L03 - Introduction to Network Security
Agenda

- Introduction
- Network Security
- Labs
- Wrap up
- Survey
Network Switch Product Overview

**Stratix® 5400**
- Layer 2 or Layer 3 routing firmware
- 8–20 ports
- 4 port or all gig port versions
- IEEE1588 PTP
- Integrated NAT
- Up to 8 separate integrated NAT ports
- Up to 12 PoE/PoE+ ports
- PRP (RedBox)
- DC and AC power input options

**Stratix® 5410**
- 19 in Rack Mount
- Layer 2 or Layer 3 routing firmware
- 28 ports
- All gig ports plus four 10 gig ports
- IEEE1588 PTP
- Up to 8 separate integrated NAT ports
- Up to 12 PoE/PoE+ ports
- PRP (RedBox)
- DC and AC power input options

**Features**
- Layer 2 firmware
- 6–20 ports
- IP30 and IP67 On-Machine™ platform
- Integrated DLR
- Integrated NAT
- IEEE1588 PTP
- PoE/PoE+
- Layer 2 or layer 3 routing firmware
- 6–26 ports
- Modular platform for maximum flexibility
- IEEE1588 PTP
- PoE/PoE+
- Layer 2 or Layer 3 routing firmware
- 8–20 ports
- 4 port or all gig port versions
- IEEE1588 PTP
- Integrated NAT
- Up to 8 separate integrated NAT ports
- Up to 12 PoE/PoE+ ports
- PRP (RedBox)
- DC and AC power input options

**Stratix® 2000**
- 5–16 ports
- Fiber port options
- Gig port option
- Plug & play

**Stratix® 6000**
- 5–9 port
- Lightly managed
- Gig Fiber option

**Stratix® 2500**
- 5–9 port
- Basic
- Traffic management
- Diagnostics
- Security

**Stratix® 5700/ArmorStratix™ 5700**
- Layer 2 firmware
- 6–20 ports
- IP30 and IP67 On-Machine™ platform
- Integrated DLR
- Integrated NAT
- IEEE1588 PTP
- PoE/PoE+

**Stratix® 8000/Stratix 8300**
- Layer 2 or layer 3 routing firmware
- 6–26 ports
- Modular platform for maximum flexibility
- IEEE1588 PTP
- PoE/PoE+

**Stratix® 2000**
- 5–16 ports
- Fiber port options
- Gig port option
- Plug & play

**Stratix® 6000**
- 5–9 port
- Lightly managed
- Gig Fiber option

**Stratix® 2500**
- 5–9 port
- Basic
- Traffic management
- Diagnostics
- Security

**Stratix® 5700/ArmorStratix™ 5700**
- Layer 2 firmware
- 6–20 ports
- IP30 and IP67 On-Machine™ platform
- Integrated DLR
- Integrated NAT
- IEEE1588 PTP
- PoE/PoE+

**Stratix® 8000/Stratix 8300**
- Layer 2 or layer 3 routing firmware
- 6–26 ports
- Modular platform for maximum flexibility
- IEEE1588 PTP
- PoE/PoE+

**Stratix® 5410**
- 19 in Rack Mount
- Layer 2 or Layer 3 routing firmware
- 28 ports
- All gig ports plus four 10 gig ports
- IEEE1588 PTP
- Up to 8 separate integrated NAT ports
- Up to 12 PoE/PoE+ ports
- PRP (RedBox)
- DC and AC power input options

**Stratix® 5400**
- Layer 2 or Layer 3 routing firmware
- 8–20 ports
- 4 port or all gig port versions
- IEEE1588 PTP
- Integrated NAT
- Up to 8 separate integrated NAT ports
- Up to 12 PoE/PoE+ ports
- PRP (RedBox)
- DC and AC power input options

**Stratix® 5700/ArmorStratix™ 5700**
- Layer 2 firmware
- 6–20 ports
- IP30 and IP67 On-Machine™ platform
- Integrated DLR
- Integrated NAT
- IEEE1588 PTP
- PoE/PoE+

**Stratix® 8000/Stratix 8300**
- Layer 2 or layer 3 routing firmware
- 6–26 ports
- Modular platform for maximum flexibility
- IEEE1588 PTP
- PoE/PoE+

**Stratix® 5410**
- 19 in Rack Mount
- Layer 2 or Layer 3 routing firmware
- 28 ports
- All gig ports plus four 10 gig ports
- IEEE1588 PTP
- Up to 8 separate integrated NAT ports
- Up to 12 PoE/PoE+ ports
- PRP (RedBox)
- DC and AC power input options
Networks & Security Infrastructure Portfolio

**MANAGED SWITCHES**
Stratix®
- Access switches & distribution switches
- High-Performance switching up to 10 GB
- Integrated Network Address Translation
- Integrated DLR with three ring support
- IT and OT configuration and support tools

**LIGHTLY MANAGED & UNMANAGED SWITCHES**
Stratix®
- Low-cost, compact solutions
- Automatically negotiates speed and duplex settings
- No configuration required, or can be configured to support security, resiliency and bandwidth optimization

**WIRELESS TECHNOLOGY**
Stratix®
- Connect hard-to-reach and remote areas
- Mobile access to equipment and key business systems
- Minimizes hardware and wiring

**SECURITY APPLIANCES**
Stratix®
- Secure real-time control communication
- Intrusion prevention using Deep Packet Inspection capabilities
- Routing and firewall capabilities
- Access control lists

**1756-Communication Modules**
- Establishes communication links between devices and ControlLogix® controller
- Can use EtherNet/IP, ControlNet, and DeviceNet network protocols
- Supports both real-time I/O messaging and message exchange

**Gateways and Linking Devices**
- Connects information/control networks to device level networks
- Leverages existing network structures for migrations
Reference Architectures
Converged Plantwide Ethernet (CPwE)

- Tested, validated and documented reference architectures
  - Developed from use cases - customer and application
  - Tested for performance, availability, scalability and security
  - Comprised of Cisco and Rockwell Automation® Validated Designs
- Built on technology and industry standards
- “Future-ready” network design
- Content relevant to both OT and IT Engineers
- Recommendations, best practices, design and implementation guidance, documented test results and configuration settings
- Simplified design, quicker deployment, reduced risk in deploying new technology
# Additional Material

<table>
<thead>
<tr>
<th>Topic</th>
<th>Design Guide</th>
<th>Whitepaper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design Considerations for Securing IACS Networks</td>
<td>—</td>
<td>ENET-WP031A-EN-P</td>
</tr>
<tr>
<td>Converged Plantwide Ethernet – Baseline Document</td>
<td>ENET-TD001E-EN-P</td>
<td>—</td>
</tr>
<tr>
<td>Resilient Ethernet Protocol in a CPwE Architecture</td>
<td>ENET-TD005B-EN-P</td>
<td>ENET-WP033A-EN-P</td>
</tr>
<tr>
<td>Deploying 802.11 Wireless LAN Technology within a CPwE Architecture</td>
<td>ENET-TD006A-EN-P</td>
<td>ENET-WP034A-EN-P</td>
</tr>
<tr>
<td>Deploying Identity Services within a CPwE Architecture</td>
<td>ENET-TD008A-EN-P</td>
<td>ENET-WP037A-EN-P</td>
</tr>
<tr>
<td>Securely Traversing IACS Data Across the Industrial Demilitarized Zone (IDMZ)</td>
<td>ENET-TD009A-EN-P</td>
<td>ENET-WP038A-EN-P</td>
</tr>
<tr>
<td>Deploying Network Address Translation within a CPwE Architecture</td>
<td>ENET-TD007A-EN-P</td>
<td>ENET-WP036A-EN-P</td>
</tr>
<tr>
<td>Migrating Legacy IACS Networks to a CPwE Architecture</td>
<td>ENET-TD011A-EN-P</td>
<td>ENET-WP040A-EN-P</td>
</tr>
<tr>
<td>Deploying A Resilient Converged Plantwide Ethernet Architecture</td>
<td>ENET-TD010A-EN-P</td>
<td>ENET-WP039B-EN-P</td>
</tr>
<tr>
<td>Site-to-site VPN to a CPwE Architecture</td>
<td>ENET-TD012A-EN-P</td>
<td>—</td>
</tr>
<tr>
<td>Deploying Industrial Firewalls within a CPwE Architecture</td>
<td>ENET-TD002A-EN-P</td>
<td>ENET-WP011B-EN-P</td>
</tr>
<tr>
<td>Agenda</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Network Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Labs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wrap up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Survey</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Growing Need for Industrial Security

51% Do not feel prepared for security attacks that abuse, exploit, or maliciously leverage insecure IIoT devices

64% Already recognize the need to protect against IIoT attacks

94% Expect IIoT to increase risk and vulnerability

96% Expect to see an increase in security attacks on IIoT in 2017

90% Expect IIoT deployment to rise

96% Large Companies Expect a significant increase in risk caused by the use of IIoT

93% Small Companies

The Industrial Internet of Things ultimately delivers value to organizations, and that’s why we’re seeing an increase in deployments. Security can’t be an industry of ‘no’ in the face of innovation, and businesses can’t be effective without addressing risks.

