User Manual

Original Instructions

Allen-Bradley

Stratix 5950 Security Appliance

Catalog Numbers 1783-SAD4T0SBK9, 1783-SAD4T0SPK9, 1783-SAD2T2SBK9, 1783-SAD2T2SPK9

Allen-Bradley • Rockwell Software

Rockwell Automation

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

⚠	**WARNING:** Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.
⚠	**ATTENTION:** Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.

Labels may also be on or inside the equipment to provide specific precautions.

⚠	**SHOCK HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.
⚠	**BURN HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.
⚠	**ARC FLASH HAZARD:** Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

Chapter 1
About the Security Appliance

Chapter 2
Industrial Firewall Use Cases

Chapter 3

Configure the Security Appliance

Chapter 4

Monitor the Security Appliance

Chapter 5

Centralized Management

Chapter 6

Hardware Bypass

Chapter 7

CIP Inspection

Chapter 8

Firewall Modes

Chapter 9

Update the Device

Chapter 10

Troubleshoot

Notes:

The Stratix® 5950 Security Appliance User Manual provides a product overview and explains how to connect and configure the security appliance. This manual is intended for people who have a high level of technical ability. Experience with Cisco® software is not a prerequisite.

This manual describes the appliance and pertinent features for the Converged Plantwide Ethernet (CPwE) architecture configuration scenarios. Common Rockwell Automation use cases include:

- Inline Transparent Mode
- Inline Transparent Monitor-only Mode
- Inline Routed Mode
- Passive Monitor-only Mode

This publication describes the embedded software features and tools to configure and manage the security appliance. In addition, this publication provides information to help you resolve basic security configuration and network issues.

This manual assumes that you understand the following:

- Local area network (LAN) switch fundamentals
- Concepts and terminology of the Ethernet protocol and local area networking
- Proficient with CLI command-line programming language

This manual is intended for users of the appliance. We assume that you are familiar with the procedures in the Stratix 5950 Security Appliance Installation Instructions, publication 1783-IN002.

The publication, Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, provides detailed information about CPwE.

Subject matter authorities at Cisco and Rockwell Automation developed a collection of tested and validated architectures that are known as CPwE. Rockwell Automation follows the Cisco Validated Design (CVD) program. The content of CPwE is relevant to both Operational Technology (OT) and Informational Technology (IT) disciplines and consists of documented architectures, proven approaches, guidance, and configuration settings. CPwE architectures help manufacturers with design and deployment of a scalable, robust, secure, and future-ready, plant-wide industrial network infrastructure. CPwE also helps manufacturers to achieve the benefits of cost reductions by using proven designs, which can help lead to quicker deployment of new technology with reduced risk.

Read and understand this manual and CPwE before using the products. Consult your Rockwell Automation representative if you have any questions or comments.

Download firmware, associated files, and access product release notes from the Product Compatibility and Download Center (PCDC) at: http://www.rockwellautomation.com/rockwellautomation/support/pcdc.page

The Cisco Firewall and FirePOWER® manuals provide detailed instructions, including the following topics.

- Cisco ASA software and hardware compatibility and requirements
- Cisco ASA series documentation
- Cisco Security Manager
- FirePOWER System, Cisco SSL Appliance, and FireAMP

Links to these manuals are available in Additional Resources on page 8.

Summary of Changes

This manual contains new and updated information.

Topic	Page
Upgrade the Bootloader	122

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

Resource	Description
Stratix 5950 Security Appliance Installation Instructions, publication 1783-IN002	Provides detailed specifications and information that is related to installation of the security appliance.
Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001	Provides specification information for Stratix switches and appliances.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guides	Provides detailed information about Converged Plantwide Ethernet (CPwE).
Product Certifications website, http://www.rockwellautomation.com/global/certification/overview.page	Provides declarations of conformity, certificates, and other certification details.
ASA and ASDM documentation http://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html	Lists the Cisco ASA software and hardware compatibility and requirements. Describes the available Cisco ASA series documentation and provides links to access the documentation online.
CSM Documentation http://www.cisco.com/c/en/us/support/security/security-manager/products-documentation-roadmaps-list.html	Lists Cisco Security Manager documentation roadmaps.
FireSIGHT™ Documentation http://www.cisco.com/c/en/us/td/docs/security/firesight/roadmap/firesight-roadmap.html	Describes the available FirePOWER System documentation, including legacy FireSIGHT System and FirePOWER 3D System documentation, Cisco SSL Appliance documentation, and FireAMP documentation and provides links to access the documentation.

You can view or download publications at http://www.rockwellautomation.com/global/literature-library/overview.page. To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales representative.

Chapter 1

About the Security Appliance

Overview

The Stratix® 5950 security appliance is a DIN rail-mounted ruggedized, 64-bit industrial product that provides firewall, threat defense, and VPN services. A DIN Rail is a standard metal rail that is widely used for mounting circuit breakers and industrial control equipment inside equipment racks.

The Stratix 5950 security appliance is low power, fanless, with a dedicated Gigabit Ethernet management port.

Table 1 - License Descriptions

License Attribute	1783-SAD4T0SBK9 Copper	1783-SAD4T0SPK9 Copper	1783-SAD2T2SBK9 Fiber	1783-SAD2T2SPK9 Fiber
4x10/100/1000 Base T	x	x		
2x10/100/1000 Base T			x	x
Management port	x	x	x	x
Base License	x		x	
2x1GbE SFP Base License			x	x
ASA SW	x	x	x	x
FirePOWER® and App Control	x	x	x	x
K9[1]	x	x	x	x

Table 1 - License Descriptions

License Attribute	1783-SAD4T0SBK9 Copper	1783-SAD4T0SPK9 Copper	1783-SAD2T2SBK9 Fiber	1783-SAD2T2SPK9 Fiber
TA License[2]	x	x	x	x
VPN for SSL [3]		x		x
Clientless SSL[4]		x		x
IPSec[5]		x		x
Supports 3DES/AES[6]	x	x	x	x

[1] A web-based filtering technology that provides automatic updates when you need a robust, real-time solution.

[2] Helps provide increased control and protection during system updates.

[3] Allows for the creation of a secure, encrypted connection without requiring specialized software.

[4] Helps deliver secure access to preconfigured network resources on a corporate network with an SSL-enabled web browser.

[5] IPSec is a standard set of protocols that provides data security at the IP packet level.

[6] Encryption standards that offer additional layers of data security.

The Stratix 5950 security appliance comes with Cisco® ASA firewall protection, which is combined with FirePOWER threat protection. The security appliance has firewall images pre-installed with appropriate licenses.

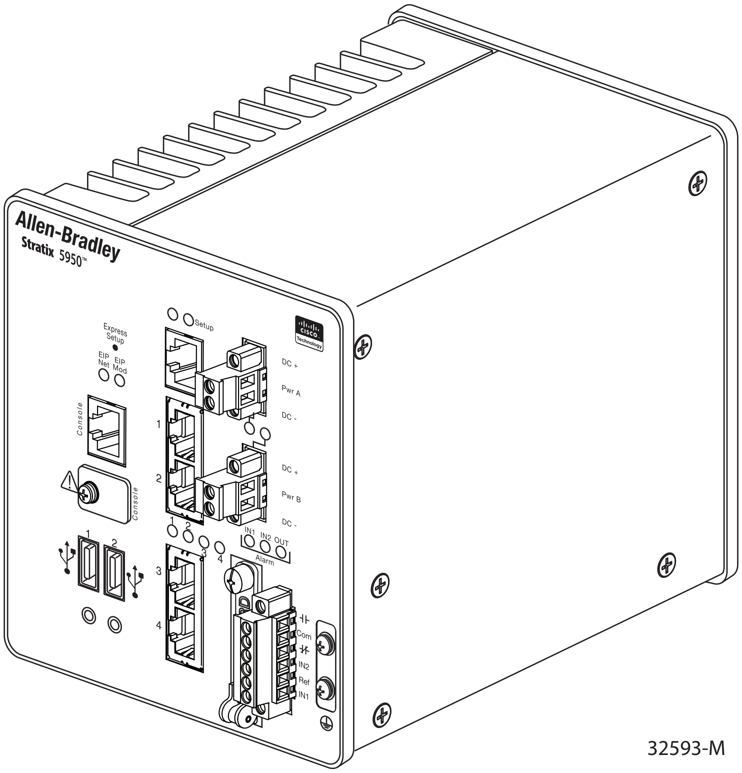
Hardware Features

The following are the hardware features of the Stratix 5950 security appliance.

- Dedicated management-only Gigabit Ethernet port
- Mini-USB and RJ45 console port
- Bypass Relay (only available on copper ports). Bypass relay is used when there is a loss of power or under software control.
- ±12V DC…48V DC Rated (9.6V DC…60V DC Maximum) redundant power inputs with 20…12 AWG screw cage terminals
- Cisco ASA firewall protection, which is combined with FirePOWER® threat protection
- Two external USB-A ports for addition of memory cards, security tokens, modems, or other USB 2.0-compliant devices
- Two alarm inputs
- Fault relay outputs
- DIN Rail mounts incorporated into the chassis
- Fan-less design
- Industrial temperature SDHC card
- Secure boot support

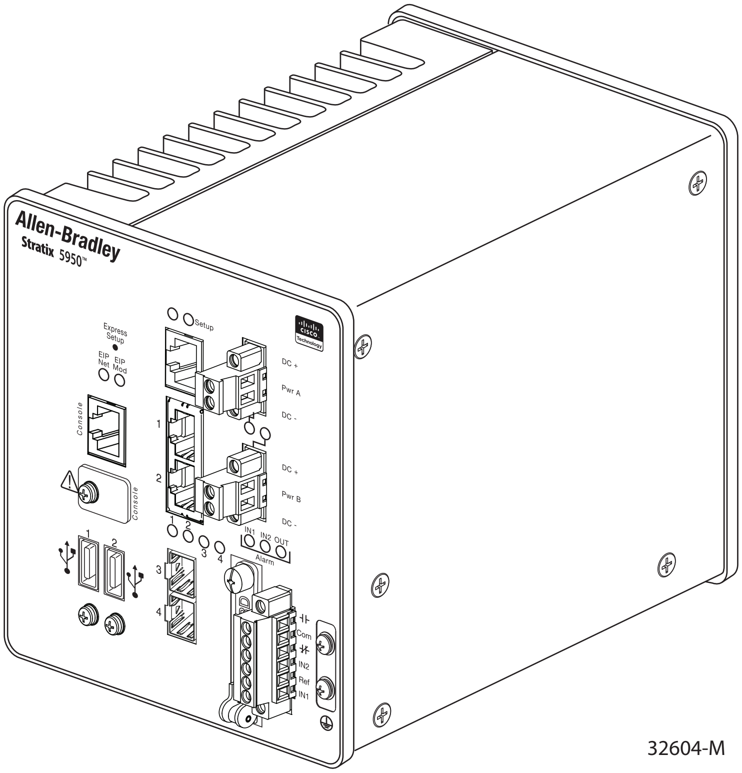
For complete information on how to install the security appliance, see the Stratix 5950 Security Appliance Installation Instructions, publication 1783-IN002.

