

Base de Conhecimento > Tofino > Tofino Configurator 03.0.01 - Project File best practices

## Tofino Configurator 03.0.01 - Project File best practices

- 2023-09-03 - Tofino

## These best practices/design considerations apply to Tofino Configurator 03.0.01

- 1. How many Tofino SAs for the application?
- +One Tofino per every PLC Network Interface Card (NIC)
- + If not possible, feasible or over budget: Add switches in between (Managed Hirschmann) minding the following topics:
- A) Maximum packet rate (do not exceed 8000 pps)
- B) Using port security, such as Port/IP/MAC Security (filtering).
- C) Consider which type of traffic for content inspection:
- i. Modbus TCP or UDP.
- ii. EtherNet/IP, class 3 explicit messaging
- iii. OPC DA\* (not UA, because this one is encrypted),
- + Check or consider allowing SMB traffic.
- 2. Keep maximum 20 Tofino Xenon's per project file (or per productive area).
- 3. Keep maximum 3-5 (depending on data rate) PLC's CPUs behind every Tofino SA.
- 4. Keep <200 firewall rules for every Tofino SA. This avoids download or configuration sessions timeouts. If you got a huge rule-set, bigger than 200 rules, maybe you need to verify if the location of your Tofino SA is the best to secure the process.
- 5. Same for any other network participant: Servers, HMIs, Remote I/O modules, VFDs, etc.
- 6. If traffic is NOT passing and the rules seem to be ok:
- + Change the order of the rules
- +Check direction of your rules.
- 7. If you got a Layer 2 flat network: Use a Tofino Xenon SA.
- 8. If you got different network segments (Layer 3 required): Use an EAGLE One or EAGLE 20/30 with DPI. Now the HiSecOS version 3.0 in the EAGLE 20/30 platform support DPI for:
- A) Modbus TCP

- B) OPC DA
- 9. VLAN's: ensure TC and SA's are members of the sam VLAN (same VLAN-TAG).
- 10. Configure several at the same time? You can do Multi-Config by connecting in parallel.
- + Make sure you use a unique IP Address for every Tofino "virtual" Syslog IP Address, this avoids trouble with monitoring and management.
- 11. The TC programming PC/station's (IP+MAC+Interface connected+Project file) get married with SAs once you make the first "apply" or get the first settings downloaded.
- 12. USB support for v2.0, FAT32.
- 13. Direction of Enforcer Rules should be set in the direction of the REQUEST packets. The REPLY is implied and will be validated by the Enforcer.
- 14. EtherNet/IP CIP Enforcer is only for Class 3 Explicit messaging. It also supports PLC.