While IIoT may bring new challenges and risks, the fundamentals of security still apply. Organizations don’t need to find new security controls, rather they need to figure out how to apply security best practices in new environments.

—Tim Erlin
Director, Security and IT Risk Strategist, Tripwire
Threat examples

WHAT’S NEXT?

....Your organization failed to consider impact of exploiting control systems....

Target Retail Stores - 2013  BACKDOOR ATTACK

The attackers backed their way into network by compromising a 3rd-party vendor to steal data.

Kemuri Water Company - 2016  PLC ATTACK

Hacked access hundreds of PLCs used to manipulate control applications altering chemicals.

Saudi Aramco & RasGas  ENTERPRISE ATTACK

Networks infected with the Shamoon virus erased information causing enterprise network outages.

Ukraine Utilities - 2015  SCADA ATTACK

Left 225,000 customers in the dark. 1st successful cyber attack to knock a power grid offline.

Project Basecamp - 2012  PLC ATTACK

A team used a penetration test on PLCs to realize how badly vulnerable their SCADA/ICS were.

Unnamed Steel Mill, Germany - 2014  INSIDER ATTACK

Hackers disrupted networks to access automation equipment resulted in massive damage.

“Unnamed” Steel Mill - 2011  ENTERPRISE INFECTION

The Conficker worm infected the control network causing an instability in the communications.

New York Dam - 2013  BACKDOOR ATTACK

Iranian hackers tried to open flood gates. Was this a dress rehearsal for something bigger?

Natanz Nuclear Facility - 2010  SCADA MALWARE

Stuxnet infected the air-gapped control network bypassing causing damage to centrifuge.

Google HQ, Wharf - 2013  MISS-CONFIGURE

SHODAN discovered over 21,000 mis-configured building automation systems.

Maroochy Water System - 2010  INSIDER ATTACK

Disgruntled ex-employee hacks into the water system and floods the community of sewage.
Holistic Approach

A secure application depends on multiple layers of protection and industrial security must be implemented as a system.

- **Defense in Depth**
  Shield targets behind multiple levels of security countermeasures to help reduce risk

- **Openness**
  Consideration for participation of various vendors in our security solutions

- **Flexibility**
  Able to accommodate a customer’s needs, including policies and procedures

- **Consistency**
  Solutions that align with Government directives and Standards Bodies
Stratix® 5950 Security Appliance

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

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

DIN rail mount offers increased design flexibility

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

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

Two Models:
- 2-port Copper & 2-port SFP
- 4 Port Copper

SFP slots enable flexibility by allowing multiple options for fiber connectivity
Architectures

- Use the Stratix® 5950 security appliance to help protect at the skid, machine and equipment zones.
Why the Stratix® 5950 Security Appliance?

- Network Security in the Industrial Automation Control System (IACS) world is becoming a growing concern
  - IACS networks are growing more into the EtherNet/IP space
  - Connecting the IACS network to the corporate network exposes risk to both networks
    - Risk requires mitigation
    - Cyber security attacks require action
  - Legacy products contain vulnerabilities – Virtual patching
- It’s better to assess your risks and help protect your network now than play catchup after being compromised
Why the Stratix® 5950 Security Appliance?

Legacy IACS and IACS-networks are no longer being actively updated.

- Zero-day vulnerabilities continue to be discovered in these devices
- It can be cost-prohibitive to change-out legacy IACS
Why the Stratix® 5950 Security Appliance?

Virtual Patching

- Using technologies within the Stratix® 5950 security appliance, the Stratix® 5950 can be updated for new exploits and vulnerabilities
  - With Cisco® Talos™, Rockwell Automation provides the subscription for updates on the Stratix® 5950 security appliance that can download new rules
  - The Stratix® 5950 security appliance can download the rule so that the device can help “detect” or “prevent” that traffic based on the known threat characteristics
## IT/OT Priorities

<table>
<thead>
<tr>
<th>Security Policies</th>
<th>IT Networks</th>
<th>OT Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Focus</strong></td>
<td>Protecting Intellectual Property and Company assets</td>
<td>24/7 Operations, Safety, Ease of use, High OEE</td>
</tr>
</tbody>
</table>
| **Priorities**          | 1. Confidentiality  
                        | 2. Integrity                                           | 1. Availability                                           |
|                         | 3. **Availability**                               | 2. Integrity                                           |
| **Types of Traffic**    | Converged Network of Data Voice and Video (Hierarchical) | Converged Network of Data Control Protocols, Information, Safety and Motion (P2P & Hierarchical) |
| **Access Control**      | Strict Network Authentication and Access Policies | Strict Physical Access Simple Network Device Access      |
| **Implications of device failure** | Continue to Operate | Could stop processes, impact markets Physical Harm |
| **Threat Protection**   | Shutdown access to detected threat and remediate | Potentially keep operating with detected threats         |
| **Upgrades and Patch Mgmt** | ASAP During uptime | Scheduled During downtime |
OT Maintenance Cycles

- Monthly
- Quarterly
- Yearly
Pre-lab

- How many people know what a certificate is and how it works?
- How many people have noticed that the Stratix® Device Manager is now using certificates through something called https?
Pre-lab: What we’re doing

- We will be connecting to a Stratix® switch
  - We will be viewing the certificate the switch presents to our computer
  - We will trust this certificate so we can gain access to the switch
- We will compare this certificate to a trusted website
  - Rockwell Automation in this case
- At the end of the lab you should understand how to view and validate a certificate
- Stratix® switches are shipping with crypto or secure firmware by default
What are certificates?

- What does this certificate mean to me and why do I need it?
  - Think of the certificate as a form of identification, similar to your drivers license and social security number
- One added benefit of a certificate is it allows for encryption of data
What is encryption?

The dictionary defines encrypt as:

To alter information using a code or mathematical algorithm to be unintelligible to unauthorized readers
What is encryption?

The dictionary defines encrypt as:

- To alter information using a code or mathematical algorithm to be unintelligible to unauthorized readers
Encryption?

To **alter** information using a code or mathematical algorithm to be **unintelligible** to unauthorized readers
## Encryption?

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Source</th>
<th>Port</th>
<th>Protocol</th>
<th>Method</th>
<th>Path</th>
<th>Status</th>
<th>Reason</th>
<th>Headers</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>192.168.1.149</td>
<td>80</td>
<td>HTTP</td>
<td>GET</td>
<td>/homed.shtml</td>
<td>301</td>
<td>Redirect</td>
<td>Location: /index.html</td>
</tr>
<tr>
<td>192.168.1.11</td>
<td>192.168.1.11</td>
<td>22</td>
<td>TCP</td>
<td>SFTP</td>
<td></td>
<td>200</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>192.168.1.149</td>
<td>0.236344 Rockwell_cd:00:34</td>
<td>80</td>
<td>HTTP</td>
<td>GET</td>
<td>/homed.shtml</td>
<td>301</td>
<td>Redirect</td>
<td>Location: /index.html</td>
</tr>
<tr>
<td>192.168.1.11</td>
<td>0.778866 Rockwell_14:29:84</td>
<td>80</td>
<td>HTTP</td>
<td>GET</td>
<td>/homed.shtml</td>
<td>301</td>
<td>Redirect</td>
<td>Location: /index.html</td>
</tr>
<tr>
<td>192.168.1.11</td>
<td>0.115848 Rockwell_cd:00:34</td>
<td>80</td>
<td>HTTP</td>
<td>GET</td>
<td>/homed.shtml</td>
<td>301</td>
<td>Redirect</td>
<td>Location: /index.html</td>
</tr>
</tbody>
</table>

### HTTP Headers

- **Host**: 192.168.1.1
- **User-Agent**: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
- **Accept**: */*
- **Accept-Language**: en-US,en;q=0.5
- **Connection**: keep-alive
- **Authorization**: Basic cm9ja3dlbGw6cm9ja3dlbGw=
- **Credentials**: rockwell:rockwell

---

```plaintext
[Next sequence number: 322 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 ..... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 64240
[Calculated window size: 64240]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x8542 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
TCP payload (321 bytes)
```

---

**Hypertext Transfer Protocol**

GET /homed.shtml HTTP/1.1

Host: 192.168.1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

Accept: */*

Accept-Language: en-US,en;q=0.5

Connection: keep-alive

**Authorization**: Basic cm9ja3dlbGw6cm9ja3dlbGw=

**Credentials**: rockwell:rockwell
Encryption?
[Next sequence number: 322] [relative sequence number]
Acknowledgment number: 1 [relative ack number]
0101 .... = Header Length: 20 bytes (5)

• Flags: 0x018 [PSH, ACK]
Window size value: 64240
[Calculated window size: 64240]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x8542 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

• [SEQ/ACK analysis]
TCP payload (321 bytes)

Hypertext Transfer Protocol
GET /home.js.html HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0) Gecko/2010011
Accept: */*
Accept-Language: en-US, en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.1/
DNT: 1
Connection: keep-alive

Authorization: Basic cm9ja3dlbGw6cm9jaWwuY29t

Credentials: rockwell:rockwell
Encryption?

