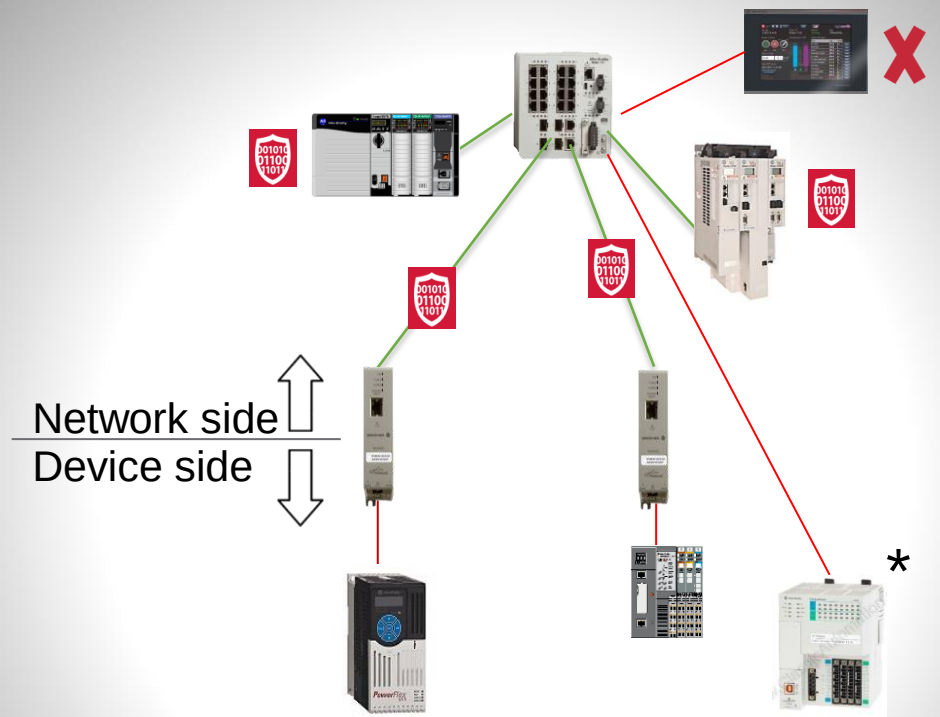
1783-CSP CIP Security™ Proxy

03 . 04 . 2021

Rockwell Automation

1783-CSP: CIP Security Proxy



* Note that in first release, CompactLogix™ controller support will be limited, see other slides

✘ Note that HMI is not supported in first release because proxy cannot open secure connections

Overview

- Standalone hardware solution that provides CIP Security for a single device that does not natively support CIP Security