Figure 1 - Stratix 5959 Security Appliance Copper



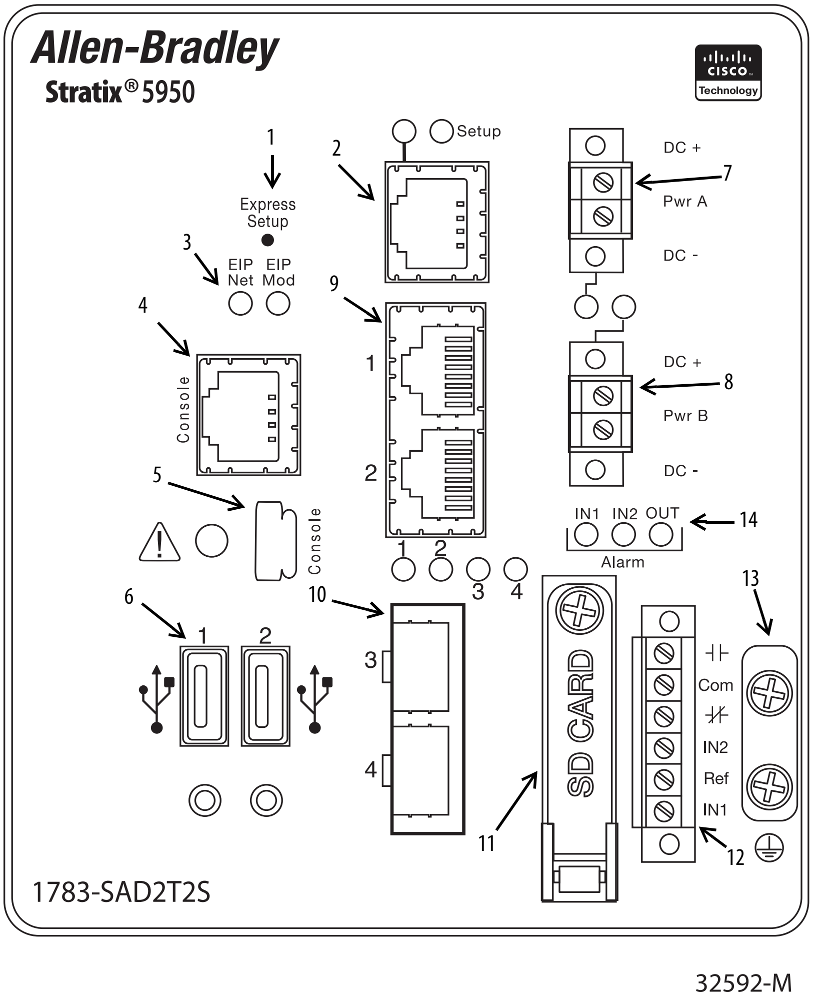
32593-M

Figure 2 - Stratix 5950 Security Appliance Fiber



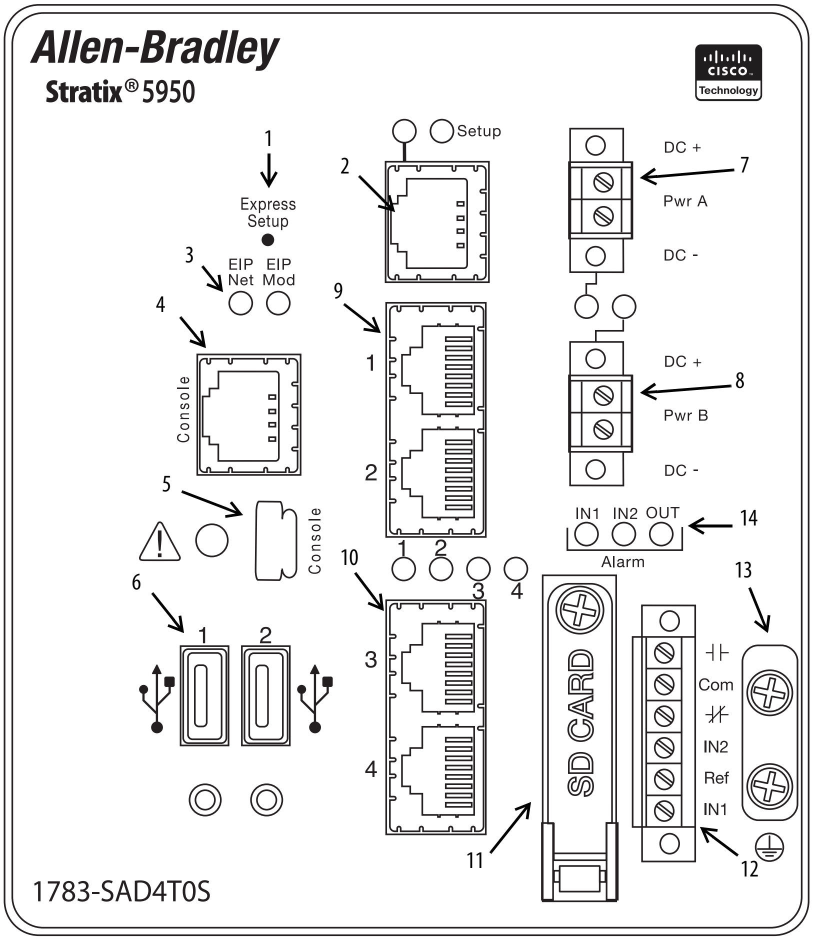
32604-M

Figure 3 - Stratix 5950 Security Appliance Fiber Front Panel



Item	Description	Item	Description
1	Express Setup pinhole Access	8	DC Power connection B
2	Console, Management	9	RJ45 10/100/100 BaseT Connectors 1 & 2
3	EIP ModStatus	10	On the Stratix 5950 Fiber SKU, the SFP sockets.
4	Console connector (RJ45)	11	SD Card Slot
5	Console connector (mini-USB)	12	Alarm Connectors
6	USB connectors	13	Grounding point
7	DC Power connection A	14	Alarm

Figure 4 - Stratix 5950 Security Appliance Copper Front Panel



Item	Description	Item	Description
1	Express Setup pinhole Access	8	DC Power connection B
2	Console, Management	9	RJ45 10/100/100 BaseT Connectors 1 and 2
3	EIP ModStatus	10	On the Stratix 5950 Copper SKU, the RJ45 10/100/100 BaseT Connectors 3 and 4
4	Console connector (RJ45)	11	SD Card Slot
5	Console connector (mini-USB)	12	Alarm Connectors
6	USB connectors	13	Grounding point
7	DC Power connection A	14	Alarm

Status Indicators

For complete information about the Stratix 5950 security appliance status indicators, see Status Indicators on page 75.

Installation of the Security Appliance

To install the Stratix 5950 security appliance, follow the introductions in the Stratix 5950 Security Appliance Installation Instructions, publication 1783-IN002.

Express Setup Button

Express Setup resets the security appliance ASA configuration to the default configuration set by the factory.

To restore the security appliance configuration to the default configuration set by the factory, follow these steps.

1. Use a standard-size #1 paper clip with wire gauge 0.033 inches or smaller and
2. Press the Express Setup button after the device is fully booted.

When depressed, the push button follows these actions.

- Depressed 0 to < 3 seconds or > 15 seconds — No action is taken.
- Depressed > 3 seconds < 15 seconds —

  The appliance automatically restarts when the button is pushed. After restart, the unit runs the original factory default configuration.

TIP The new configuration does not take effect until after the system restarts. The system boots with the original factory default configuration, including ROMMON variables. The administrator can disable this feature via ASA CLI so that no action is taken when the push button is depressed.

The FirePOWER module is NOT reset to Factory Default with the Express Setup button pressed for >3 seconds and < 15 seconds.

Power Supply

The Stratix 5950 security appliance comes with redundant external power connector. The connector supports 12 - 48V DC. The connectors are Molex 5.00 mm Pitch Eurostyle Horizontal Plug, with Retention Screws.

The power supply does not support reverse polarity, but does have reverse polarity protection. If you reverse + & - connections, the system does not power on and there is no damage.

The + terminal always has to be greater than the - terminal for the system to operate. The difference is in the system grounding scheme that is used.

The Stratix 5950 security appliance supports three basic schemes:

- Isolated DC in, neither + nor - terminal is tied to chassis GND
- Positive DC in, negative (-) terminal is tied to chassis GND
- Negative DC in, positive (+) terminal is tied to chassis GND

TIP To confirm uninterrupted operation, the redundant power connections must be connected to independently separated power sources.

Small Form Factor Pluggable (SFP) Modules

Table 2 - Small Form Factor Pluggable (SFP) Modules

SFP P/N	Catalog	Description	Purchased Cisco PN	Cisco Catalog
PN-27874	1783-SFP100FX A	100FX SFP Fiber Transceiver	PN-29262	GLC-FE-100FX-RGD
PN-27875	1783-SFP100LX A	100LX SFP Fiber Transceiver	PN-29249	GLC-FE-100LX-RGD
PN-27876	1783-SFP1GSX A	1000SX SFP Fiber Transceiver	PN-29264	GLC-SX-MM-RGD
PN-27877	1783-SFP1GLX A	1000LX SFP Fiber Transceiver	PN-29265	GLC-LX-SM-RGD

Memory and Storage

The Stratix 5950 security appliance has 8 GB of DRAM. It also has two storage devices, a 50 GB SSD and a 15 GB update device. All memory components are factory default and not upgradeable by the end user.

SD Card

The Stratix 5950 security appliance has an SD card slot as shown in Figure 3 on page 13. The SD card lets you have easy access to updates, copy logs, and crash-dumps. You can copy anything from the ASA file-system (disk0) to the SD card. One, blank SD card (1 GB) is shipped with the appliance.

USB Ports

The Stratix 5950 security appliance has two externally accessible Type-A USB (4-pin) connectors. Each USB port supports output of 5 volts power and up to a maximum of 500 mA.

Management Ethernet Port

A management-only 10/100/1000 BaseT Ethernet port is provided. This port is the only port that is able to configure the device for initial setup of the system. This port is Management1/1 in the ASA configuration.

Console Port

You can configure the Stratix 5950 security appliance through a web interface, or through the console port. The console port is either an RJ45 or a Mini USB connector. You can use the Rockwell Automation USB to RJ45 console cable (part number 9300-USBCBL-CNSL).

The RJ45 console port uses the following default configuration settings:

- 9600 baud
- 8 data bits
- no parity
- 1 stop bit
- no flow control

If the USB Console Port is active, by default, the console switches from RJ45 to USB when the USB cable is detected. The USB Console Port is active when a cable is inserted and remote personal computer drivers are enabled. When both ports are connected, the Mini USB console port is used.

This table shows the pinouts for the CON/AUX RJ45 connector.

Table 3 - Pinouts for the CON/AUX RJ45 Connector

Pin	Signal	Direction
1	DTR	Output
2	3.3	Output
3	TXD	Output
4	GND	
5	GND	
6	RXD	Input
7	-	NC
8	-	NC

IMPORTANT The console port does not support a remote dial-in modem.

Alarm Ports

The Stratix 5950 security appliance has alarm ports as shown in Figure 1 on page 12. There are two conditions that can generate an alarm:

- When dual power supply is configured, and there is a failed or missing power supply.
- When the CPU temperature is in critical condition below -40 °C or above 105 °C (below -40 °F or above 221 °F)

When either condition is met, the alarm status indicator turns red, and a syslog message and SNMP trap is triggered.

The Stratix 5950 security appliance has alarm relay contacts that can be used for an external alert system. The alarm condition of a missing/failed power supply, when 'power-supply dual' is configured, triggers Alarm Relay output. This alarm condition also sets the alarm output status indicator to solid RED and sends out a syslog message.

Power Supply

The CLI command to configure dual power supplies is `power-supply dual`. When set, the system expects to see both power supplies functioning properly.