- How do we help prevent our data from being read or overheard?
Encryption

- How do we help prevent our data from being read or overheard?
Encryption

To **alter** information using a code or mathematical algorithm to be **unintelligible** to unauthorized readers.
## Encryption

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>0.000933</td>
<td>192.168.1.1</td>
<td>192.168.1.149</td>
<td>TLSv1.2</td>
<td>107</td>
<td>Encrypted Alert</td>
</tr>
<tr>
<td>17</td>
<td>0.000175</td>
<td>192.168.1.149</td>
<td>192.168.1.1</td>
<td>TCP</td>
<td>54</td>
<td>62273 → 443 [ACK] Seq=676 Ack=1260 Win=62982 Len=0</td>
</tr>
<tr>
<td>18</td>
<td>0.000913</td>
<td>192.168.1.149</td>
<td>192.168.1.1</td>
<td>TCP</td>
<td>54</td>
<td>62273 → 443 [FIN, ACK] Seq=676 Ack=1260 Win=62982 Len=0</td>
</tr>
<tr>
<td>19</td>
<td>0.001635</td>
<td>192.168.1.149</td>
<td>192.168.1.1</td>
<td>TCP</td>
<td>66</td>
<td>62274 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256</td>
</tr>
<tr>
<td>20</td>
<td>0.000033</td>
<td>192.168.1.1</td>
<td>192.168.1.149</td>
<td>TCP</td>
<td>60</td>
<td>443 → 62274 [ACK] Seq=1260 Ack=677 Win=3453 Len=0</td>
</tr>
<tr>
<td>21</td>
<td>0.002242</td>
<td>192.168.1.1</td>
<td>192.168.1.149</td>
<td>TCP</td>
<td>60</td>
<td>443 → 62274 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460</td>
</tr>
<tr>
<td>22</td>
<td>0.000283</td>
<td>192.168.1.149</td>
<td>192.168.1.1</td>
<td>TCP</td>
<td>54</td>
<td>62274 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0</td>
</tr>
<tr>
<td>23</td>
<td>0.000666</td>
<td>192.168.1.149</td>
<td>192.168.1.1</td>
<td>TLSv1.2</td>
<td>254</td>
<td>Client Hello</td>
</tr>
<tr>
<td>24</td>
<td>0.003301</td>
<td>192.168.1.149</td>
<td>192.168.1.1</td>
<td>TCP</td>
<td>60</td>
<td>443 → 62274 [ACK] Seq=1 Ack=201 Win=3928 Len=0</td>
</tr>
<tr>
<td>25</td>
<td>0.004733</td>
<td>192.168.1.149</td>
<td>192.168.1.1</td>
<td>TLSv1.2</td>
<td>939</td>
<td>Server Hello, Certificate, Server Key Exchange, Server Key</td>
</tr>
<tr>
<td>26</td>
<td>0.012126</td>
<td>192.168.1.149</td>
<td>192.168.1.1</td>
<td>TLSv1.2</td>
<td>204</td>
<td>Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message</td>
</tr>
<tr>
<td>27</td>
<td>0.017195</td>
<td>192.168.1.149</td>
<td>192.168.1.1</td>
<td>TLSv1.2</td>
<td>129</td>
<td>Change Cipher Spec, Encrypted Handshake Message</td>
</tr>
<tr>
<td>28</td>
<td>0.001674</td>
<td>192.168.1.149</td>
<td>192.168.1.1</td>
<td>TLSv1.2</td>
<td>427</td>
<td>Application Data</td>
</tr>
</tbody>
</table>

- Frame 28: 427 bytes on wire (3416 bits), 427 bytes captured (3416 bits)
- Transmission Control Protocol, Src Port: 62274, Dst Port: 443, Seq: 3

**Secure Sockets Layer**

- TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
- Content Type: Application Data (23)
- Version: TLS 1.2 (0x0303)
- Length: 368

**Encrypted Application Data**: f6c82d725a83b14dfc8e500f02f58b-f21d1
Encryption

[Next sequence number: 322  (relative sequence number)]
Acknowledgment number: 1  (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 64240
[Calculated window size: 64240]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x8542 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

TCP payload (321 bytes)

Hypertext Transfer Protocol
GET /home.html HTTP/1.1\r\nHost: 192.168.1.11\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0) Gecko/201001
Accept: */*\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nReferer: http://192.168.1.11\r\nDNT: 1\r\nConnection: keep-alive\r\nAuthorization: Basic cm9ja33db6w6cm9ja33db6w=\r\n
Encrypted Application Data: f6c82d725a83b14dfc8e500f92f58bf21d1

Secure Sockets Layer
TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 368

Frame 28: 427 bytes on wire (3416 bits), 427 bytes captured (3416 bits)
Ethernet II, Src: Dell_4f:01:25 (18:db:02:4f:01:25), Dst: Rockwell_1a
Transmission Control Protocol, Src Port: 62274, Dst Port: 443, Seq: 2

Rockwell Automation
Certificate Authorities and Encryption

- Ok so devices have encryption, but how do they know how to decrypt a message that another device encrypted?
- How do certificates work and what is a Certificate Authority (CA)?
  - A CA provides verified certificates to devices, basically a stamp of approval
Certificate Authorities

1. Server requests certificate from CA by providing critical identifying information.
2. CA provides “signed” certificate of server identity.
3. Client requests secure connection.
4. Server provides certificate.
5. Client verifies certificate with “trusted” CA.
Why was the Stratix® Device Manager certificate invalid or not trusted?
Comparing the Certificates (Self-signed)

Signed or Trusted

Self-signed or Untrusted
Comparing the Certificates ( Trusted )
Comparing the Certificates (Trusted)

Certificate Viewer: "custhelp.com"

General Details

This certificate has been verified for the following uses:
SSL Client Certificate
SSL Server Certificate

Issued To
Common Name (CN) custhelp.com
Organization (O) Oracle Corporation
Organizational Unit (OU) Oracle OSE, RAINBOW

Issued By
Common Name (CN) Symantec Class 3 Secure Server CA - G4
Organization (O) Symantec Corporation
Organizational Unit (OU) Symantec Trust Network

Period of Validity
Begins On Thursday, September 15, 2016
Expires On Saturday, December 16, 2017

Fingerprints
SHA-256 Fingerprint
SHA-1 Fingerprint

Certificate Viewer: "custhelp.com"

General Details

This certificate has been verified for the following uses:
SSL Client Certificate
SSL Server Certificate

Issued To
Common Name (CN) custhelp.com
Organization (O) Oracle Corporation
Organizational Unit (OU) Oracle OSE, ASHURN

Issued By
Common Name (CN) Symantec Class 3 Secure Server CA - G4
Organization (O) Symantec Corporation
Organizational Unit (OU) Symantec Trust Network

Period of Validity
Begins On Monday, September 25, 2017
Expires On Wednesday, December 26, 2018

Fingerprints
SHA-256 Fingerprint
SHA-1 Fingerprint

Expired
Valid
### Everyday Authorities

- **Common Certificate Authorities**
  - Installed in FireFox by default

<table>
<thead>
<tr>
<th>Certificate Name</th>
<th>Security Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hongkong Post</td>
<td></td>
</tr>
<tr>
<td>IdenTrust</td>
<td></td>
</tr>
<tr>
<td>Internet Security Research Group</td>
<td></td>
</tr>
<tr>
<td>IGS Self-Signed Certificate:89659360</td>
<td></td>
</tr>
<tr>
<td>IZENPE S.A.</td>
<td></td>
</tr>
<tr>
<td>Japan Certification Services, Inc.</td>
<td></td>
</tr>
<tr>
<td>Krugova Eba Rascalensiowa S.A.</td>
<td></td>
</tr>
<tr>
<td>LusTrust S.A.</td>
<td></td>
</tr>
<tr>
<td>Microsoft Ltd.</td>
<td></td>
</tr>
<tr>
<td>Netlock XFL</td>
<td></td>
</tr>
<tr>
<td>Network Solutions L.L.C.</td>
<td></td>
</tr>
<tr>
<td>OpenTrust</td>
<td></td>
</tr>
<tr>
<td>Quotellio Limited</td>
<td></td>
</tr>
<tr>
<td>SECOM Trust Systems CO., LTD.</td>
<td></td>
</tr>
<tr>
<td>SECOM Trust.net</td>
<td></td>
</tr>
<tr>
<td>SecureTrust Corporation</td>
<td></td>
</tr>
<tr>
<td>Sistema Nacional de Certificacion Electronica</td>
<td></td>
</tr>
<tr>
<td>Sociedad Cameral de Certificacion Digital - Certicamera S.A.</td>
<td></td>
</tr>
<tr>
<td>Sonera</td>
<td></td>
</tr>
<tr>
<td>Staat der Niederlanden</td>
<td></td>
</tr>
<tr>
<td>Steinfel Technologies, Inc.</td>
<td></td>
</tr>
<tr>
<td>StartCom Ltd.</td>
<td></td>
</tr>
<tr>
<td>Swisscom</td>
<td></td>
</tr>
<tr>
<td>SwissSign AG</td>
<td></td>
</tr>
<tr>
<td>Symantec Corporation</td>
<td></td>
</tr>
</tbody>
</table>
Stratix® Firmware

- How do I get all of these great benefits?