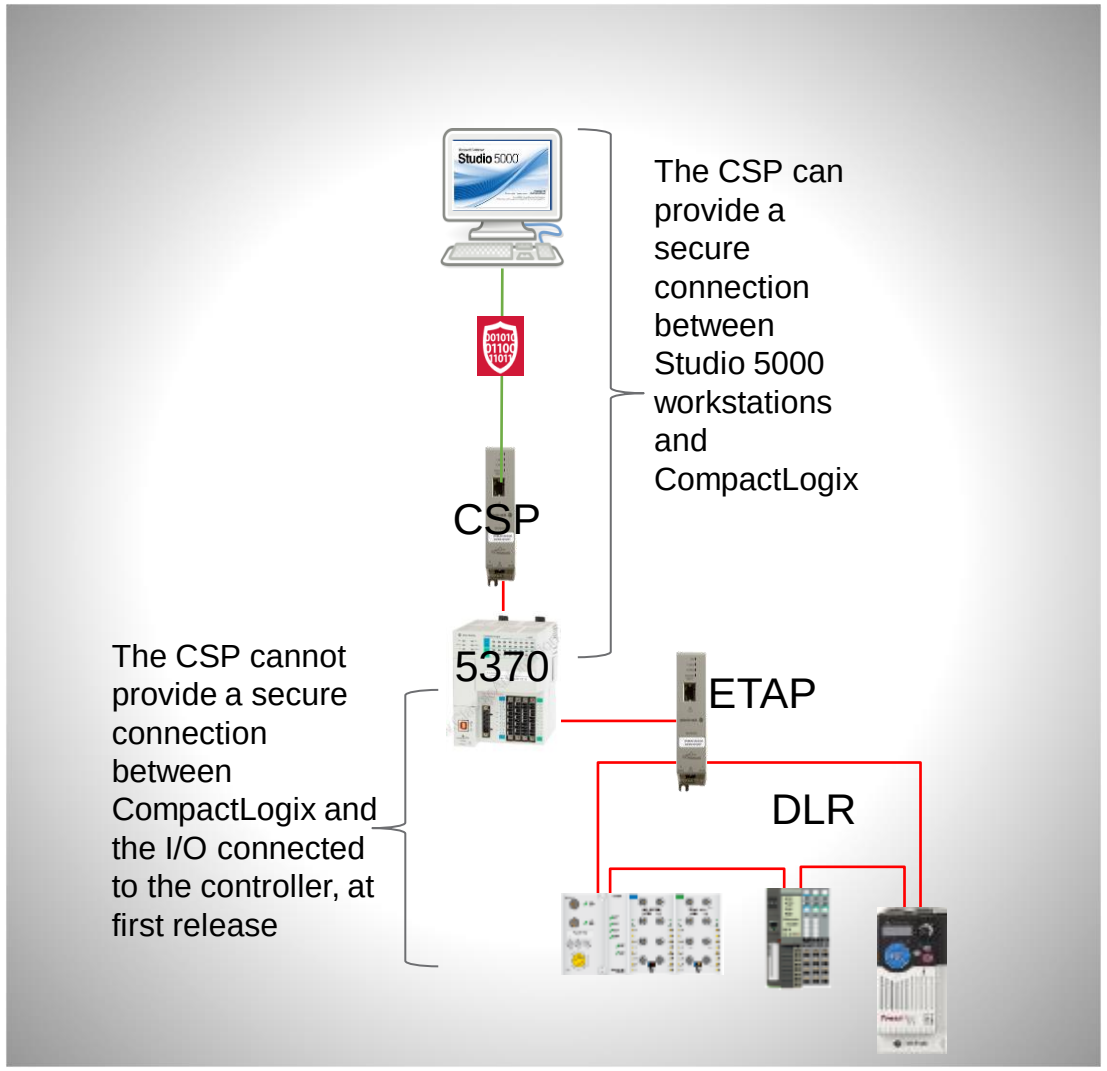
Key Features

- CIP Security
- 10M/100M/1G ports on the network side
- 10M/100M/1G port on the device side
- Support For DLR on network side

Customer Benefits

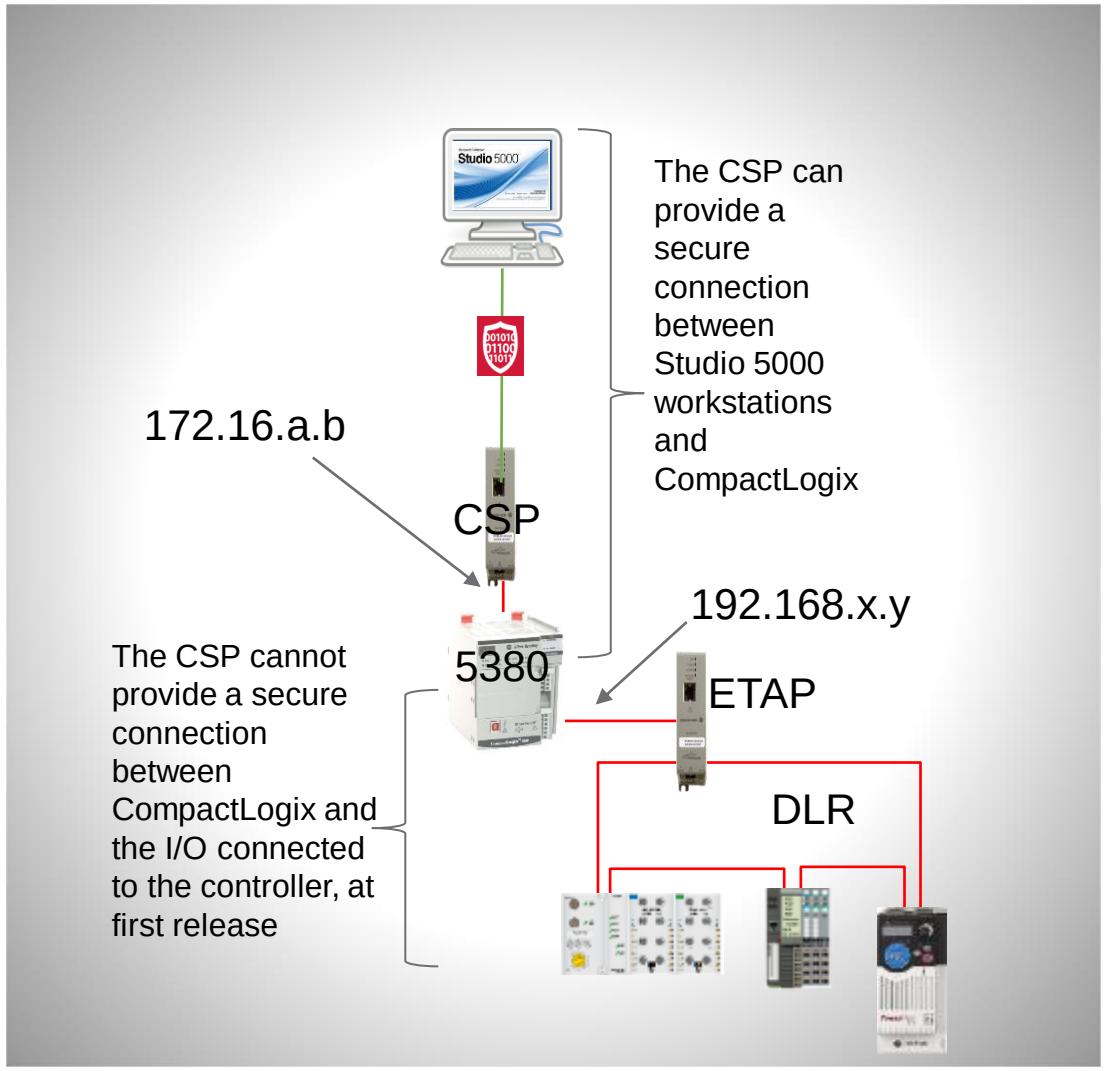
- Allows customers with non-CIP Security embedded products to define and implement their unique migration roadmap to a CIP Security architecture
- Provides a path forward for non-CIP Security capable products