CLI Commands

```
stratix5950(config)# power-supply dual
```

This command informs ASA that system administration expects dual power-supply functioning. If any of the power supplies fails, alarm events can be triggered.

```
stratix5950(config)# no power-supply dual
(default)
```

This command informs ASA that system administration does not expect dual power-supply (either one or two power supplies that are functional are acceptable).

IMPORTANT When configured for dual power supply, and a failure occurs, the Alarm Out status indicator turns red. The alarm relay is also energized. A syslog message is generated:

```
Syslog: %ASA-1-735006: Power Supply Unit Redundancy Lost
```

When configured for dual power supply, and a failure recovers, the Alarm Out status indicator turns off. A syslog message is generated:

```
Syslog: %ASA-1-735005: Power Supply Unit Redundancy OK
```

Temperature Sensor

The operating system monitors the CPU temperature when it is running.

- If the CPU temperature is in a critical condition, below -40 °C or above +105 °C (below -40 °F or above +221 °F) the Alarm Out status indicator turns red.
- When the CPU temperature returns to a normal condition, the Alarm Out status indicator turns off.

The critical range of temperature is not configurable. It is hard-coded as below -40° C or above +105 °C (below -40 °F or above +221 °F).

Software Features

The following software features support the hardware.

- Software based on ASA version 9.12.0 and FirePOWER 6.4.0 supports the Stratix 5950 security appliance hardware platform.
- The software provides firewall, Network Address Translation (NAT), VPN, and intrusion prevention system (IPS) features
- ASDM Bundled Version 7.12.1 (including ASA FirePOWER)
- CSM version 4.11 and FireSIGHT Management Center version 5.4.1.6

TIP The Stratix 5950 security appliance is a joint technology collaboration with Cisco. You can leverage the CSM and FireSIGHT Management Center Cisco software bundles with this device.

- Windows 10 is not supported.

Industrial Firewall Use Cases

An industrial automation and control system (IACS) is deployed in a wide variety of discrete and process manufacturing industries. Such industries include automotive, pharmaceuticals, consumer goods, pulp and paper, oil and gas, and mining and energy. IACS applications are composed of multiple control and information disciplines such as continuous process, batch, discrete and hybrid combinations. A challenge that manufacturers face is the industrial hardening of standard Ethernet and IP converged with IACS networking technologies. Manufacturers must take advantage of the business benefits that are associated with the Industrial Internet of Things (IIoT).

Industrial Firewall Technology Overview

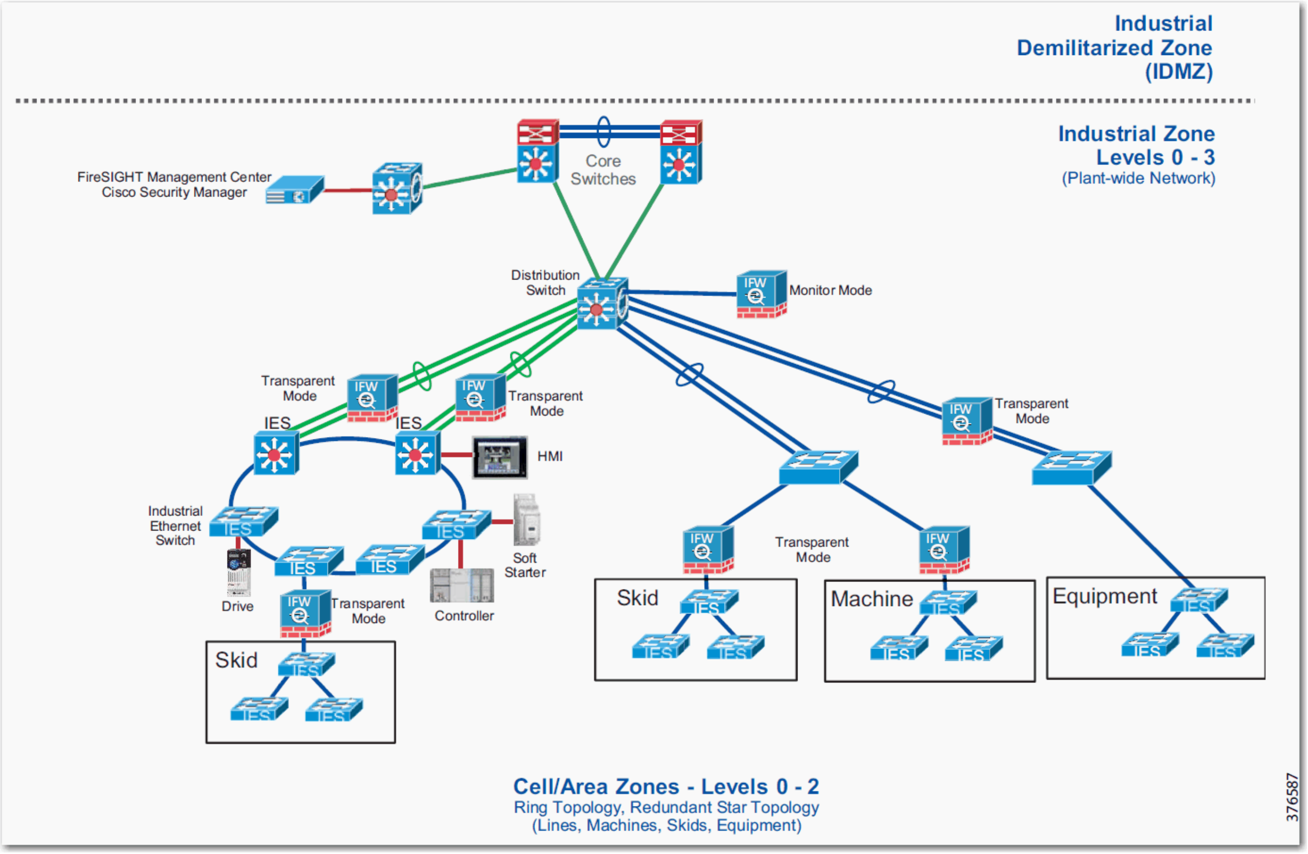
The industrial firewall (IFW) is used to separate networks with different security requirements and is also strategically placed within a network to monitor and log traffic. In this section, several architectures and the use cases they are meant to address are discussed.

Table 4 shows a summary of the use cases.

Table 4 - Types of Supported Industrial Firewall Technologies

Item	Description
Mode of operation	• Inline Transparent mode • Inline Routed mode • Passive Monitor-only mode
Network Protection	• Cisco® adaptive security appliance (ASA) • Intrusion prevention and detection (Cisco FirePOWER®) • Deep packet inspection (DPI)
Industrial firewall (IFW)	• The Allen-Bradley® Stratix® 5950 industrial network security appliance • Cisco industrial security appliance (ISA)
Application Use Cases	• Equipment/machine/skid protection • Cell/area zone protection – Redundant star topology – Ring Topology • Cell/area zone monitoring
Management Use Cases	• Local management – Command-line interface (CLI), adaptive security device manager • Centralized management – Cisco FireSIGHT™ management center, Cisco security manager • Change from local to centralized management of industrial firewalls

Figure 5 - Plant-wide Industrial Firewall Deployments


Industrial Demilitarized Zone (IDMZ)
Industrial Zone Levels 0 - 3 (Plant-wide Network)
FireSIGHT Management Center
Cisco Security Manager
Core Switches
Distribution Switch
IFW
Monitor Mode
Transparent Mode
IES
HMI
Industrial Ethernet Switch
Soft Starter
Drive
Controller
Skid
Machine
Equipment
Cell/Area Zones - Levels 0 - 2
Ring Topology, Redundant Star Topology
(Lines, Machines, Skids, Equipment)
376587

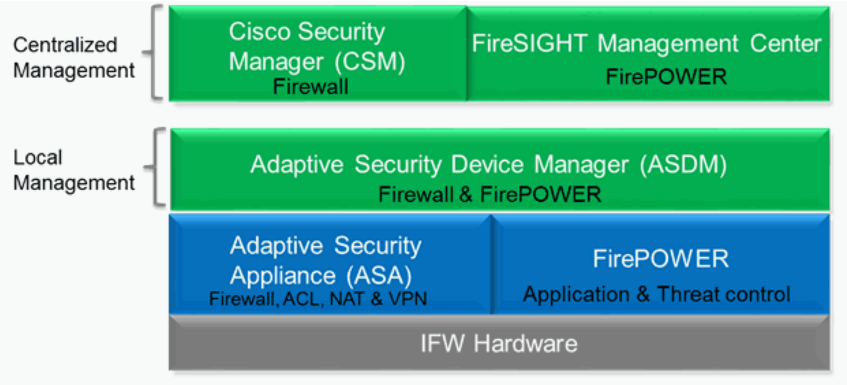
Logical Framework

Figure 6 provides a logical overview of the industrial firewall (IFW). The IFW has two components:

- Adaptive security appliance (ASA)
- FirePOWER module

The ASA provides firewall functionality, which can allow or deny traffic based on configured rules. The FirePOWER module performs application-specific protocol analysis for deep packet inspection (DPI). The IFW can be managed through either a local Adaptive Security Device Manager (ASDM) or through a centralized management server.

Figure 6 - Logical Framework


Centralized Management
Cisco Security Manager (CSM)
Firewall
FireSIGHT Management Center
FirePOWER
Local Management
Adaptive Security Device Manager (ASDM)
Firewall & FirePOWER
Adaptive Security Appliance (ASA)
Firewall, ACL, NAT & VPN
FirePOWER
Application & Threat control
IFW Hardware

Network Protection (Adaptive Security Appliance)

Firewalls are traditionally used to separate networks with different security requirements, such as the Enterprise zone and the Industrial Zone. One of the primary functions of a firewall is to help prevent unauthorized traffic from entering or exiting the network. To support this key functionality, firewalls are typically placed at the entrance or exit points of the network. Firewalls are known as ‘boundary’ or ‘edge’ security appliances because they define the boundary or the edge of a security zone.

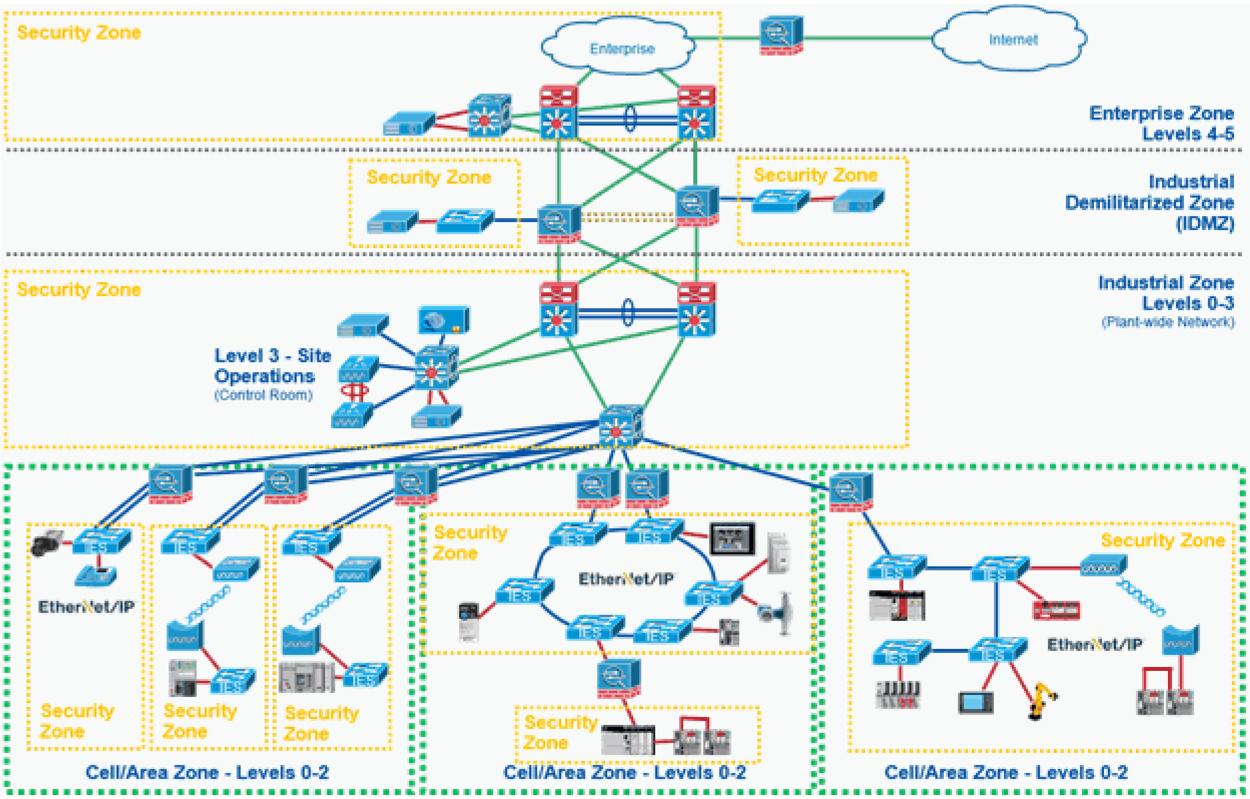
Figure 7 shows a high-level view of how a network can be segmented into security zones using firewalls.