Available Downloads

Product Selected: Stratix 5400
Product Version: 15.2(S)EA.fc4

Release Notes

- Custom Release Note

AOP - Add On Profiles

- AOP for 1783 Stratix 5400/5410/5700/8000/8300 Switches v13.02.03
- AOP for Stratix 5400, 5410, 8000, 8300, Armor and Stratix 5700 v13.03.06
- AOP for Stratix 5400/5410/5700/8000/8300/2500 Switches v14.01.05

Firmware

- Firmware for Stratix 5400 [1783-HMSxxx] v15.2(S)EA.fc4
- Firmware for Stratix 5400 CRYPTO [1783-HMSxxx] v15.2(S)EA.fc4
Stratix® Firmware – Crypto (K9)

- How do I get all of these great benefits?
Questions

Lab 1 – Certificates and Encryption
Lab Layout
Pre-lab

- Our story is that we are commissioning a new OEM machine that has the 1769-L24 controller and will need to communicate to the 1756-L73 through our existing security infrastructure.

- Our HMI display monitors a connection between the 1769-L24 and 1756-L73.

- We need to make sure the HMI reports good communication.
  - This will indicate that the two controllers are communicating.
Pre-Lab 2: What we’re doing

- “Troubleshoot” connection problem with 1769-L24
  - Using the Stratix® faceplate
  - Using Syslog in Stratix® device manager
- Configure Port Security via Stratix® device manager
Unauthorized Access

- When the 1769-L24 was connected, we saw an error on our HMI
Unauthorized Access

- When the 1769-L24 was connected, we saw an error on our HMI

!!!!Unauthorized device detected!!!!
Unauthorized Access

- When the 1769-L24 was connected, we saw an error on our HMI
- We used MAC address based port security to generate this error via controller tags
  - A MAC address is a unique address that every device has that typically cannot be changed

!!!!Unauthorized device detected!!!!
The Stratix® faceplate can give us insight as to what alarms are currently being triggered.

- We saw the two errors of Unauthorized Device and a Port Security Violation Alarm.

- These are generated from an Add-On Instruction running in the 1756-L73.
Device Manager Diagnostics

- The Syslog gives us more information into the alarm. We see specifics like which MAC address is causing the alarm and on which port the alarm is occurring.

%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address ABCD.ABCD.ABCD on port GigabitEthernet1/4

<table>
<thead>
<tr>
<th>Time Stamp</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 9 01:08:13</td>
<td>critical</td>
<td>%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 654.3354.1db7 on port GigabitEthernet1/4.</td>
</tr>
<tr>
<td>Apr 9 01:08:19</td>
<td>critical</td>
<td>%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 654.3354.1db7 on port GigabitEthernet1/4.</td>
</tr>
<tr>
<td>Apr 9 01:08:25</td>
<td>critical</td>
<td>%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 654.3354.1db7 on port GigabitEthernet1/4.</td>
</tr>
<tr>
<td>Apr 9 01:08:30</td>
<td>critical</td>
<td>%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 654.3354.1db7 on port GigabitEthernet1/4.</td>
</tr>
<tr>
<td>Apr 9 01:08:37</td>
<td>critical</td>
<td>%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 654.3354.1db7 on port GigabitEthernet1/4.</td>
</tr>
<tr>
<td>Apr 9 01:08:42</td>
<td>critical</td>
<td>%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 654.3354.1db7 on port GigabitEthernet1/4.</td>
</tr>
<tr>
<td>Apr 9 01:08:47</td>
<td>critical</td>
<td>%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 654.3354.1db7 on port GigabitEthernet1/4.</td>
</tr>
<tr>
<td>Apr 9 01:08:53</td>
<td>critical</td>
<td>%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 654.3354.1db7 on port GigabitEthernet1/4.</td>
</tr>
<tr>
<td>Apr 9 01:08:58</td>
<td>critical</td>
<td>%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 654.3354.1db7 on port GigabitEthernet1/4.</td>
</tr>
<tr>
<td>Apr 9 01:09:03</td>
<td>critical</td>
<td>%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 654.3354.1db7 on port GigabitEthernet1/4.</td>
</tr>
</tbody>
</table>
Port Security

- The Stratix® managed switches have security features that track the MAC address of a device connected to a port and only allows some MAC addresses
Port Security

- The Stratix® managed switches have security features that track the MAC address of a device connected to a port and only allows some MAC addresses.

- Another option for port security is to manually enter MAC addresses into a table. The Stratix® switch will only allow those specific MAC addresses to communicate through the port.
Port Security

- The Stratix® managed switches have security features that track the MAC address of a device connected to a port and only allows some MAC addresses.

- Another option for port security is to manually enter MAC addresses into a table. The Stratix® switch will only allow those specific MAC addresses to communicate through the port.
- If no MAC addresses are manually added, then the switch dynamically learns the addresses per port, we simply specify how many addresses we expect to be connected.

<table>
<thead>
<tr>
<th>Port Name</th>
<th>G1/4</th>
<th>Enable</th>
<th>Maximum MAC Count</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port Name</th>
<th>G1/4</th>
<th>Enable</th>
<th>Maximum MAC Count</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>
Port Security

- Besides changing the Maximum MAC Count, how else could we have fixed this?
  - Smartport roles
Did everyone notice that we still are having communication issues?
Questions

Lab – Port Security
Communication is still not working between the Produced/Consumed controllers, what else could be blocking this?

- **Stratix® 5950 security appliance**
  We have a firewall in place and we likely did not create a rule to allow our CIP™ traffic
Firewalls

What do firewalls do?

At their essence, firewalls contain lists of rules that permit or deny traffic based on certain criteria.

The major criteria are:

- Source IP address
- Source port number
- Destination IP address
- Destination port number
- Protocol

Rules are similar to a list of questions.
Firewalls

What do Firewalls do?

At their essence Firewalls contain lists of rules that permit or deny traffic based on certain criteria.

The major criteria are:

- Source IP address
- Source port number
- Destination IP address
- Destination port number
- Protocol

Where did you come from?

Source IP address
Source port number
What do Firewalls do?
- At their essence Firewalls contain lists of rules that permit or deny traffic based on certain criteria.
  - The major criteria are:
    - Source IP address
    - Source port number
    - Destination IP address
    - Destination port number
    - Protocol
Firewalls

- What do Firewalls do?
  - At their essence Firewalls contain lists of rules that permit or deny traffic based on certain criteria
    - The major criteria are:
      - Source IP address
      - Source port number
      - Destination IP address
      - Destination port number
      - Protocol

Where did you come from?

Where are you going?

How are you getting there?
What do Firewalls do?

Firewalls create security “Boundaries”

- This is similar to how airport security works. Pre-TSA is an unsecured area, after TSA, it is a secured area
- In the secured areas, we can assume that we are safe because TSA has helped to prevent any threats from entering the area
  - TSA is the Firewall

Arrivals, ticketing, insecure

Terminal gates, boarding, secure
Firewalls
Pre-Lab

- If you recall, we are commissioning a new machine, which is adding CIP traffic flows that did not exist on our network before.
- Let's review what our new network traffic is going to look like.
TCP Connection Established

Source: 192.168.1.56 (1756-L73)
Destination: 192.168.1.69 (1769-L24)
Port: 44818
What is a TCP connection exactly?

When you add a device in the Studio 5000® I/O tree, a TCP connection is created to that device. This connection must be established before the passing of I/O data. The connection monitors the status of the I/O module and in the event the connection is lost, the I/O data will stop.
UDP Data

New machine controller

UDP Data Stream
Source/Destination: 192.168.1.56 and 192.168.1.69
Port: 2222
Pre-Lab: What we’re doing

- Connect to Stratix® 5950 Security Appliance
  - Review the log of blocked traffic
  - Add 1769-L24 to our firewall rules
- Test other methods of communication to devices
15:00
Post-Lab

- At the beginning of the lab why is it that RSLinx® Classic could see all devices but the HMI still reported a problem?
The Firewall log shows us all traffic that is being blocked, in our case traffic from the 1756-L73 to the 1769-L24 was being blocked

Deny TCP src inside1:192.168.1.56/51314 dst outside1:192.168.1.69/44818
What do Firewalls do?

- At their essence Firewalls contain lists of rules that permit or deny traffic based on certain criteria.
  - The major criteria are:
    - Source IP address
    - Source port number
    - Destination IP address
    - Destination port number
    - Protocol

Where did you come from?

Where are you going?

