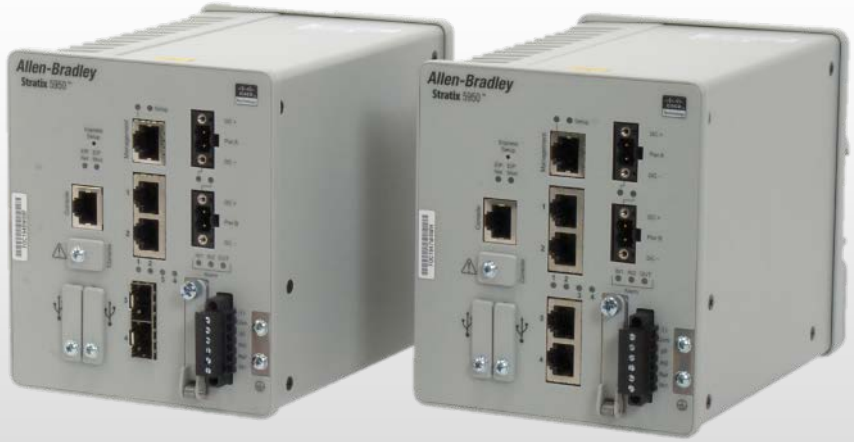


Stratix® 5950 Security Appliance

June 2019

Rockwell Automation

Agenda

1 Connected Enterprise Message

2 Differentiating Factors

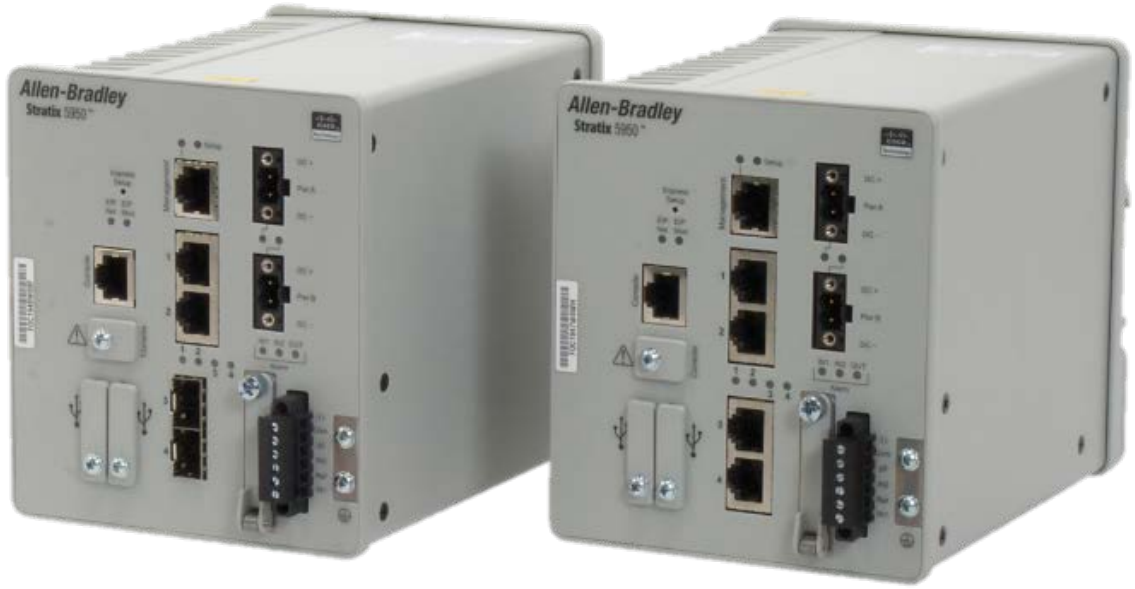
3 Firewall Features

4 DPI Features

5 CIP categories

6 New Features

Stratix® 5950 Security Appliance



The Stratix® 5950 Security Appliance brings an industrially-hardened security product to the networks and security infrastructure portfolio of products. The Stratix® 5950 Security Appliance helps provide increased visibility and control with Deep Packet Inspection (DPI) capabilities to help protect your assets down to the machine level.

Stratix® 5950 Security Appliance

Applications

The Stratix® 5950 security appliance is ideal for resolution of the following challenges:

Lacking visibility and control to help prevent erroneous activity and to **maintain integrity of operations** on the plant floor For example, prevention of tampered firmware being downloaded to a Controller by confirming only an authorized user can conduct the download		**Intrusion Prevention** capability and detailed network visibility which enhances traditional **firewall** functionality to allow for informed decision making through the use **of Deep Packet Inspection technology**
Threat control for vulnerable Industrial Control Systems (**ICS**) devices, and/or **legacy equipment** Protection against communications from ICS components at risk of compromise		Allows for vulnerability identification and mitigation through configuration of policies to **block actions, like CIP™ protocol Reads, Writes, and Downloads** to provide protections for communications with ICS devices like HMI, etc.