Organizations have used firewalls as a means to control ingress and egress traffic from external untrusted networks to internal networks or systems. For example, organizations use firewalls to construct a demilitarized zone (DMZ) to provide ingress and egress traffic inspection. Firewalls are placed at the edge of a security zone and provide protection for Enterprise servers that communicate with the Internet.

Firewalls have also been placed between internal networks where security requirements are different between security zones. For example, the Enterprise Zone is oftentimes within another security zone than the Industrial Zone. It is a recommended practice to architect an industrial demilitarized zone (IDMZ) between these two security zones. The IDMZ is implemented using firewalls to define the security boundaries between the Enterprise and Industrial security zones.

Figure 7 shows how the security zones depicted can be applied to the CPwE network architecture to create DMZs and other types of segmentation.

Figure 7 - Security Zones within CPwE Architecture



Firewalls are normally positioned either as a node, where the network splits into multiple paths, or inline with one network path. In routed networks, the firewall usually resides at the location immediately before traffic enters the router. Most firewalls provide routing and, in some network designs, the firewall acts as both the firewall and the router.

Most firewalls inspect the following elements of a packet:

- Source MAC or IP address
- Destination MAC or IP address
- Source TCP or UDP Port
- Destination TCP or UDP Port
- Protocol - Layer 2, 3, 4, or 7

Firewalls that inspect these elements of a packet are commonly known as five-tuple firewalls. Typically, firewall rules include these five elements to configure a rule. The firewall is configured to permit or deny ingress and egress traffic that is based on these five-tuple rules.

A firewall can inspect traffic for conformance with proper protocol behavior and drop non-compliant traffic, but the firewall does not have deep knowledge of the protocol. To inspect and make permit-and-deny decisions at the protocol level, deep packet inspection (DPI) capabilities are needed. These DPI capabilities are discussed in the following section.

Intrusion Prevention and Detection (FirePOWER)

Deep packet inspection (DPI) views 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 while Intrusion Detection and Intrusion Prevention use DPI technology. IPS and intrusion detection system (IDS) relate to what is to be done after DPI inspects the packet.

As mentioned in the previous section, the primary function of the firewall is to permit or deny traffic between networks based on configured rules. Some firewalls can inspect traffic for conformance with proper protocol behavior and drop non-compliant traffic, but DPI functionality is required to interpret beyond the basic protocol behavior. Protocol interpretation is added to the DPI module so an administrator can configure DPI rules to monitor, log, permit, or deny packets as they relate to the protocol.

IPS inspects traffic that flows through a network and blocks or, otherwise, provides remediation for flows that it determines are malicious. Usually, IPS devices are placed inline with the traffic so the traffic can be blocked before it enters or exits the network, or before it reaches the end hosts.

IDS is similar to IPS, but it does not affect flows in any way. IDS only logs or alerts on malicious traffic based on the DPI rules.

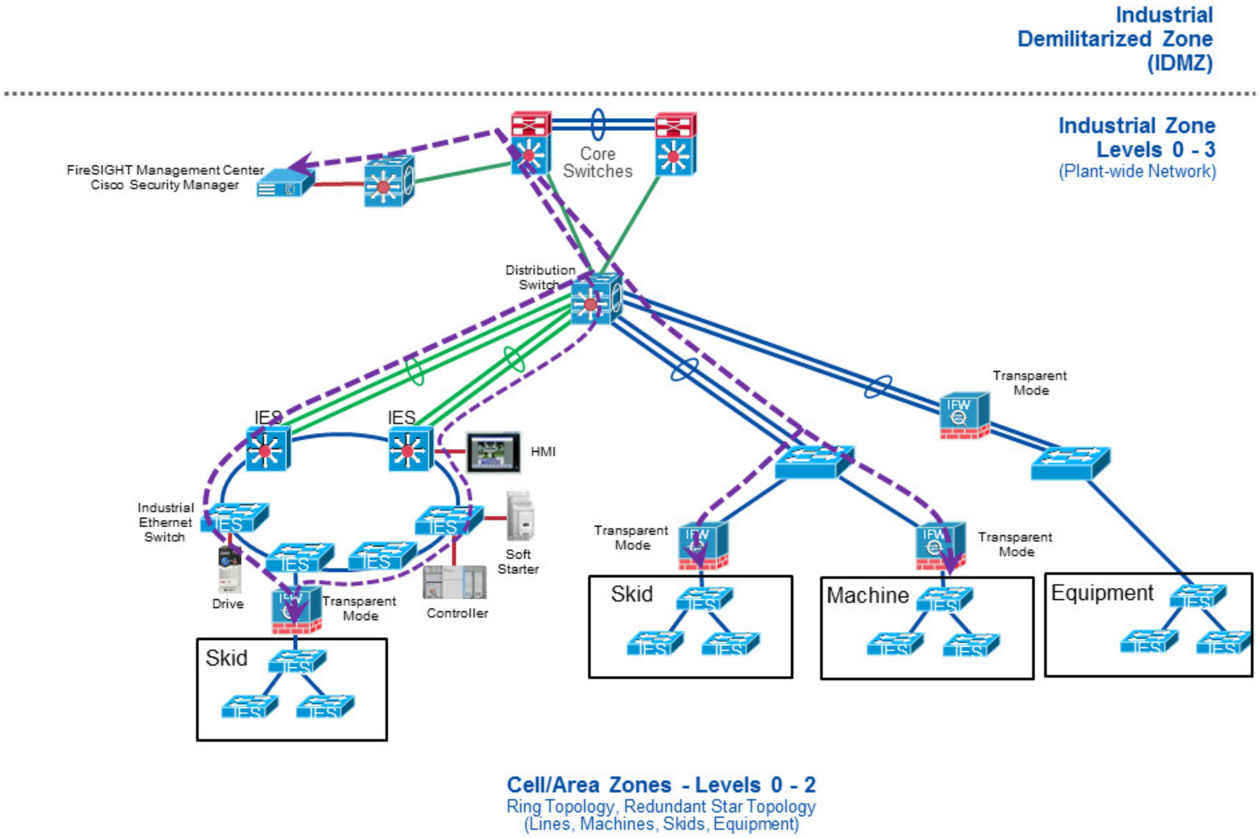
Machine/Skid Protection

The machine/skid protection use case is used to separate a machine, skid, or unit from a higher-level network. This use case can be to support different security requirements between the larger network and the machine/skid, or to restrict ingress and egress traffic. In this placement, the IFW can be run in either transparent or routed mode (refer to the corresponding subsection for details).

Transparent Mode

As shown below, the Transparent Mode firewalls are placed between a larger network and a grouping of automation equipment that act as a machine, skid, or unit. In each case, the IFW acts as an ingress and egress point to the machine/skid, where traffic can be monitored or controlled through firewall or DPI security policies.

Figure 8 - Industrial Firewall Placement for Machine/Skid Protection



Routed Mode

NAT

The ASAFirePOWER module supports the use of NAT in both transparent and routed mode. In most IACS environments, NAT is only be applied when the IFW is configured for routed mode, which is used when the interfaces are assigned to different networks. In most IACS NAT applications, the designer wants to assign different networks to the ingress and egress interfaces because they wish to reuse the inside or private IP addresses.

Address translation substitutes the real address in a packet with a mapped address that is routable on the destination network. NAT is composed of two steps: the process by which a real address is translated into a mapped address, and the process to undo translation for returned traffic.

The IFW translates an address when a NAT rule matches the traffic. If no NAT rule matches, processing for the packet continues

Considerations

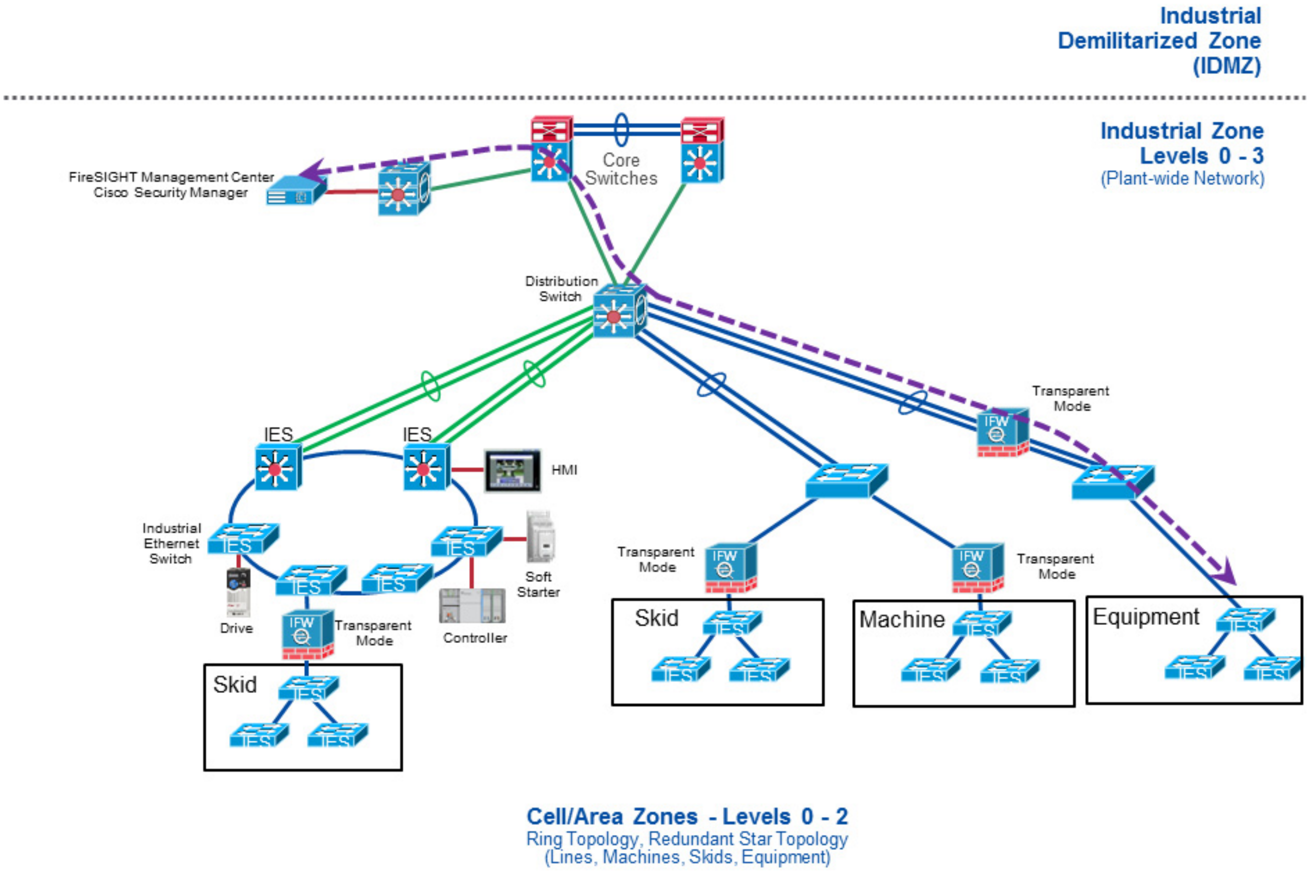
Before implementing the IFW in a machine/skid protection architecture, we recommended that the designer understand and document:

- Ingress and egress traffic-source and destination-host communications. For example, IP addresses of controllers, HMI, engineering workstations, and all communications that enter or leave the machine/skid must be known so firewall and DPI security policies can be configured.
- Ingress and egress traffic source and destination protocols must be known to configure the firewall and DPI rules.
- Ingress and egress traffic volume (refer to performance subsections within the Industrial Firewall Deployment Considerations section)
- Redundancy and availability requirements. For example, when considering high availability, one must consider the security considerations while in hardware bypass mode.
- Hardware bypass is only supported when the IFW is placed inline with an access link. When the IFW is placed inline with a trunk link, hardware bypass is not supported.

Redundant Star Cell/Area Zone Protection

When a redundant star network configuration is required to meet redundancy requirements, the IFW can be built in a manner to support redundant Layer 2 EtherChannel links. In Figure 9, the IFW is placed between the distribution switch and the plant floor equipment. This architecture is typically used when the IFW monitors or blocks traffic at a higher level in the network architecture, and a redundant star network is designed or deployed.

Figure 9 - Industrial Firewall Placement for Redundant Star Cell/Area Zone Protection



Considerations

Before implementing the IFW in a redundant star architecture, we recommend that the designer understands and documents:

- Ingress and egress traffic-source and destination-host communications. For example, IP addresses of controllers, HMI, engineering workstations, and all communications that enter or leave the machine/skid must be known so firewall and DPI security policies can be configured.
- Ingress and egress traffic source and destination protocols must be known to configure the firewall and DPI rules.
- Ingress and egress traffic volume (refer to performance subsections within the Industrial Firewall Deployment Considerations section)
- Redundancy and availability requirements. For example, when the IFW is configured with trunk ports, then hardware bypass mode is not available in this architecture.
- Hardware bypass is only supported when the IFW is placed inline with an access link. When the IFW is placed inline with a trunk link, hardware bypass is not supported.

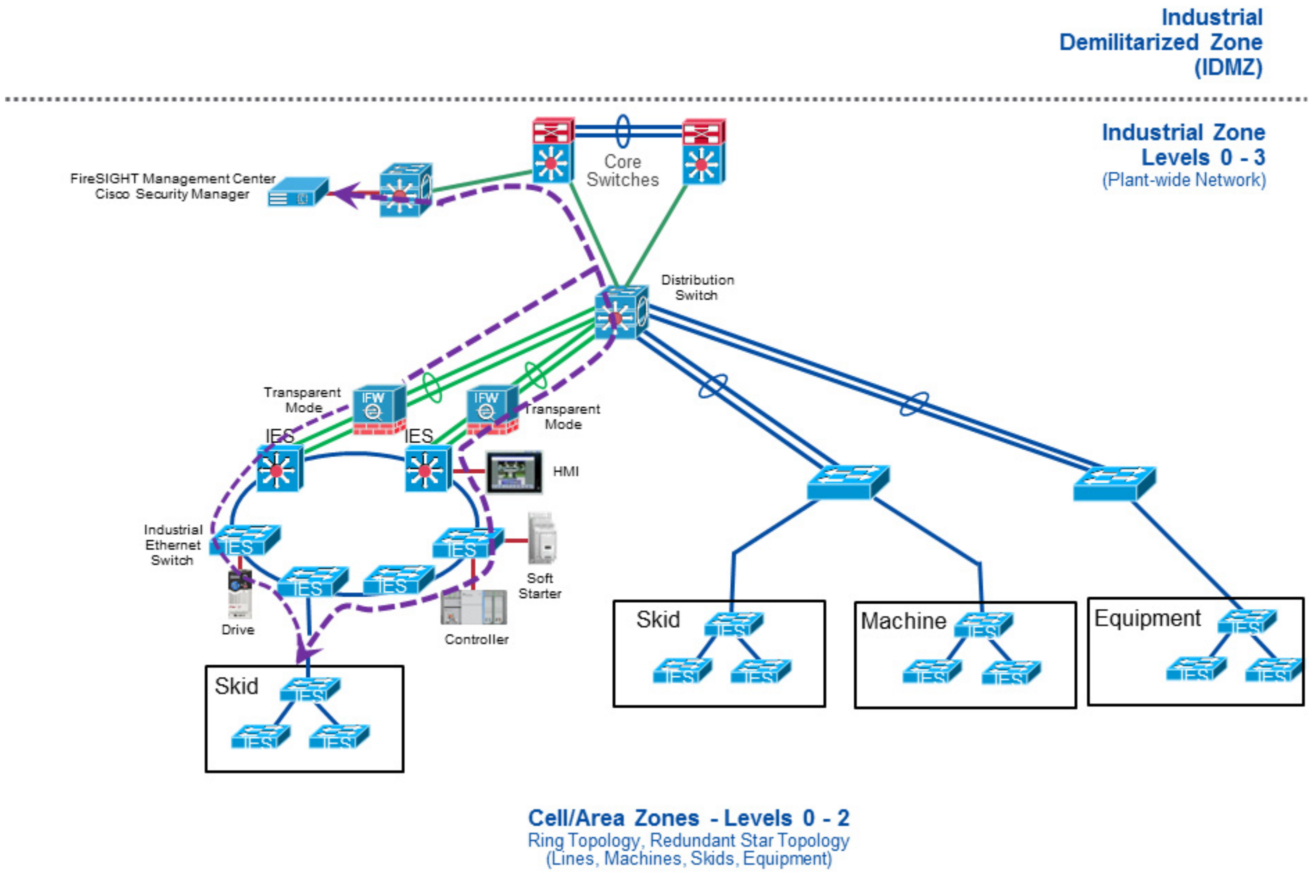
Ring Cell/Area Zone Protection

The ring cell/area zone protection use case is used to monitor and apply security policies to a ring. As shown in Figure 10, two Transparent Mode firewalls are placed between the distribution switches and the ring. The IFWs are not acting as an active/standby firewall pair in this configuration; rather, they simply provide firewall and, possibly, DPI functionality on both ingress points of the network ring.

Figure 10 - Industrial Firewall Placement for Ring Cell_Area Zone Protection

Considerations

IMPORTANT While it is a valid use case, ring cell/area zone protection implementation with the IFW as described in this section is not recommended due to architectural limitations of this deployment. Since active/standby pairing of the IFWs is not supported in this use case, when one IFW is disrupted, its connection state information is lost. Any persistent connections that are established via the disrupted IFW must expire, then re-establish via the remaining IFW, which results in significant communication downtime.


Industrial
Demilitarized Zone
(IDMZ)
Industrial Zone
Levels 0 - 3
(Plant-wide Network)
Core
Switches
FireSIGHT Management Center
Cisco Security Manager
Distribution
Switch
Transparent
Mode
IFW
IFW
Transparent
Mode
IES
IES
HMI
Industrial
Ethernet
Switch
IES
IES
IES
IES
Soft
Starter
Drive
Controller
Skid
IES
IES
IES
Skid
IES
IES
IES
Machine
IES
IES
IES
Equipment
IES
IES
IES
Cell/Area Zones - Levels 0 - 2
Ring Topology, Redundant Star Topology
(Lines, Machines, Skids, Equipment)

Before implementing the IFW in a ring cell/area zone protection architecture, it is recommended that the designer understands and documents:

- Ingress and egress traffic-source and destination-host communications. For example, IP addresses of controllers, HMI, engineering workstations, and all communications that enter or leave the machine/skid must be known so firewall and DPI security policies can be configured.

- Ingress and egress traffic source and destination protocols must be known to configure the firewall and DPI rules.

- Ingress and egress traffic volume (refer to performance subsections within the Industrial Firewall Deployment Considerations section)

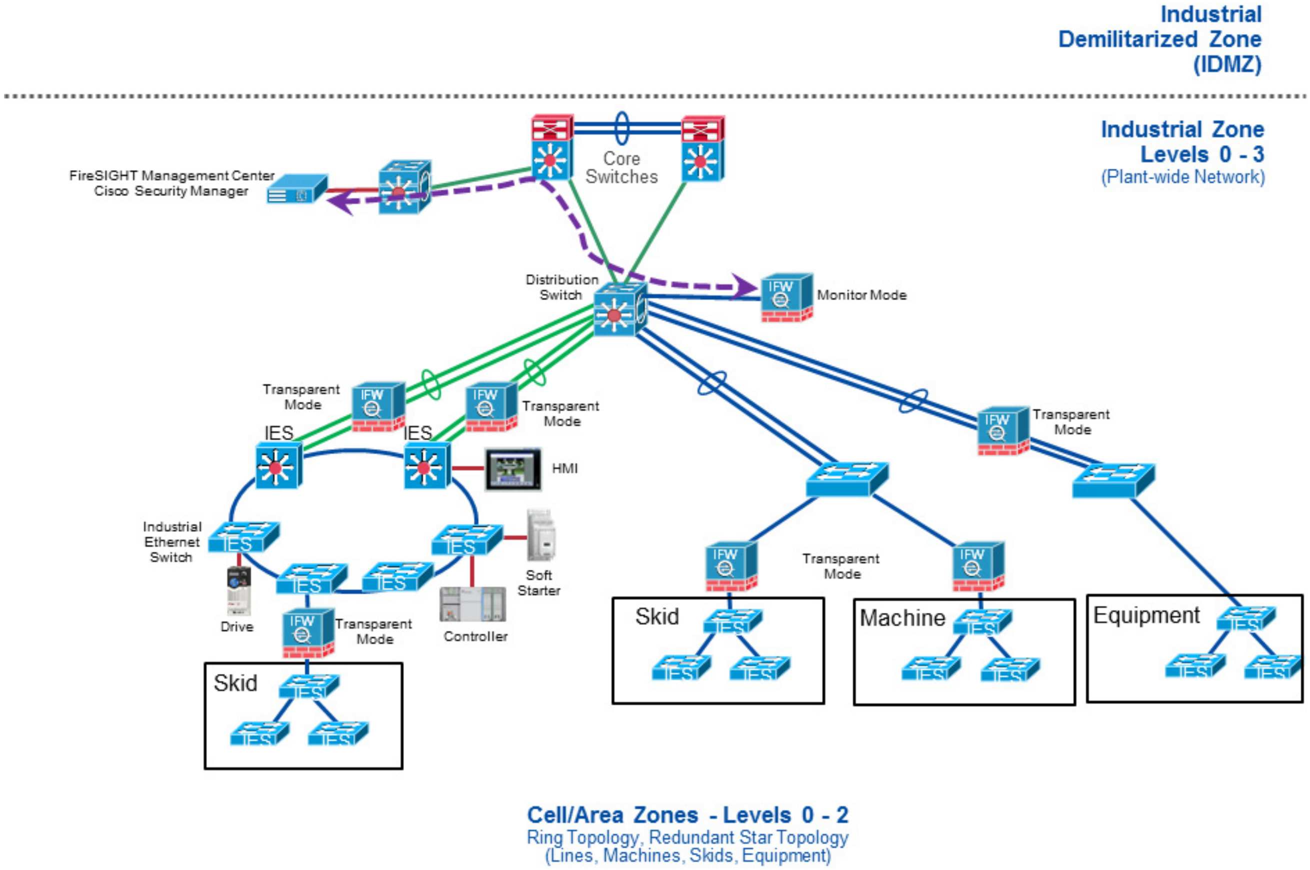
- Redundancy and availability requirements. In this use case, the ports are configured for Layer 3 EtherChannel.