How are you getting there?
The Firewall log shows us all traffic that is being blocked, in our case traffic from the 1756-L73 to the 1769-L24 was being blocked.

- Deny TCP src inside1:192.168.1.56/51314 dst outside1:192.168.1.69/44818
The Firewall log shows us all traffic that is being blocked, in our case traffic from the 1756-L73 to the 1769-L24 was being blocked

- Deny TCP src inside1:192.168.1.56/51314 dst outside1:192.168.1.69/44818

Where you came from
The Firewall log shows us all traffic that is being blocked, in our case traffic from the 1756-L73 to the 1769-L24 was being blocked.

Deny TCP src inside1:192.168.1.56/51314 dst outside1:192.168.1.69/44818
The Firewall log shows us all traffic that is being blocked, in our case traffic from the 1756-L73 to the 1769-L24 was being blocked.

Deny TCP, src inside1:192.168.1.56/51314 dst outside1:192.168.1.69/44818

How you get there  Where you came from  Where you’re going
The Firewall log shows us all traffic that is being blocked, in our case traffic from the 1756-L73 to the 1769-L24 was being blocked.

Deny TCP src inside1:192.168.1.56/51314 dst outside1:192.168.1.69/44818
## Firewall Access Rules

<table>
<thead>
<tr>
<th>#</th>
<th>Enabled</th>
<th>Source Criteria:</th>
<th>Destination Criteria:</th>
<th>Service</th>
<th>Action</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Source</td>
<td>User</td>
<td>Security Group</td>
<td>Destination</td>
<td>Security Group</td>
</tr>
<tr>
<td>1</td>
<td>☑</td>
<td>inside1</td>
<td>1756-L73</td>
<td></td>
<td>any</td>
<td>tcp-explicit</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>inside1</td>
<td>1756-L73</td>
<td></td>
<td>1769-L24</td>
<td>tcp-explicit-tcp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>inside2</td>
<td>any</td>
<td>Any less secure net</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>outside1</td>
<td>any</td>
<td></td>
<td>any</td>
<td>tcp-explicit</td>
</tr>
<tr>
<td>1</td>
<td>☑</td>
<td>outside1</td>
<td>Engineering_PC</td>
<td>1756-L73</td>
<td></td>
<td>Permit</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>outside1</td>
<td>Engineering_PC</td>
<td>1756-L73</td>
<td>Stratix5700</td>
<td>Permit</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>outside1</td>
<td>Stratix5700</td>
<td>https</td>
<td></td>
<td>Permit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Global</td>
<td>any</td>
<td></td>
<td>any</td>
<td>tcp-explicit-tcp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>any</td>
<td></td>
<td>any</td>
<td>https</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>any</td>
<td></td>
<td>any</td>
<td>ip</td>
</tr>
</tbody>
</table>
Firewall Access Rules

### Where you came from

<table>
<thead>
<tr>
<th>#</th>
<th>Enabled</th>
<th>Source Criteria:</th>
<th>Destination Criteria:</th>
<th>Service</th>
<th>Action</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Source</td>
<td>Destination</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User</td>
<td>Security Group</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Group</td>
<td>Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Action</td>
<td>Hits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
<td>------------------</td>
<td>------------------------</td>
<td>---------</td>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>1</td>
<td>on</td>
<td>1756-L73</td>
<td>any</td>
<td>UDP</td>
<td>Permit</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>on</td>
<td>1756-L73</td>
<td>1759-L24 Stratix5400</td>
<td>TCP</td>
<td>Permit</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td>Any less secure net...</td>
<td>TCP</td>
<td>Permit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td>Engineering_PC</td>
<td>UDP</td>
<td>Permit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td>Stratix5700</td>
<td>TCP</td>
<td>Permit</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td>Stratix5700</td>
<td>TCP</td>
<td>Permit</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td>any</td>
<td>UDP</td>
<td>Permit</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td>any</td>
<td>TCP</td>
<td>Permit</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td>any</td>
<td>TCP</td>
<td>Permit</td>
<td>1</td>
</tr>
</tbody>
</table>

- **Source Criteria:**
  - inside1 (2 incoming rules)
  - inside2 (1 implicit incoming rule)
  - management (0 implicit incoming rules)
  - outside1 (3 incoming rules)
  - outside2 (0 implicit incoming rules)
  - Global (1 implicit rule)

- **Destination Criteria:**
  - any
  - 1756-L73
  - 1759-L24
  - Stratix5400
  - Stratix5700
  - any
  - any
  - any
  - any
  - any
  - any
  - any
  - any

- **Service:**
  - UDP
  - TCP

- **Action:**
  - Permit
  - Deny
## Firewall Access Rules

<table>
<thead>
<tr>
<th>#</th>
<th>Enabled</th>
<th>Source Criteria:</th>
<th>Destination Criteria:</th>
<th>Service</th>
<th>Action</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Source:</td>
<td>Security Group:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1756-L73</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1756-L73</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td>1756-L24</td>
<td>ip-implicit</td>
<td>Permit</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1756-L73</td>
<td>Stratix5400</td>
<td>ip-explicit-tcp</td>
<td>Permit</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management</td>
<td>Any less secure net...</td>
<td>tcp</td>
<td>Permit</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1756-L73</td>
<td>Stratix5700</td>
<td>ip-explicit-tcp</td>
<td>Permit</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Outside</td>
<td>Stratix5700</td>
<td>tcp</td>
<td>Permit</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Global</td>
<td>any</td>
<td>tcp</td>
<td>Deny</td>
<td>1</td>
</tr>
</tbody>
</table>
# Firewall Access Rules

## Where you came from

<table>
<thead>
<tr>
<th>#</th>
<th>Enabled</th>
<th>Source Criteria:</th>
<th>Destination Criteria:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Source</td>
<td>User</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>any</td>
<td>any</td>
</tr>
</tbody>
</table>

## Where you’re going

<table>
<thead>
<tr>
<th>#</th>
<th>Enabled</th>
<th>Source Criteria:</th>
<th>Destination Criteria:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Source</td>
<td>User</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>any</td>
<td>any</td>
</tr>
</tbody>
</table>

## How you get there

<table>
<thead>
<tr>
<th>#</th>
<th>Enabled</th>
<th>Source Criteria:</th>
<th>Destination Criteria:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Source</td>
<td>User</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>any</td>
<td>any</td>
</tr>
</tbody>
</table>
# Firewall Access Rules

<table>
<thead>
<tr>
<th>#</th>
<th>Enabled</th>
<th>Source Criteria:</th>
<th>Destination Criteria:</th>
<th>Service</th>
<th>Action</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Source</td>
<td>User</td>
<td>Security Group</td>
<td>Destination</td>
<td>Security Group</td>
</tr>
<tr>
<td>1</td>
<td>✓</td>
<td>1756-L73</td>
<td></td>
<td></td>
<td>any</td>
<td>1759-L24</td>
</tr>
<tr>
<td>2</td>
<td>✓</td>
<td>1756-L73</td>
<td></td>
<td></td>
<td>10</td>
<td>Stratx5400</td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td></td>
<td></td>
<td>10</td>
<td>Any less secure network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td></td>
<td></td>
<td>10</td>
<td>Engineering_PC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td></td>
<td></td>
<td>10</td>
<td>1756-L73</td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td></td>
<td></td>
<td>10</td>
<td>Stratx5700</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>any</td>
<td></td>
<td></td>
<td>10</td>
<td>Stratx5700</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>any</td>
<td></td>
<td></td>
<td>10</td>
<td>Stratx3700</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>any</td>
<td></td>
<td></td>
<td>10</td>
<td>Global</td>
</tr>
</tbody>
</table>

- **Where you came from**: Source
- **Where you’re going**: Destination
- **How you get there**: Security Group
- **Action**: tcp-implicit, tcp-explicit-tcp, https, permit, deny

---

**Note**: The table details firewall access rules with specific configuration for incoming and outgoing traffic, including source and destination criteria, security groups, and allowed services and actions.
Why did we have a rule in place for the Stratix® 5400 managed switch and why did we add the 1769-L24 to it?
The Network is Still Broken

