TXOne Release Note - Firmware

<table>
<thead>
<tr>
<th>Product type</th>
<th>Industrial EdgeFire</th>
<th>Release Date</th>
<th>2020/10/20</th>
</tr>
</thead>
</table>

1. Release version
   - Firmware name: ief.fw01_IEF_T01_1.1.3.acf
   - Version: IEF_T01_1.1.3
   - Revision: 09435f3b
   - SHA256 Checksum: 69d1423c97a7945a3d4689b0d85acc1dd339a560ceb8e7989e97a7169dc7cc4
   - Signature info: TM_200806_16

2. Applied models
   - Platform: ARM64
     - IEF-1012-TM

3. Release info
   - TOS: ief_t01_1.1.3
   - Platform (cn80xx): ief_t01_1.1.2
   - Import: ief_t01_1.1.2
   - TDTS: ics/2.3.6

A. Support Features
   - [New Feature] - Active Query supported in “Visibility Page > Asset View”.
   - [New Feature] - DMZ supported in “Network > Network Interface”.
   - [New Feature] - Bridge Mode supported in “Network > Operation Mode”.
   - [New Feature] - IPS Profile (Rule Editing) supported in “Object Profiles > IPS Profiles”.
   - [New Feature] - New OT protocols and options below are supported in “Object Profiles > Protocol Filter Profiles”.
     - Added OT protocols support (Basic Settings) - SECS/GEM and IEC61850-MMS
     - Added OT protocols support (Advanced Settings) - CIP, Siemens S7COMM, Siemens S7COMM PLUS, SLMP, MELSOFT, and TOYOPUC.
     - Added “Drop Malformed” for strictly packet format checking.
     - The maximum profile number increases from 16 to 32.
     - New object types support - IPS profile (New) and protocol filter profiles (New OT Protocols).
     - Added VLAN support in bridge mode (Up to 5 VLAN ID).
     - The maximum rule number increases from 64 to 512.

B. Improvement
   - [Enhancement] - New design of web console.
   - [Enhancement] - Firmware downgrade feature supported.
   - [Enhancement] - LEEF log format supported.
   - [Enhancement] - New log information supported.
     - Cyber Security Logs: Direction, Interface and Attacker
     - Policy Enforcement Logs: Direction and Interface
     - Protocol Filter Logs: Direction and Interface
     - Asset Detection Logs: Interface
   - [Enhancement] – Configuration interface of date and time is optimized in “Administration > System Time”.

TXOne Networks
C. BugFix

- [TXN-1876] - [Common] WEB GUI will crash when the user clicks the dropdown list and resize the browser on some page.
- [TXN-2010] - When the user changes the optional DNS setting in operation mode (bridge mode) and save the configuration, the web console will redirect to the waiting page of switching operation mode.
- [TXN-2019] - After the user configures a DNS address for one time, the optional DNS setting in operation mode (bridge mode) can't be set to blank for configuration.
- [TXN-2034] - [Visibility] In gateway mode, asset interface info is incorrect if the user moves the OT assets from one network interface to another.
- [TXN-2043] - [Policy Enforcement] device pop up the error message “CIDR” is not allowed to be empty' if the CIDR is empty and user input a valid single/range IP
- [TXN-2044] - [Policy Enforcement] Information display of “Total Number of Records” is inconsistent with ODC.
- [TXN-2081] - NAT loopback does not work.

D. Known issue

- [TXN-1255/2070] - [Upgrade] The EdgeFire web console gets "something went wrong" or "An unexpected error occurred" even the user refreshes the browser.
- [TXN-2113] - [Account] Firmware upgrade will be failed w/o error messages if the network is unstable.

E. SW limitation

- Not support WAN2 features.
- Asset visibility detection limitation
  - According to the proprietary protocol and the specific setting in the some OT environment, there is a possibility that EdgeFire cannot detect some OT assets since EdgeFire can support the well-known OT protocol only and do the best effort.
- Some rules of DoS cannot work
  - Due to kernel behavior, conntrack won’t be attached to skbs of which the TCP flag is invalid. For LAN to WAN traffic, SNAT won’t be taken for these packets w/o conntrack and EdgeFire cannot receive RST packets from victims. TCP port NULL/FIN/XMAS scan won’t be detected w/o receiving RST packets in the current design.
- Direction field in logs
  - In gateway mode, this field may display ‘-‘ in logs if the incoming interface of a packet equals to its outgoing interface, including ‘WAN to WAN’ and ‘DMZ to DMZ’.
  - In bridge mode, this field always displays ‘-‘.
- Ports are blocked due to STP
  - In bridge mode, If STP is enabled and a network loop happens, users cannot know which port is blocked in GUI or system logs.

F. Notes

- [TXN-1255] This is a browser cache issue. The browser caches the data of the previous version. To open a new browser can resolve this issue.