- Hardware bypass is supported when the IFW is placed inline with a Layer 3 link.

Cell/Area Zone Monitoring

The cell/area zone monitoring mode use case in Figure 11 monitors traffic without placing the IFW directly inline of a controller, skid, machine, or cell/area zone of interest. The IFW is connected to a switch that has visibility to the traffic that is required to be monitored. A span session or port mirror is created to send the traffic of interest to the IFW.

Figure 11 - Industrial Firewall Placement for Cell/Area Zone Monitoring


Industrial Demilitarized Zone (IDMZ)
Industrial Zone Levels 0 - 3
(Plant-wide Network)
FireSIGHT Management Center
Cisco Security Manager
Core Switches
Distribution Switch
IFW
Monitor Mode
Transparent Mode
IES
HMI
Industrial Ethernet Switch
Soft Starter
Drive
Controller
Skid
Machine
Equipment
Cell/Area Zones - Levels 0 - 2
Ring Topology, Redundant Star Topology
(Lines, Machines, Skids, Equipment)

The Passive Monitor Mode architecture with CIP™ DPI is not recommended for monitoring and logging CIP connections. When OpenAppID rules are used with the FirePOWER module, the first packet that matches the CIP access control policy event is logged and the particular CIP connection is noted. Packets that match the access control policy and those packets that have the same connection ID are not sent to the log. For this reason, passive monitor mode with the CIP protocol it is not recommended.

Considerations

Before implementing the IFW in passive monitor-only mode, we recommended that the designer understands and documents:

- Ingress and egress traffic volume
- Hardware bypass is not applicable in passive monitor-only mode, since the IFW is not placed inline.

Time Synchronization

Along with the initial setup steps, the IFW must be configured with information on where to obtain its time synchronization data. The firewall and FirePOWER components of the IFW have separate settings for time, and both must be configured independently.

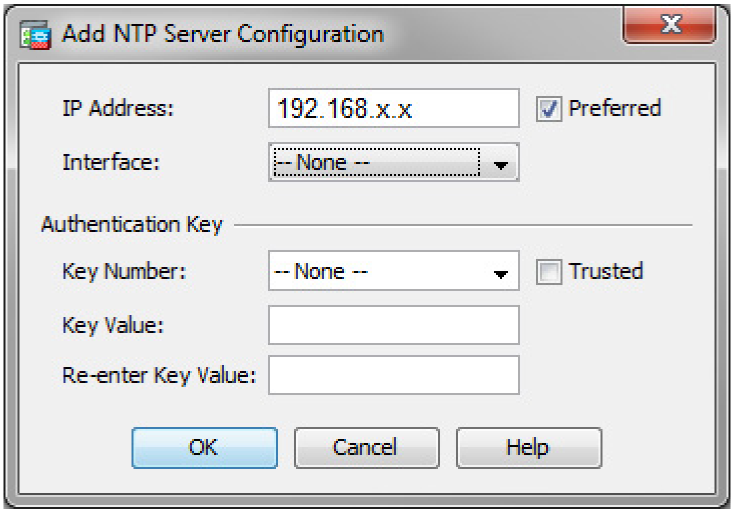
IMPORTANT Without properly configured timing information, unexpected behaviors can be observed; for example, intrusion events cannot be displayed in the real-time event log.

To configure time synchronization for the firewall component, complete the following steps:

1. Click Configuration at the top left, then Device Setup at the bottom left. From the Device Setup pane, select System Time > NTP.
2. To open the NTP server configuration window, click Add.

   Enter the IP address of the NTP server, and check Preferred to make this server the definitive time source. Choose from the Interface pull-down menu if NTP packets can be sent out of a particular interface. Finally, enter any NTP authentication information in the Authentication Key section of the window, and click OK.

Figure 12 - Firewall Add NTP Server Configuration Window



Add NTP Server Configuration

IP Address: 192.168.x.x ☑ Preferred

Interface: -- None --

Authentication Key

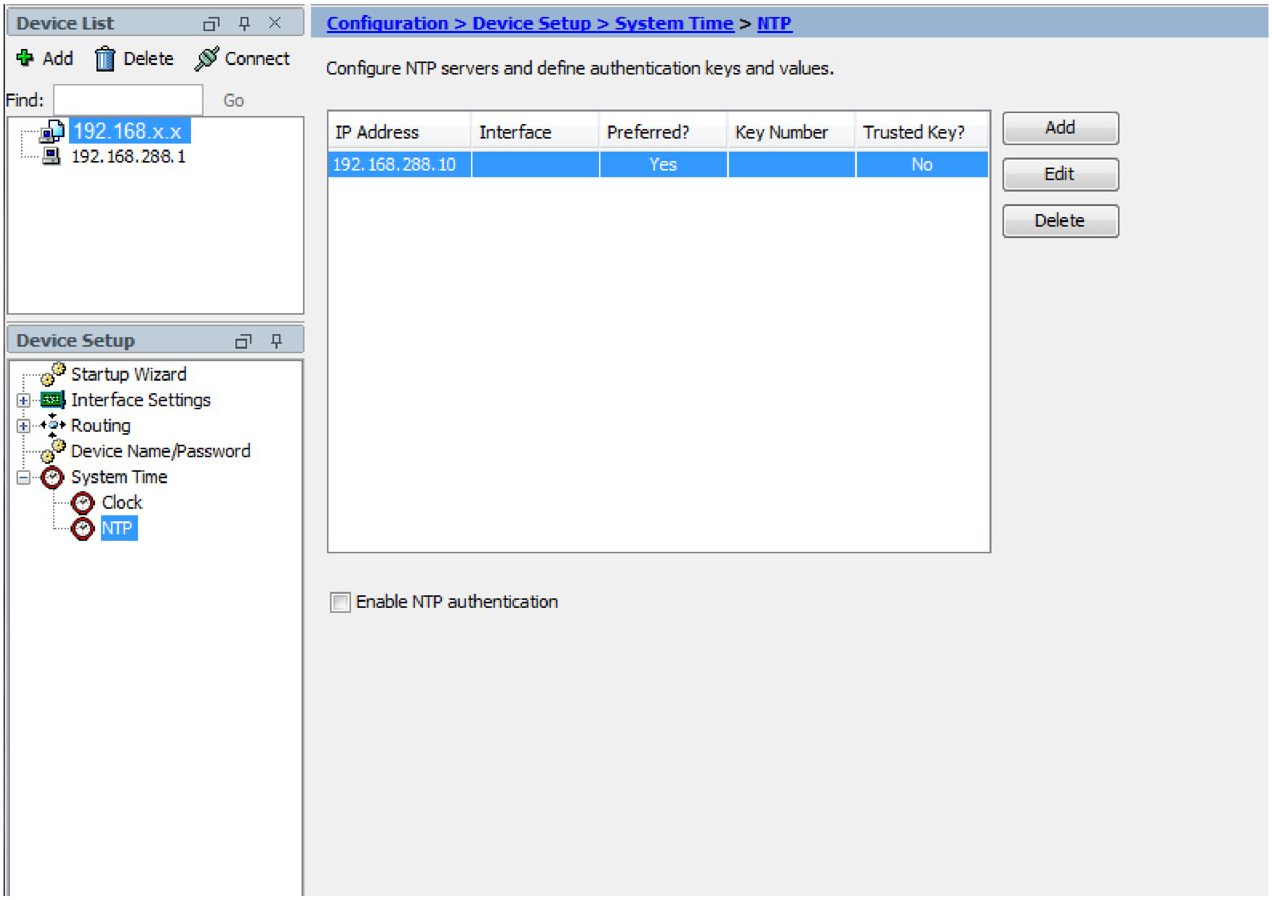
Key Number: -- None -- □ Trusted

Key Value:

Re-enter Key Value:

3. Confirm the NTP server settings that are displayed in the table, then click Apply to make the changes take effect.

Figure 13 - Firewall NTP Server Configuration Table



Configuration > Device Setup > System Time > NTP

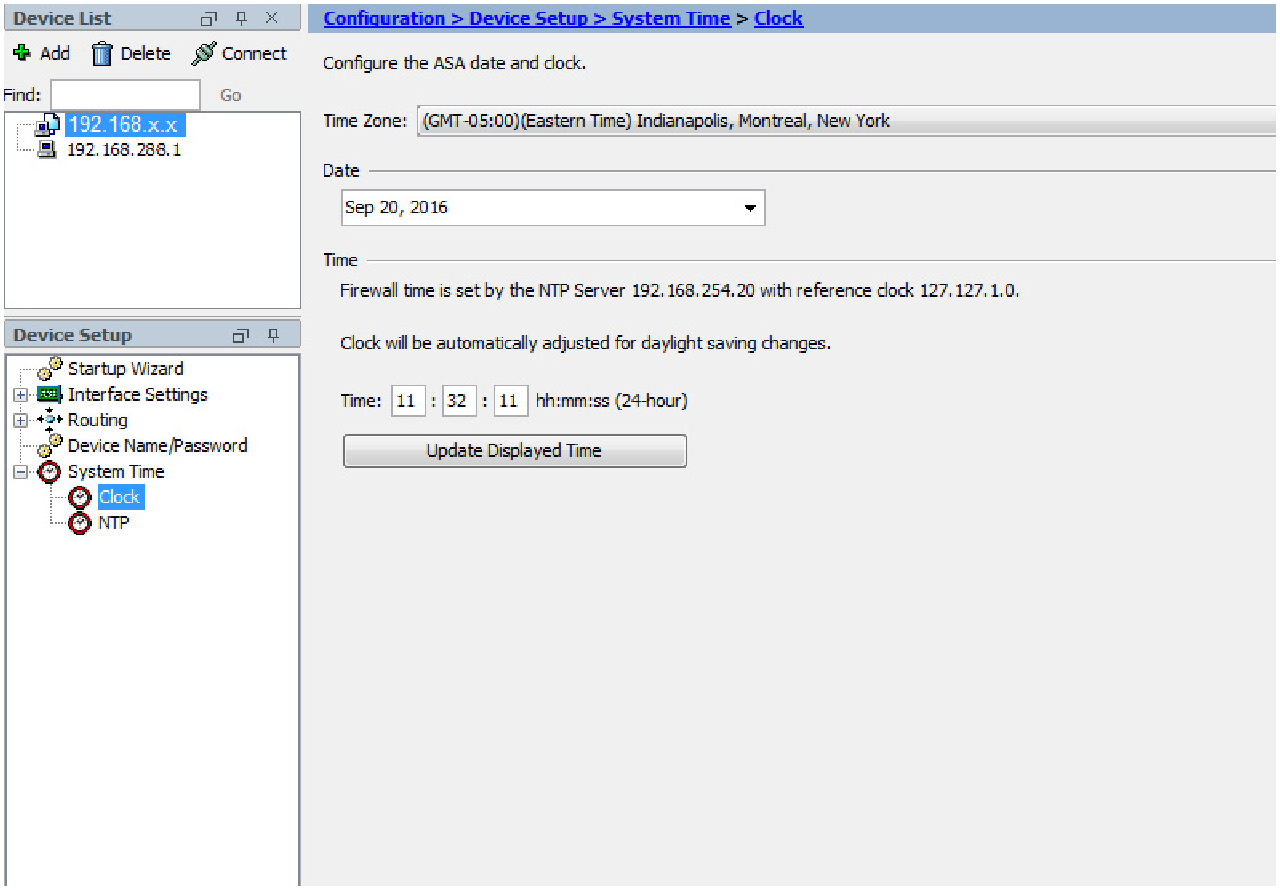
Configure NTP servers and define authentication keys and values.

