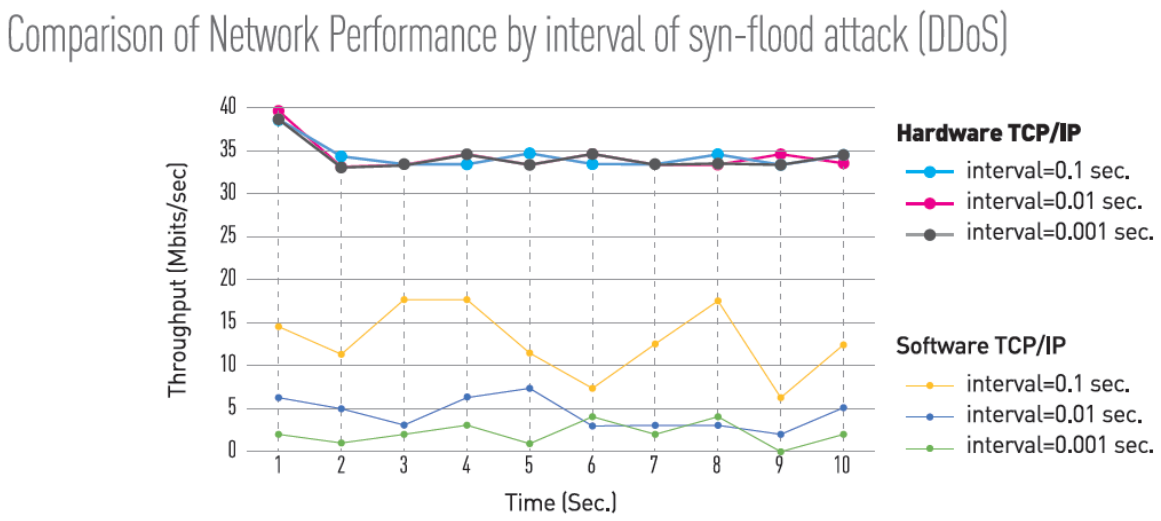
- Device configurations change the behavior of the device.
- The device upgrade mechanism is used to replace code.

Therefore, the gateway interfaces must safeguard how these configurations and code changes occur.

WIZnet Hardwired TCP/IP Stack

WIZnet hardwired TCP/IP Stack is a chip-level "unattackable" hardware network engine for preventing network attacks such as flooding, spoofing, and injection. The hardware TCP/IP Offload Engine (TOE) technology, implemented as hardwired logic from the Ethernet MAC Layer to the TCP/IP Layer, can protect the IoT system against network attack under an excessive number of flooding packets by discarding flooding packets detected. Additionally, the hardware TOE shows superior performance compared to the software TCP/IP stack solutions. The TOE supports up to eight independent hardware sockets concurrently.





Configurable Interfaces

The Ethernet Gateway has the following interface options available:

1. **System Socket Interfaces**: These IP standard sockets implement the standard DHCP, DNS, and SNTP protocols. These protocols, by design, are outbound-based queries used when the gateway is required to automatically establish/maintain the device IP address, resolve “server names” into networked IP addresses, and query a time server. By default, both DHCP and DNS are used by the gateway. SNTP is disabled by default. Additionally, DHCP and DNS sockets cannot be directly disabled. However, if static IP settings are used for the gateway IP settings and an IP address is used instead of a server name, both interfaces will be effectively inactive.
2. **Default Server Interface**: This enables one intermittent outbound TCP port for server communication. By default, this interface is enabled and set to communicate on outbound TCP port 3000. This interface is primarily responsible for providing time for the gateway. The inbound port associated with an open socket is not fixed (TCP Standard implementation). This socket is activated on demand or on a dedicated poll interval (gateway heartbeat setting). After the dialog concludes, the TCP connection is closed. On “unlocked” versions of the gateway, this interface can be disabled, and no socket-level operations are attempted.
3. **Modbus TCP Interface**: This enables one TCP listening socket on a configurable port number. By default, Modbus TCP utilizes the INIA-directed TCP Port 502, and the interface is disabled by default. After this interface is enabled, traffic directed to the configured port number will be sent to the Modbus TCP application for handling.
4. **SNMP v1 Interface**: This enables one UDP listening socket, and up to three UDP Trap sending sockets on configurable port numbers. By default, this interface is disabled and is preconfigured to use the SNMP request port of 161 and SNMP Trap Port of 162 (INIA recommendations). If the interface is enabled, SNMP requests will be received and sent to the SNMP application for handling. If the Trap ports are enabled, the SNMP application can send trap events when they occur.
5. **HTTP Interface**: This enables a local webpage viewing for status and configuration. By default, this interface is enabled on INIA TCP port 80. If enabled, all traffic for this interface is directed to the HTTP application. If the interface is disabled, no socket-level operations are allowed.

Application-specific Security Features

- Default Server Application: This communicates utilizing EncryptRF© and the proprietary Monnit Server (MSVR) protocol. This security suite enables the gateway to form a secure communications link between an authorized server and the gateway. This secure link is authorized to perform gateway configurations. Additionally, gateway updates are only permitted across this secure link, and the gateway verifies the integrity of the new code before completing the updates.
- Modbus TCP Application: This enables Modbus TCP register read-access to collect gateway status and current sensor data. No write access is supported.
- SNMP v1 Application: This enables SNMP OID read-access to collect gateway status and current sensor data. No write-access is supported. If SNMP traps are enabled, the application will initiate qualified Trap events when they occur.
- HTTP Application: This uses the following "access configurations" to control access to this interface:
    - "Read-Only" – Interface will process all HTTP GET requests. This enables the viewing of gateway status and current configurations. However, HTTP POST messages will be ignored, and a read-only warning will be delivered to the caller. This removes this interface's ability to change the operation of the gateway.
    - "5-Minute Access" – For five minutes after a boot event or the pressing of the Gateway Utility button, the gateway will accept HTTP POST messages. This enables configuration changes during this time.
    - "30-Minute Access" – For 30 minutes after a boot event or the pressing of the Gateway Utility button, the gateway will accept HTTP POST messages. This enables configuration changes during this time.
    - "Unlimited Access" – This interface will always accept HTTP POST messages. No security limit here.

Default Enabled Interface Summary:

- DHCP (UDP Port 67) – Standard implementation
- DNS (UDP Port 53) – Standard implementation
- Default Server (TCP Outbound Port 3000) – secured by EncryptRf©, Propriatary MSVR Protocol
- HTTP (TCP Inbound Port 80) – Default as "read-only"