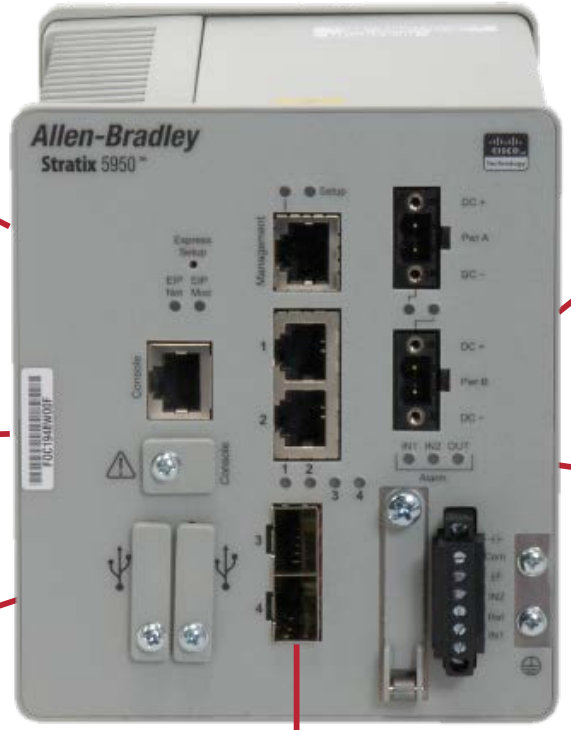
Stratix® 5950 security appliance addresses the challenge for Industrial Automation professionals to maintain operations integrity while making data more available from the ICS

Stratix® 5950 Security Appliance Differentiators

Maintain your protection against threats and control your assets with subscription based licensing

DIN rail mount offers increased design flexibility

Deep Packet Inspection technology provides the visibility and controls needed for implementing policies around access, applications, and protocols on the plant floor



Industrially-hardened for high temperature demands (-40°C to 60°C)

Cisco® ASA firewall and FirePOWER® technology provide prevention services to identify, log or block potentially malicious traffic

SFP slots enable flexibility by allowing multiple options for fiber connectivity

Firewalls and Deep Packet Inspection

- Typical IT firewalls are capable of inspecting
  - Source or destination MAC or IP Address
  - Source or destination TCP or UDP Ports, or
  - Protocol elements of a packet
- Deep Packet Inspection extends upon these firewalls' capabilities
  - Provides granular protection per protocol (ex. CIP™ protocol, Modbus, DNP3) in the Industrial Zone
  - Giving the visibility and control to help prevent erroneous or malicious activity down to the Cell / Area zone level
- Intrusion Prevention uses DPI
  - What you want to do after you have inspected the packet?
  - After inspecting the packet using DPI, achieve granular control through security rules that act on matched network traffic
  - Do we allow this application or command, or is this a known threat?

IPS – IDS – Firewall Comparison

IPS	• Inspects traffic flowing through a network and is capable of blocking what it determines to be malicious
IDS	• Similar to IPS but does not affect traffic flows in any way; only logs or alerts on malicious traffic
Firewall	• Helps prevent or allow traffic between interfaces based on policies • Often use network address translation (NAT) to isolate private network addresses from public ones • May inspect traffic for conformance with proper protocol behavior

7

Deep Packet Inspection (DPI) Features

- DPI functionality is required to inspect the packet past the basic header information at the protocol level.
- DPI determines the contents of a particular packet, and then either:
  - Records that information for statistical purposes, or
  - Performs an action on the packet such as permit or discard.
- DPI is a capability used by Intrusion Detection (IDS) and Intrusion Prevention (IPS). IPS and IDS relate to what is to be done after the packet has been inspected by DPI.
- Protocol interpretation is added to the DPI module so that an administrator can configure DPI rules to monitor, log, and permit or deny packets as they relate to the protocol.

CIP™ Protocol Categories

- The preprocessor is responsible for handling the interpretation of the packet before being handled by the rules engine. The Industrial Firewall has a CIP™ protocol preprocessor that is capable of interpreting the it. This allows the system administrator to author policy rules related to the CIP™ protocol actions.
- Two types of CIP™ DPI rule categories:
  - CIP™ generic – Related to the open CIP™ standard
  - Rockwell Automation specific CIP™ protocol - CIP™ protocol extensions specific to Rockwell Automation products

Categories	Description	Application(s)	Usage
CIP™ Rockwell Automation Admin	Rockwell Automation specified commands that change the state of a device	• CIP™ Admin • CIP™ Rockwell Automation Admin Download • CIP™ Rockwell Automation Admin Firmware Update • CIP™ Rockwell Automation Admin Other	• Block ControlFlash or any tool that flashes Rockwell Automation® firmware • Blocks Rockwell Automation® Logix Designer from Downloading programs • Uses RSLinx® software to change a module's networking properties, such as: IP address, netmask, gateway, DNS server, domain name, host name, speed, duplex mode, interface speed • Uses any tool to reset a device
CIP™ Rockwell Automation Read	Rockwell Automation specified commands that read data from a device	• CIP™ Infrastructure , CIP Read • CIP™ Rockwell Automation Infrastructure • CIP™ Rockwell Automation Read Tag • CIP™ Read Tag Other	Any general read action. Example: RSLinx® software browsing, HMI reading a tag
CIP™ Rockwell Automation Write	Rockwell Automation specified commands that write data into a device	• CIP™ Write • CIP™ Rockwell Automation Write Tag • CIP™ Rockwell Automation Write Tag Other	Block tools or commands that set values via CIP™ protocol. Example: HMI setting a tag value, RSLinx® software changing various properties of a device (properties that don't fall under CIP™ Rockwell Automation Admin)

Summer 2019 New Features

- Overview:
  - First firmware update to be released for the Stratix® 5950 security appliance (v6.4.0)
  - Targeting Summer 2019 Available for Customers via PCDC

- New Features:
  - URL filtering - allows customer to write a condition in an access control rule in order to determine the traffic that traverses a network based on non-encrypted URL requests by the monitored hosts.
  - Advanced Malware Protection - can detect, track, store, analyze, and optionally block the transmission of malware in network traffic.
  - Denial of Service Vulnerability fix
  - No hardware changes needed for these features

Thank you

www.rockwellautomation.com

Rockwell Automation