- Why did the ping fail? RSLinx® Classic can see the device!

```
C:\Users\Labuser>ping 192.168.1.56
Pinging 192.168.1.56 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.56:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```


### Why did the ping fail? Let's review the rules

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>1756-173</td>
<td></td>
<td></td>
<td>any</td>
<td></td>
<td>TCP</td>
<td>Permit</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>1756-173</td>
<td></td>
<td></td>
<td>1769-124</td>
<td>Stratix5400</td>
<td>TCP</td>
<td>Permit</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dp-implicit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dp-explicit-tcp</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>any</td>
<td></td>
<td>Any less secure network</td>
<td>ip</td>
<td>Permit</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>any</td>
<td></td>
<td>Any less secure network</td>
<td></td>
<td>Permit</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Engineering_PC</td>
<td></td>
<td></td>
<td>1756-173</td>
<td>Stratix5700</td>
<td>TCP</td>
<td>Permit</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>Global</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TCP</td>
<td>Deny</td>
<td></td>
</tr>
</tbody>
</table>

### The Network is Still Broken
Why did the ping fail? Let's review the rules

- All rules I see on inside1 and outside1 are Permit, how do items get denied?

<table>
<thead>
<tr>
<th>#</th>
<th>Enabled</th>
<th>Source Criteria:</th>
<th>Destination Criteria:</th>
<th>Service</th>
<th>Action</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Source</td>
<td>User</td>
<td>Security Group</td>
<td>Destination</td>
<td>Security Group</td>
</tr>
<tr>
<td>1</td>
<td>yes</td>
<td>1756-173</td>
<td></td>
<td></td>
<td>any</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>yes</td>
<td>1756-173</td>
<td></td>
<td></td>
<td>1769-1.24</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td></td>
<td></td>
<td>any</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td></td>
<td></td>
<td>Any less secure net...</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>yes</td>
<td>any</td>
<td></td>
<td></td>
<td>any</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>yes</td>
<td>Engineering_PC</td>
<td></td>
<td></td>
<td>1756-173</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>yes</td>
<td>Engineering_PC</td>
<td></td>
<td></td>
<td>Stratis5700</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td></td>
<td></td>
<td>Stratis5700</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>any</td>
<td></td>
<td></td>
<td>any</td>
<td></td>
</tr>
</tbody>
</table>
All rules I see on inside1 and outside1 are Permit, how do items get denied?

- **Global Implicit rule**

<table>
<thead>
<tr>
<th>#</th>
<th>Enabled</th>
<th>Source Criteria:</th>
<th>Destination Criteria:</th>
<th>Service</th>
<th>Action</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Source</td>
<td>User</td>
<td>Security Group</td>
<td>Destination</td>
<td>Security Group</td>
</tr>
<tr>
<td>1</td>
<td>✓</td>
<td>any</td>
<td></td>
<td></td>
<td>any</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>✓</td>
<td>1756-1773</td>
<td></td>
<td></td>
<td>1769-124</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>1756-1773</td>
<td></td>
<td>Stratix5400</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>any</td>
<td></td>
<td></td>
<td>Any less secure net...</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>any</td>
<td></td>
<td></td>
<td>any</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Engineering_PC</td>
<td></td>
<td></td>
<td>1756-1773</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Engineering_PC</td>
<td></td>
<td>Stratix5700</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Rule Processing

- Rules are processed sequentially, in order, first in first out
  - All criteria must match

| # | Enabled | Source Criteria: | | | Destination Criteria: | | | Service | Action | Hits |
|---|---|---|---|---|---|---|---|---|---|
|   | | Source | User | Security Group | Destination | Security Group | | | |
| 1 | | any | Engineering_PC | | any | | | | |
| 2 | | 1756-L73 | | | 1756-L73 | | | | |
| 3 | | 1756-L73 | | | Stratix5400 | | | | |
| 4 | | Stratix5400 | | | any | | | | |

Incoming traffic:
- 1
- 2
- 3
Questions

Lab – Stratix® 5950 Security Appliance Access Control Lists
Pre-lab 4

- The focus of this lab will be on a feature of the Stratix® 5950 security appliance known as Deep Packet Inspection (DPI)
What is DPI?

- As we learned before, firewalls can only take action based on certain criteria.
- What if all criteria matched, but there is malicious content in the traffic?
What is DPI?

- As we learned before, firewalls can only take action based on certain criteria.
- What if all criteria matched, but there is malicious content in the traffic?

Where did you come from?

Where are you going?

How are you getting there?

Source IP address
Source port number

Destination IP address
Destination port number

Protocol
What is DPI?

- As we learned before, firewalls can only take action based on certain criteria.
- What if all criteria matched, but there is malicious content in the traffic?

<table>
<thead>
<tr>
<th>Version</th>
<th>IHL</th>
<th>Type of service</th>
<th>Total length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>D</td>
<td>M</td>
<td>F</td>
</tr>
<tr>
<td>Time to live</td>
<td>Protocol</td>
<td>Fragment offset</td>
<td></td>
</tr>
<tr>
<td>Header checksum</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

32 Bits

How you get there
Where you came from
Where you’re going
What is DPI?

- We need to gain insight into what is actually in the data
- DPI provides us with that ability and can take action

![Diagram of IP header]

- How you get there
- Where you came from
- Where you’re going
Pre-lab 4: What We’re Doing

- The focus of this lab will be on a feature of the Stratix® 5950 security appliance known as Deep Packet Inspection (DPI)
- We will review the available logging for the DPI
- We will be reviewing the configuration options for DPI
  - We will be exploring the CIP™ DPI options
  - We will see the result of the CIP™ DPI action from the end-user perspective
Why did Downloading the ACD file take us offline?

![Logix Designer error message](image-url)

*Logix Designer*

Can't communicate with RSLinx.
Logix Designer has been taken offline.

If online operations are in progress, they will not be completed.

Offline operations after communication loss will result in loss of correlation. To avoid loss of correlation, close views without applying changes before attempting to go online.
# DPI Log Event

- Lets dissect the information from the log besides the Policy

<table>
<thead>
<tr>
<th><strong>Event Details</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initiator</strong></td>
</tr>
<tr>
<td>Initiator IP</td>
</tr>
<tr>
<td>Initiator Country and Continent</td>
</tr>
<tr>
<td>Source Port/ICMP Type</td>
</tr>
<tr>
<td>User</td>
</tr>
<tr>
<td><strong>Transaciton</strong></td>
</tr>
<tr>
<td>Initiator Packets</td>
</tr>
<tr>
<td>Responder Packets</td>
</tr>
<tr>
<td>Total Packets</td>
</tr>
<tr>
<td>Initiator Bytes</td>
</tr>
<tr>
<td>Responder Bytes</td>
</tr>
<tr>
<td>Connection Bytes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Policy</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
</tr>
<tr>
<td>Firewall Policy Rule/Category</td>
</tr>
<tr>
<td>Monitor Rules</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Responder</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Responder IP</td>
</tr>
<tr>
<td>Responder Country and Continent</td>
</tr>
<tr>
<td>Destination Port/ICMP Code</td>
</tr>
<tr>
<td>URL</td>
</tr>
<tr>
<td>URL Category</td>
</tr>
<tr>
<td>URL Reputation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Traffic</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Security Zone</td>
</tr>
<tr>
<td>Egress Security Zone</td>
</tr>
<tr>
<td>Ingress Interface</td>
</tr>
<tr>
<td>Egress Interface</td>
</tr>
<tr>
<td>TCP Flags</td>
</tr>
<tr>
<td>NetBIOS Domain</td>
</tr>
</tbody>
</table>

- Application: CIP
- Application Categories: network protocols/services
- Application Tag: Common Industrial Protocol
- Client Application: CIP client
- Client Version: not available
- Client Categories: not available
- Client Tag: not available
- Web Application: CIP RA Admin Other
- Web Application Categories: network protocols/services, CIP RA Admin
- Web Application Tag: Common Industrial Protocol
- Application Risk: Very Low
- Application Business Relevance: Very High
### DPI Log Event

- **Let's dissect the information from the log besides the Policy**

#### Event Details

<table>
<thead>
<tr>
<th>initiator</th>
<th>responder</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>initiator IP</strong></td>
<td>192.168.1.149</td>
</tr>
<tr>
<td><strong>initiator country and continent</strong></td>
<td>not available</td>
</tr>
<tr>
<td><strong>source port/ICMP type</strong></td>