IP Address	Interface	Preferred?	Key Number	Trusted Key?
192.168.288.10		Yes		No

□ Enable NTP authentication

4. Once synchronization is complete, in the Device Setup pane, select System Time>Clock and check the Time section to confirm that the firewall is receiving accurate time from the NTP server.

Figure 14 - Firewall Clock Settings Window



Configure the ASA date and clock.

Time Zone: (GMT-05:00)(Eastern Time) Indianapolis, Montreal, New York

Date

Sep 20, 2016

Time

Firewall time is set by the NTP Server 192.168.254.20 with reference clock 127.127.1.0.

Clock will be automatically adjusted for daylight saving changes.

Time: 11 : 32 : 11 hh:mm:ss (24-hour)

The equivalent CLI for this interface configuration is the following:

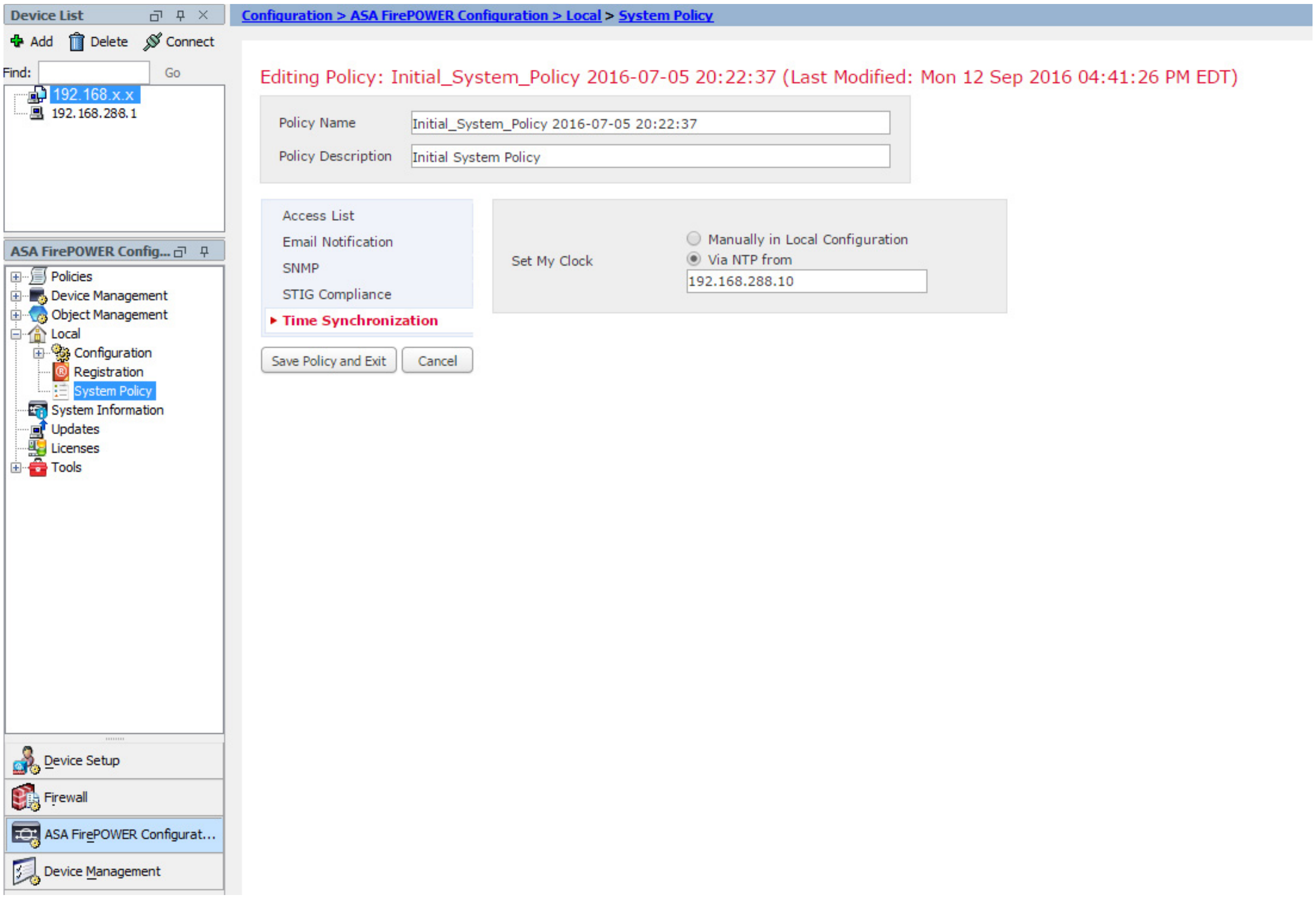
```
ntp server 192.168.254.20 prefer
```

To configure time synchronization for the FirePOWER component, complete the following steps:

1. Click Configuration at the top left, then ASA FirePOWER Configuration at the bottom left.
2. From the ASA FirePOWER Configuration pane, go to Local > System Policy.
3. For the policy labeled Initial System Policy, click the small pencil icon on the right side to edit the policy.
4. On the left side of the edit window, click the Time Synchronization option.
5. Next to Set My Clock, ‘Via NTP from’ and enter the IP address of the NTP server to be the same as the one for the firewall component.
6. Click Save Policy and Exit.
7. To apply the changes, click the green checkbox to the right of the Initial System Policy.

After the process is complete, a small window appears at the top, labeled Success.

Figure 15 - FirePOWER Time Synchronization Settings



Configuration > ASA FirePOWER Configuration > Local > System Policy

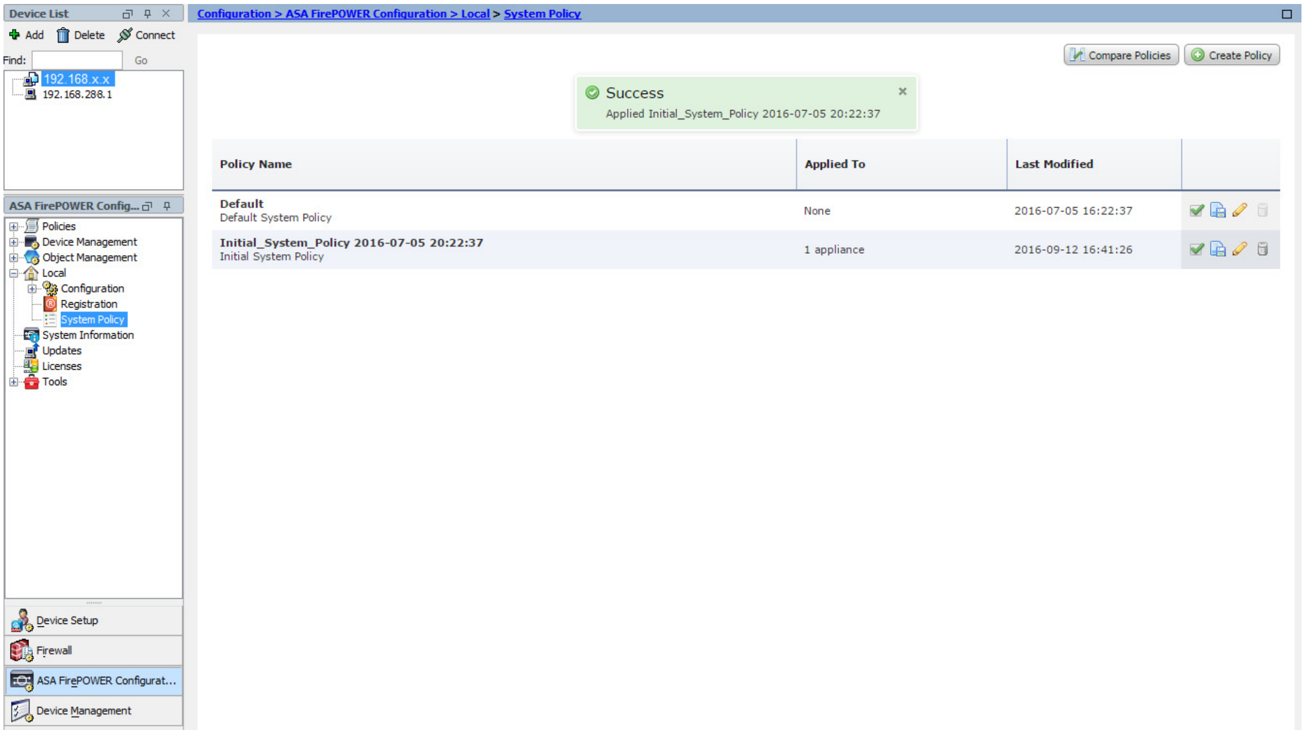
Editing Policy: Initial_System_Policy 2016-07-05 20:22:37 (Last Modified: Mon 12 Sep 2016 04:41:26 PM EDT)