Use CIP Security Proxy to secure the workstation connection to CompactLogix 5370



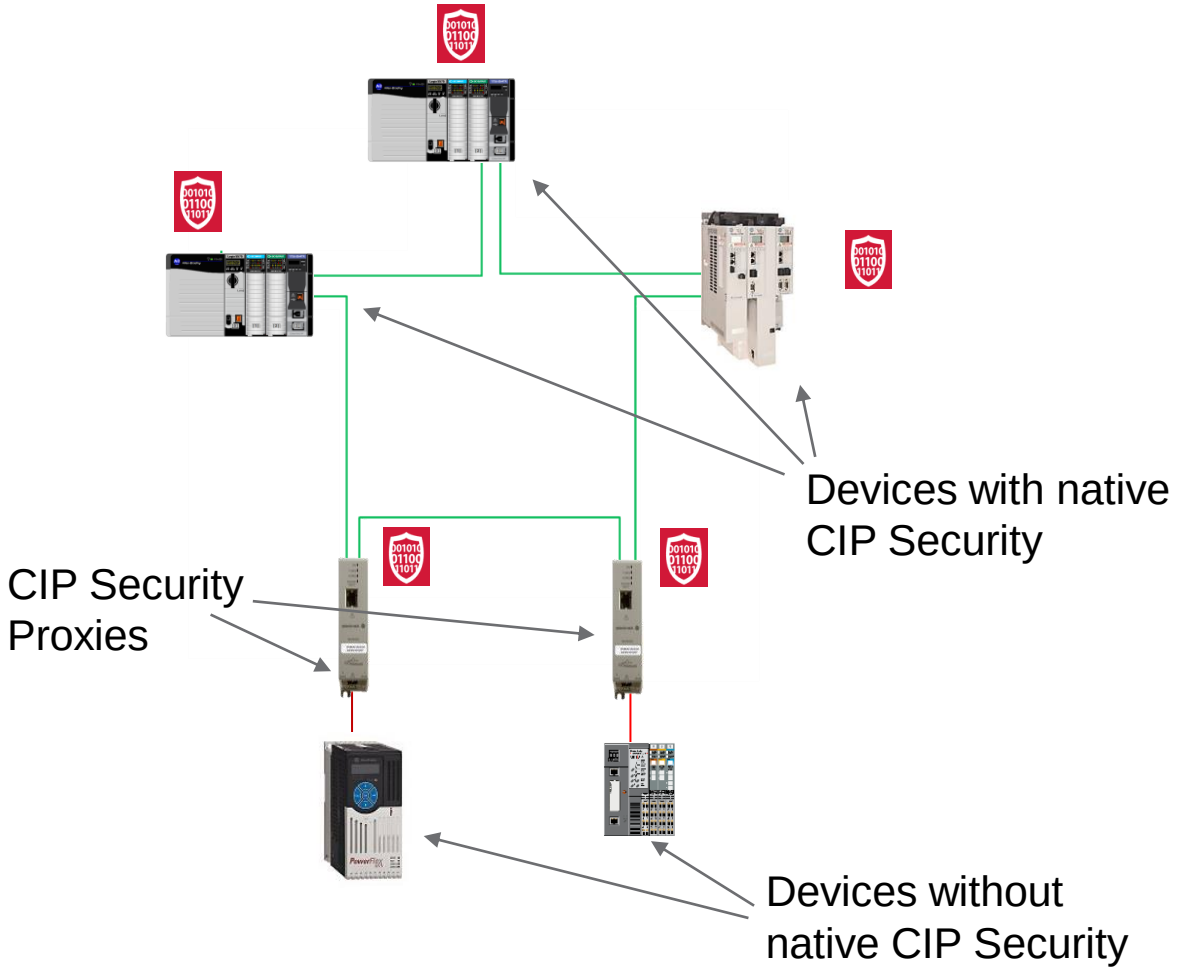
- A CIP Security Proxy can be placed between the CompactLogix 5370 controller and a workstation to secure the workstation connection to the controller.
- One CompactLogix 5370 port is connected to the proxy and then to the workstation, one port of the CompactLogix 5370 to the I/O.
- After the CompactLogix 5370 has been paired to the proxy and CIP Security has been applied, the workstation will no longer be able to browse to the I/O devices because those I/O devices are not part of the security policy. The controller will still be able to control the I/O.
- The CIP Security connection between a CompactLogix 5370 and the proxy must be configured with the I/O devices temporarily disconnected from the controller port. These devices need to be temporarily disconnected so that the CIP Security Proxy discovers only the controller and none of the I/O devices.
- After the proxy is configured with the CompactLogix 5370, the I/O devices that were connected to it can then be connected to the controller via an ETAP or switch. The connection from the controller up to the Studio 5000® workstation is now CIP Security protected.
- Because the connections between the controller and the I/O devices are not CIP Security protected, these devices should all reside in secured enclosures.