<td>54031</td>
</tr>
<tr>
<td><strong>user</strong></td>
<td>not available</td>
</tr>
<tr>
<td><strong>initiator packets</strong></td>
<td>2002.0</td>
</tr>
<tr>
<td><strong>initiator bytes</strong></td>
<td>300908.0</td>
</tr>
<tr>
<td><strong>initiator connection bytes</strong></td>
<td>670313.0</td>
</tr>
<tr>
<td><strong>responder packets</strong></td>
<td>2754.0</td>
</tr>
<tr>
<td><strong>responder bytes</strong></td>
<td>369405.0</td>
</tr>
<tr>
<td><strong>total packets</strong></td>
<td>4756.0</td>
</tr>
<tr>
<td><strong>total bytes</strong></td>
<td>not available</td>
</tr>
<tr>
<td><strong>total connection bytes</strong></td>
<td>not available</td>
</tr>
</tbody>
</table>

#### Traffic

- **ingress security zone**: not available
- **egress security zone**: not available
- **ingress interface**: outside1
- **egress interface**: inside1
- TCP flags: 0
- NetBIOS domain: not available

#### Application

- **application**: CIP
- **application categories**: network protocols/services
- **application tag**: Common Industrial Protocol
- **client application**: CIP client
- **client version**: not available
- **client categories**: not available
- **client tag**: not available
- **web application**: CIP RA Admin Other
- **web app categories**: network protocols/services, CIP RA Admin
- **web application tag**: Common Industrial Protocol
- **application risk**: Very Low
- **application business relevance**: Very High

**Policy**

- **policy**: Block PAC Changes
- **firewall policy rule/SI category**: Policy 1.a to 1756-173
- **monitor rules**: not available

**Where you came from**
## DPI Log Event

- Lets dissect the information from the log besides the Policy

### Event Details

<table>
<thead>
<tr>
<th>Initiator</th>
<th>Responder</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initiator IP</strong></td>
<td>192.168.1.149</td>
</tr>
<tr>
<td><strong>Response IP</strong></td>
<td>192.168.1.56</td>
</tr>
<tr>
<td><strong>Initiator Country and Continent</strong></td>
<td>not available</td>
</tr>
<tr>
<td><strong>Responder Country and Continent</strong></td>
<td>not available</td>
</tr>
<tr>
<td><strong>Source Port/ICMP Type</strong></td>
<td>50431</td>
</tr>
<tr>
<td><strong>Destination Port/ICMP Code</strong></td>
<td>44818</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>not available</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>not available</td>
</tr>
<tr>
<td><strong>URL Category</strong></td>
<td>not available</td>
</tr>
<tr>
<td><strong>URL Reputation</strong></td>
<td>Risk unknown</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transaction</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initiator Packets</strong></td>
<td>2002.0</td>
</tr>
<tr>
<td><strong>Responder Packets</strong></td>
<td>2754.0</td>
</tr>
<tr>
<td><strong>Total Packets</strong></td>
<td>4756.0</td>
</tr>
<tr>
<td><strong>Initiator Bytes</strong></td>
<td>309008.0</td>
</tr>
<tr>
<td><strong>Responder Bytes</strong></td>
<td>369405.0</td>
</tr>
<tr>
<td><strong>Connection Bytes</strong></td>
<td>670313.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application</strong></td>
<td>CIP</td>
</tr>
<tr>
<td><strong>Application Categories</strong></td>
<td>network protocols/services</td>
</tr>
<tr>
<td><strong>Application Tag</strong></td>
<td>Common Industrial Protocol</td>
</tr>
<tr>
<td><strong>Client Application</strong></td>
<td>CIP client</td>
</tr>
<tr>
<td><strong>Client Version</strong></td>
<td>not available</td>
</tr>
<tr>
<td><strong>Client Categories</strong></td>
<td>not available</td>
</tr>
<tr>
<td><strong>Client Tag</strong></td>
<td>not available</td>
</tr>
<tr>
<td><strong>Web Application</strong></td>
<td>CIP RA Admin Other</td>
</tr>
<tr>
<td><strong>Web App Categories</strong></td>
<td>network protocols/services, CIP RA Admin</td>
</tr>
<tr>
<td><strong>Web Application Tag</strong></td>
<td>Common Industrial Protocol</td>
</tr>
<tr>
<td><strong>Application Risk</strong></td>
<td>Very Low</td>
</tr>
<tr>
<td><strong>Application Business Relevance</strong></td>
<td>Very High</td>
</tr>
</tbody>
</table>
## DPI Log Event

- Lets dissect the information from the log besides the Policy

### Event Details

<table>
<thead>
<tr>
<th>Initiator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiator IP</td>
</tr>
<tr>
<td>Initiator Country and Continent</td>
</tr>
<tr>
<td>Source Port/ICMP Type</td>
</tr>
<tr>
<td>User</td>
</tr>
<tr>
<td>Initiator Packets</td>
</tr>
<tr>
<td>Initiator Bytes</td>
</tr>
<tr>
<td>Initiator Bytes</td>
</tr>
<tr>
<td>Initiator Bytes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Responder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responder IP</td>
</tr>
<tr>
<td>Responder Country and Continent</td>
</tr>
<tr>
<td>Source Port/ICMP Type</td>
</tr>
<tr>
<td>User</td>
</tr>
<tr>
<td>URL</td>
</tr>
<tr>
<td>URL Category</td>
</tr>
<tr>
<td>URL Reputation</td>
</tr>
<tr>
<td>Traffic</td>
</tr>
<tr>
<td>Ingress Security Zone</td>
</tr>
<tr>
<td>Egress Security Zone</td>
</tr>
<tr>
<td>Ingress Interface</td>
</tr>
<tr>
<td>Egress Interface</td>
</tr>
<tr>
<td>TCP Flags</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiator Packets</td>
</tr>
<tr>
<td>Responder Packets</td>
</tr>
<tr>
<td>Total Packets</td>
</tr>
<tr>
<td>Initiator Bytes</td>
</tr>
<tr>
<td>Responder Bytes</td>
</tr>
<tr>
<td>Connection Bytes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
</tr>
<tr>
<td>Application Categories</td>
</tr>
<tr>
<td>Application Tag</td>
</tr>
<tr>
<td>Client Application</td>
</tr>
<tr>
<td>Client Version</td>
</tr>
<tr>
<td>Client Categories</td>
</tr>
<tr>
<td>Client Tag</td>
</tr>
<tr>
<td>Web Application</td>
</tr>
<tr>
<td>Web App Categories</td>
</tr>
<tr>
<td>Web Application Tag</td>
</tr>
<tr>
<td>Application Risk</td>
</tr>
<tr>
<td>Application Business Relevance</td>
</tr>
</tbody>
</table>

### Analysis

- **Where you came from**: Initiator IP: 192.168.1.149, Source Port: 54031.
- **What you’re bringing**: Initiator Packets: 2002.0, Initiator Bytes: 300908.0.

---

Note: The red box highlights the policy details: Policy = Block PAC Changes, Firewall Policy Rule/Category = Policy 1.a to 1756-173.
DPI Rule Creation

- Like on the firewall, we can add IP address or network objects
Like on the firewall, we can add IP address or network objects.
Why is our action Block with reset?
What actions will the CIP™ RA Admin category block?
CIP™ Rockwell Automation Admin

Graphical Summary
CIP™ Rockwell Automation Admin

Graphical Summary

Studio 5000® Download
Graphical Summary
CIP™ Rockwell Automation Admin

Graphical Summary

Studio 5000® Download

Studio 5000® Upload
CIP™ Rockwell Automation Admin

Graphical Summary
CIP™ Rockwell Automation Admin

Graphical Summary

- Studio 5000® Download
- Studio 500® Upload
- Studio 5000® Online Edits
CIP™ Rockwell Automation Admin

Graphical Summary

- Studio 5000® Download
- Studio 5000® Upload
- Studio 5000® Online Edits
CIP™ Rockwell Automation Admin

Graphical Summary

Studio 5000® Download
Studio 5000® Upload
Studio 5000® Online Edits
RSLinx® Classic Configuration Changes
Graphical Summary

- Studio 5000® Download
- Studio 5000® Upload
- Studio 5000® Online Edits
- RSLinx® Classic Configuration Changes
Stratix® 5950 Security Appliance Benefits

- How else does the Stratix® 5950 security appliance help protect you?

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP_MALFORMED</td>
<td>CIP data is malformed. For example, if a packet data field specifies the size of data to follow, but that many bytes of data do not actually exist, it may flag this rule.</td>
</tr>
<tr>
<td>CIP_NON_CONFORMING</td>
<td>CIP data is non-conforming to ODVA standard. For example, if the standard specifies a limited range of values for a particular packet field, and packet data contains values outside of that range, it may flag this rule.</td>
</tr>
<tr>
<td>CIP_CONNECTION_LIMIT</td>
<td>CIP connection limit per TCP connection exceeded. Least recently used connection removed.</td>
</tr>
<tr>
<td>CIP_REQUEST_LIMIT</td>
<td>CIP concurrent unconnected request limit per TCP connection exceeded. Oldest request removed.</td>
</tr>
</tbody>
</table>
Questions

Lab - Deep Packet Inspection (DPI) using the Stratix® 5950 security appliance
What are Policies and Procedures in relation to Network Security?
What are Policies and Procedures in relation to Network Security?

- A set of objectives for the company to set rules of behavior for users and administrators and requirements for systems and networks that confirm security of the cyber environment
What are Policies and Procedures in relation to Network Security?

Three reasons for policies and procedures

- Inform users, staff and managers
- Specify mechanisms for security
- Provide a baseline
What are Policies and Procedures in relation to Network Security?

- Results of policies and procedures
  - Protects people, assets and information
  - Sets rules
  - Defines consequences
Our IACS network has a policy in place, for lab purposes this policy is called “Policy 1.a”