Use CIP Security Proxy to secure the workstation connection to CompactLogix 5380



- A CIP Security Proxy can be placed between the CompactLogix 5380 controller and a workstation to secure the workstation connection to the controller.
- One CompactLogix 5380 port is connected to the proxy and then to the workstation, one port of the CompactLogix 5380 to the I/O.
- If the CompactLogix 5380 is in Dual IP Address Mode, after the CompactLogix 5380 has been paired to the proxy and CIP Security has been applied, the workstation will be able to browse to the I/O devices because the controller performs CIP™ routing.
- The CIP Security connection between a CompactLogix 5380 and the proxy must be configured with the I/O devices temporarily disconnected from the controller port. These devices need to be temporarily disconnected so that the CIP Security Proxy discovers only the controller and none of the I/O devices.
- After the proxy is configured with the CompactLogix 5380, the I/O devices that were connected to it can then be connected to the controller via an ETAP or switch. The connection from the controller up to the Studio 5000 workstation is now CIP Security protected.
- Because the connections between the controller and the I/O devices are not CIP Security protected, these devices should all reside in secured enclosures.

1783-CSP: CIP Security Proxy in DLR ring



1783-CSP: CIP Security Proxy

- Provides CIP Security for a single device that does not natively support CIP Security
- 3 EtherNet/IP ports:
  - 1 - 10M/100M/1Gigabit device port
  - 2 - DLR network ports, 10M/100M/1Gigabit
- DLR w/ Ring Supervisor capability
- Rotary switches for 192.168.1.xyz IP addressing
- 24VDC input power
- DIN rail mounted
- Temperature range -25 to +70 degrees C

1783-CSP: CIP Security Proxy

- Configuration through the common CIP Security tools: FactoryTalk® Policy Manager and FactoryTalk System Services
  - Adding the Proxy to the Logix Designer project is optional but not required
- Motion support for Kinetix® drives
- Web server for diagnostics
- Explicit Protected Mode
- Certificates and keys:
  - The proxy will have its own set of certificates and keys
  - The proxy will also maintain a set of certificates and keys for the proxied device
- Throughput:
  - Expected 10,000 pps class 1
  - Expected 1,000 pps class 3
- Secure Event Generation (syslog) support

1783-CSP: CIP Security Proxy

- Certifications:
  - cULus and Haz
  - CE
  - RCM (Australia)
  - KC (Korea)
  - BSMI (EMC, Safety-UL60950, RoHS)
  - UAE RoHS
  - EAC (Russia)
  - DNV GL
  - ATEX, IECEx
  - CE RoHS
  - China RoHS
  - EU Packaging
  - EU WEEE

1783-CSP: CIP Security Proxy

- Future releases:
  - Secure connection origination
    - Because the proxy cannot open connections, the initial release cannot support HMI or secure a controller on the port that is opening I/O connections
  - K and XT versions

- Other solutions available to add CIP Security
  - Computers should use FactoryTalk Linx to provide CIP Security
  - Use devices with CIP Security natively built in, such as 1756-EN4TR
  - Add devices to the model that do not have CIP Security built in (results in permitted communications but not secure communications)
    - Not as secure of a solution