- This policy simply state, any administrative changes to the PLC must be made at the local switch and are not allowed to traverse the network
- We saw this policy enforced in the Stratix® 5950 log in the last lab
Pre-lab: What we’re doing

- We will be following this policy and connect locally to the Stratix® 5700 managed switch
- An HMI will help us in enabling a “maintenance connection” on the switch
- We will have full access to the 1756-L73 to download our program
Why do we need to enable a maintenance port? Can't we connect?

- It's a common security practice to shut down all unused ports
Why do we need to enable a maintenance port? Can’t we connect?

- It’s a common security practice to shut down all unused ports
  - However, with the proper credentials we can use our CIP™ integration to activate or deactivate the port easily from the HMI
Post-lab

- Additionally, ports typically have a port lock in place
  - Can only be removed using special tools
Post-lab

- You can even lock cables and help prevent them from being removed!
Post-lab

- Why did downloading to the controller work this time?
Post-lab

- Why did downloading to the controller work this time?
  - We were connected to the Stratix® 5700 managed switch within the Inside or Trusted zone
    - Traffic was no longer traveling through the Stratix® 5950 security appliance
Why couldn’t RSLinx® Classic see these two devices?
Why couldn’t RSLinx® Classic see these two devices?
Questions

Lab – Following “Policy 1.a”
Agenda

Introduction

Network Security

Labs

Wrap up

Survey
The Defense-in-depth security approach is recommended in:

- IEC 62443 standard series (formerly ISA99).
- NIST Special Publication 800-82.
Your action items

1. Update your networks
   - Gain an understanding of your network and applications
   - Establish policies and procedures and access control that reflect your network and needs

2. Understand the application
   - Who talks to what
   - What are they talking about
   - Establish baselines
   Helps understand what security is needed and where

3. Find help
   - IT has been overcoming these challenges for years
   - Use design guides
   - Consider our Network Security Services
   Act
   - Work towards a better security posture
Misc. Reading

Additional Material
CPwE Architectures - Cisco and Rockwell Automation®

- CPwE website
- Overview Documents
  - Alliance Profile
  - Top 10 Recommendations for Plant-wide EtherNet/IP Deployments
  - Design Considerations for Securing Industrial Automation and Control System Networks
### Additional Material

<table>
<thead>
<tr>
<th>Topic</th>
<th>Design Guide</th>
<th>Whitepaper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design Considerations for Securing IACS Networks</td>
<td>—</td>
<td>ENET-WP031A-EN-P</td>
</tr>
<tr>
<td>Converged Plantwide Ethernet – Baseline Document</td>
<td>ENET-TD001E-EN-P</td>
<td>—</td>
</tr>
<tr>
<td>Resilient Ethernet Protocol in a CPwE Architecture</td>
<td>ENET-TD005B-EN-P</td>
<td>ENET-WP033A-EN-P</td>
</tr>
<tr>
<td>Deploying 802.11 Wireless LAN Technology within a CPwE Architecture</td>
<td>ENET-TD006A-EN-P</td>
<td>ENET-WP034A-EN-P</td>
</tr>
<tr>
<td>Deploying Identity Services within a CPwE Architecture</td>
<td>ENET-TD008A-EN-P</td>
<td>ENET-WP037A-EN-P</td>
</tr>
<tr>
<td>Securely Traversing IACS Data Across the Industrial Demilitarized Zone (IDMZ)</td>
<td>ENET-TD009A-EN-P</td>
<td>ENET-WP038A-EN-P</td>
</tr>
<tr>
<td>Deploying Network Address Translation within a CPwE Architecture</td>
<td>ENET-TD007A-EN-P</td>
<td>ENET-WP036A-EN-P</td>
</tr>
<tr>
<td>Migrating Legacy IACS Networks to a CPwE Architecture</td>
<td>ENET-TD011A-EN-P</td>
<td>ENET-WP040A-EN-P</td>
</tr>
<tr>
<td>Deploying A Resilient Converged Plantwide Ethernet Architecture</td>
<td>ENET-TD010A-EN-P</td>
<td>ENET-WP039B-EN-P</td>
</tr>
<tr>
<td>Site-to-site VPN to a CPwE Architecture</td>
<td>ENET-TD012A-EN-P</td>
<td>—</td>
</tr>
<tr>
<td>Deploying Industrial Firewalls within a CPwE Architecture</td>
<td>ENET-TD002A-EN-P</td>
<td>ENET-WP011B-EN-P</td>
</tr>
</tbody>
</table>
Additional Material

- Ethernet Design Considerations Reference Manual
  - ENET-RM002C-EN-P
  - EtherNet/IP Overview, Ethernet Infrastructure Components, EtherNet/IP Protocol
- EtherNet/IP IntelliCENTER® Reference Manual (MCC-RM001)

- The OEM Guide to Networking
  - ENET-RM001A-EN-P
  - Intended to help OEMs understand relevant technologies, networking capabilities and other considerations that could impact them as they develop EtherNet/IP solutions for the machines, skids or equipment they build
- Segmentation Methods Within the Cell/Area Zone ENET-AT004B-EN-E
Additional Material

- **Integrated Architecture® Builder (IAB)**
  - Updates and additions to better-reflect CPwE structure, hierarchy and best practices
  - Improved Switch Wizard for distribution (for example, Stratix® 5410 switch) and access (for example, Stratix® 5700 switch)
  - Easier to create a large EtherNet/IP network with many topologies
  - CIP™ traffic is measured per segment, not just controller scanner and adapter centric

- **EtherNet/IP Capacity Tool**
- **Popular Configuration Drawings (PCDs)**
  - Updates and additions to better reflect CPwE recent enhancements
Training Resources
Training Resources
Education - Industrial IoT / Industrial IT (Bridging OT-IT)

- A ‘go-to’ resource for training and educational information on standard Internet Protocol (IP), security, wireless and other emerging technologies for industrial applications
- Led by Cisco, Panduit, and Rockwell Automation®
- Receive monthly e-newsletters with articles and videos on the latest trends
- Scenario-based training on topics such as: logical topologies, protocols, switching, routing, wireless and physical cabling

Network Design eLearning course available at promotional price for TechEd Attendees! Earn PDHs by signing up today at www.industrial-ip.org with code “EVENTS2017”
Training Resources

Four eLearning courses cover key aspects of implementing networked, industrial control systems. 20-30 minutes interactive, scenario-based courses cover automation controls and physical infrastructure considerations.
Courses 1 and 2: Designing for the Cell/Area Zone
- Design secure, robust, future-ready networks for cells, machines, skids and other functional units by implementing reference architectures and standard IP.

Course 3: Designing for the Industrial Zone
- Learn design principles on line integration, high-availability networks and wireless architectures to optimize plant networks.

Course 4: IT/OT Integration
- Understand how to effectively converge a smart manufacturing facility with IT and OT stakeholders.
Training Resources

- Cisco Industrial Networking Specialist Training and Certification
  - Classroom training
    - Managing Industrial Networks with Cisco Networking Technologies (IMINS)
  - Exam: 200–401 IMINS
  - CPwE Design Considerations and Best Practices

CCNA Industrial Training and Certification
- Classroom training
  - Managing Industrial Networks for Manufacturing with Cisco Technologies (IMINS2)
  - Exam: 200–601 IMINS2
  - CPwE Design Considerations and Best Practices
## Training Resources

### Industrial Networking Specialist

<table>
<thead>
<tr>
<th>Module</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module 1</td>
<td>Industrial Networking Solutions and Products</td>
</tr>
<tr>
<td>Module 2</td>
<td>Industrial Network Documentation and Deployment Considerations</td>
</tr>
<tr>
<td>Module 3</td>
<td>Installing Industrial Network Switches, Routers, and Cabling</td>
</tr>
<tr>
<td>Module 4</td>
<td>Deploying Industrial Ethernet Devices</td>
</tr>
<tr>
<td>Module 5</td>
<td>Maintaining Industrial Ethernet Networks</td>
</tr>
<tr>
<td>Module 6</td>
<td>Troubleshooting Industrial Ethernet Networks</td>
</tr>
</tbody>
</table>

### CCNA Industrial

<table>
<thead>
<tr>
<th>Module</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module 1</td>
<td>Industrial Networking Concepts and Components</td>
</tr>
<tr>
<td>Module 2</td>
<td>General Troubleshooting Issues</td>
</tr>
<tr>
<td>Module 3</td>
<td>EtherNet/IP</td>
</tr>
<tr>
<td>Module 4</td>
<td>Troubleshooting EtherNet/IP</td>
</tr>
<tr>
<td>Module 5</td>
<td>PROFINET</td>
</tr>
<tr>
<td>Module 6</td>
<td>Configuring PROFINET</td>
</tr>
<tr>
<td>Module 7</td>
<td>Troubleshooting PROFINET</td>
</tr>
<tr>
<td>Module 8</td>
<td>Exploring Security Concerns</td>
</tr>
<tr>
<td>Module 9</td>
<td>802.11 Industrial Ethernet Wireless Networking</td>
</tr>
</tbody>
</table>
Training Resources
Rockwell Automation® - Webinars

- Industrial Automation Webinars
- On-Demand Webinars
  - Introduction to Building a Robust, Secure and Future-ready Network Infrastructure
  - Increase Business Agility by Converging Manufacturing and Business Systems
  - The Power of Building a Secure Network Infrastructure
  - Design Considerations for Building a Secure Network Infrastructure
Agenda

Introduction

Network Security

Labs

Wrap up

Survey
Thank You!