Policy Name: Initial_System_Policy 2016-07-05 20:22:37

Policy Description: Initial System Policy

Set My Clock: ○ Manually in Local Configuration ● Via NTP from 192.168.288.10

Figure 16 - FirePOWER Initial System Policy Applied Changes



Configuration > ASA FirePOWER Configuration > Local > System Policy

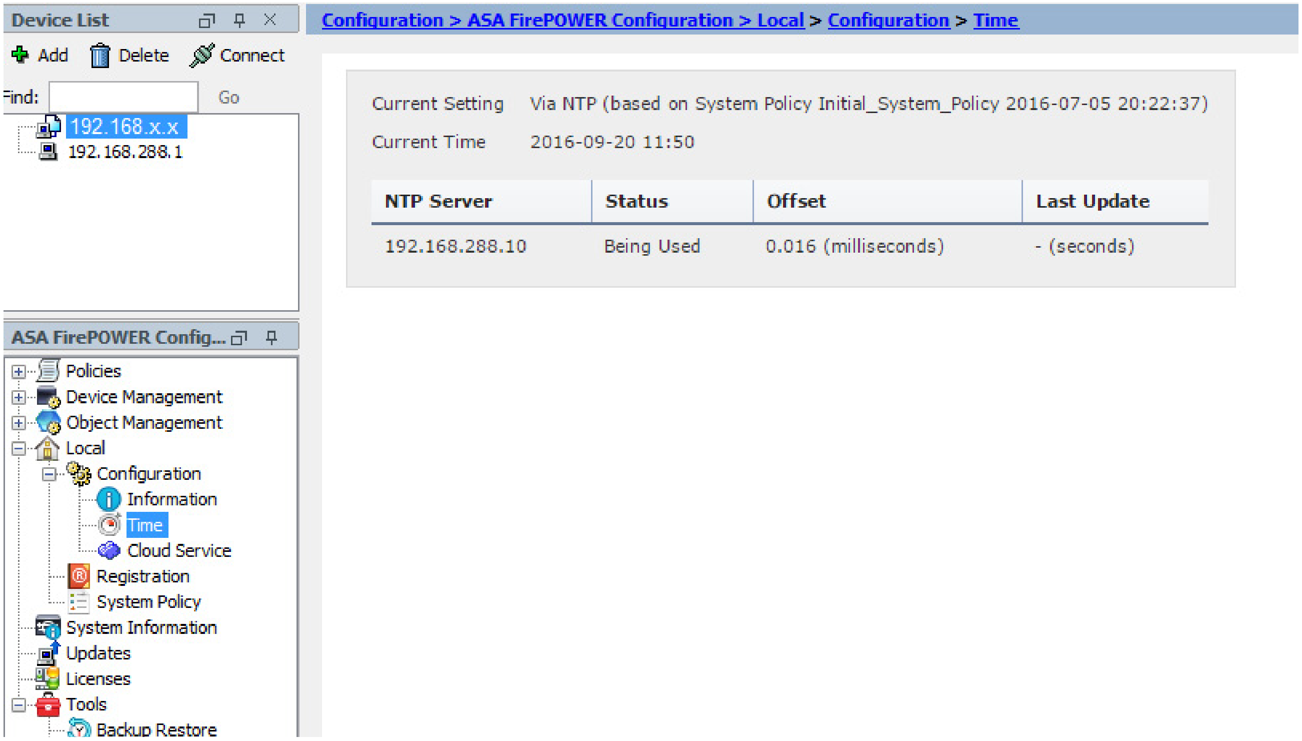
Success
Applied Initial_System_Policy 2016-07-05 20:22:37

Policy Name	Applied To	Last Modified
Default Default System Policy	None	2016-07-05 16:22:37
Initial_System_Policy 2016-07-05 20:22:37 Initial System Policy	1 appliance	2016-09-12 16:41:26

8. To confirm that time synchronization is working properly, in the ASA FirePOWER Configuration pane, select Local > Configuration > Time.

   The NTP server is listed here with a status of ‘Being Used’.

Figure 17 - FirePOWER Time Settings Window



Configuration > ASA FirePOWER Configuration > Local > Configuration > Time

Current Setting Via NTP (based on System Policy Initial_System_Policy 2016-07-05 20:22:37)

Current Time 2016-09-20 11:50

NTP Server	Status	Offset	Last Update
192.168.288.10	Being Used	0.016 (milliseconds)	- (seconds)

Configure the Security Appliance

IMPORTANT Every step that is described in this chapter must be followed for the security appliance to work as expected. If the steps are not followed as described, the appliance can appear to be working properly when it is not.

Deviation from the prescribed steps can cause the appliance not to behave as expected. Make sure to test your system configuration before using it. Do not assume it works as expected.

Rockwell Automation does not assume any responsibility for incorrect operation of the appliance due to misconfigured settings or applications. All IP addresses are fictional and for reference only. They are not related to your network configuration.

This scenario describes the basic out-of-the-box configuration, which is based on the following versions of Cisco® software.

- ASA: 9.12.0
- ASDM: 7.12.1
- ASA FirePOWER®: 6.4.0-97

Prerequisites

Follow these prerequisite steps before you attempt to configure the Stratix® 5950 security appliance. There are two deployment configurations that are described in this chapter. You must select a deployment configuration mode: Inline or SPAN Port.

All steps that are listed in this chapter apply to both configurations unless otherwise noted.

Here is what you need:

- Deployment Configuration Guide
- Power supply
- Console cable
- Ethernet cable
- Device
- Personal computer

Ethernet Devices

Identify the Ethernet devices that you are going to connect to the device: switch, servers, and workstations or personal computers. Verify that each device has a network interface card (NIC) for connecting to Ethernet ports.

Partially configuration of the device using Cisco ASA commands through the console port is required. An ASCII terminal or a personal computer that is running terminal emulation software to connect to the console port is needed.

1. Make sure that you are using a personal computer that is configured with a supported operating system. For a list of supported operating systems, see the release notes at:

   http://www.cisco.com/c/en/us/td/docs/security/asdm/7_6/release/notes/rn76.html
2. Install the latest version of Java.

   Go to https://www.java.com
3. Install a Terminal Emulator, such as PuTTY.
4. Obtain the Stratix 5950 security appliance from the factory, no cables connected.
5. Obtain the cable, DB9-to-RJ45 that is shipped with the appliance.
6. Determine the Management network for the device, for example: 10.0.1.0.24
7. Contact your Network Administrator, and obtain two IP addresses in the Management network.
   a. IP address 1 is for the ASA management IP address, for example: 10.0.1.1
   b. IP address 2 is for the SFR management IP address, for example: 10.0.1.2

8. Determine the network that you want to use the appliance to monitor, for example: 192.168.1.0/24 (Inline configuration mode only)
9. Contact your Network Administrator and obtain an IP address in the network that you want to monitor, for example: 192.168.1.218 (Inline configuration mode only)
10. Obtain a list of DNS servers from your Network Administrator.

Device Setup

Follow these steps to configure the Cisco ASA software.

1. Set NIC on your computer to DHCP.

Next, you must connect the Management interface on the Stratix 5950 security appliance to the NIC on your computer.

2. Connect the serial cable from Console port on the security appliance to the serial port on your computer.
3. Apply power to the security appliance.
4. Wait until the EIP Mod status indicator turns solid green.

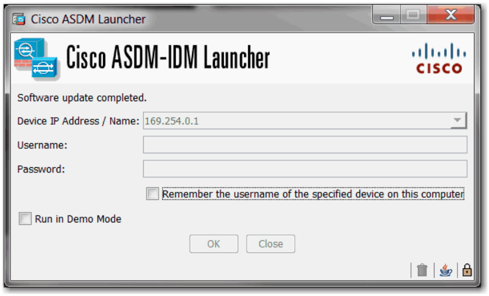
   The green status indicator flashes until complete, about 5 minutes.
5. Connect to https://169.254.0.1/admin.

   Ignore self-signed certificate warnings.
6. Click either Install ASDM Launcher or Run ASDM, depends on what your system displays.

   If you are required to click Install ASDM Launcher, steps 8…10 apply.
7. When prompted for a username and password, leave the fields blank and click login.
8. Run the dm-launcher.msi file that was downloaded.
9. Install using the default options.

   Cisco ASDM-IDM Launcher launches automatically.

10. In the Device IP address / Name field, enter 169.254.0.1.



Cisco ASDM Launcher

Cisco ASDM-IDM Launcher

Software update completed.

Device IP Address / Name: 169.254.0.1

Username:

Password:

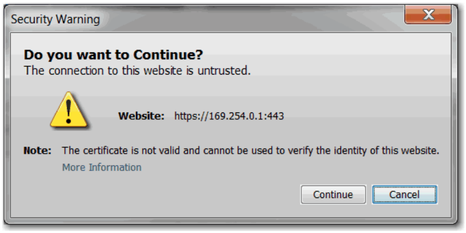
□ Remember the username of the specified device on this computer

□ Run in Demo Mode

11. Leave the Username/Password field blank.

12. Select OK.

13. Ignore certificate warnings, click continue.



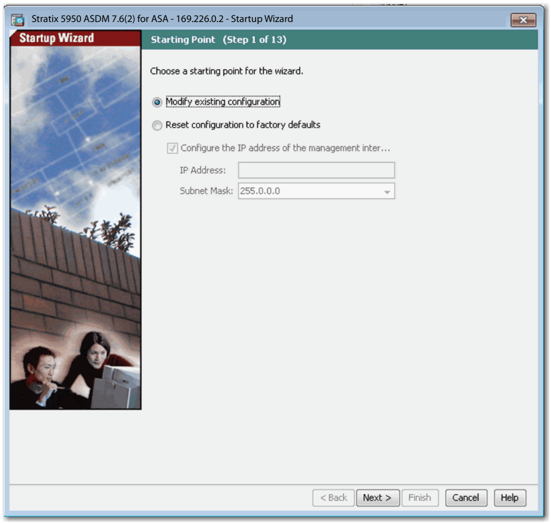
Security Warning

Do you want to Continue?
The connection to this website is untrusted.

Website: https://169.254.0.1:443

Note: The certificate is not valid and cannot be used to verify the identity of this website.
More Information

14. ASDM launches.



Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard

Startup Wizard

Starting Point (Step 1 of 13)

Choose a starting point for the wizard.

● Modify existing configuration

○ Reset configuration to factory defaults

☑ Configure the IP address of the management inter...

IP Address:

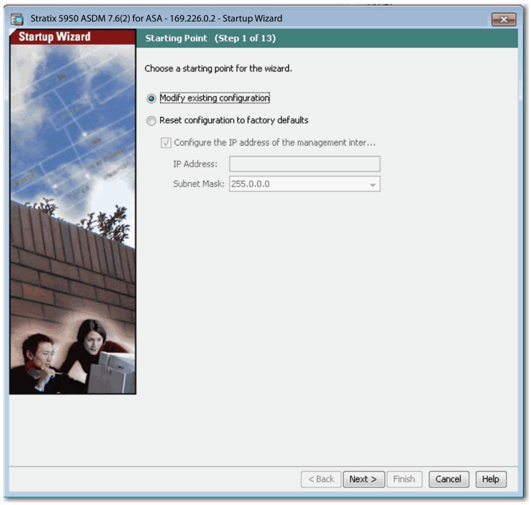
Subnet Mask: 255.0.0.0

The Startup Wizard launches automatically.

Startup Wizard

Follow these steps to complete the configuration by using the Startup Wizard. Be sure to complete all screens.

1. Choose a starting point and click Next.



Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard

Startup Wizard

Starting Point (Step 1 of 13)

Choose a starting point for the wizard.

● Modify existing configuration

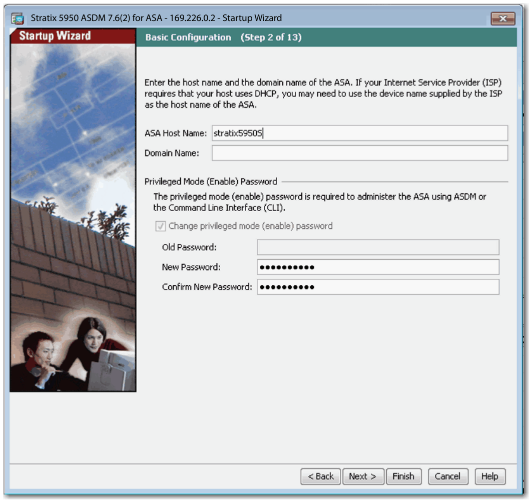
○ Reset configuration to factory defaults

☑ Configure the IP address of the management inter…

IP Address:

Subnet Mask: 255.0.0.0

2. Enter the host name and the domain name of the ASA.



Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard

Startup Wizard

Basic Configuration (Step 2 of 13)

Enter the host name and the domain name of the ASA. If your Internet Service Provider (ISP) requires that your host uses DHCP, you may need to use the device name supplied by the ISP as the host name of the ASA.

ASA Host Name: stratix5950S

Domain Name:

Privileged Mode (Enable) Password

The privileged mode (enable) password is required to administer the ASA using ASDM or the Command Line Interface (CLI).

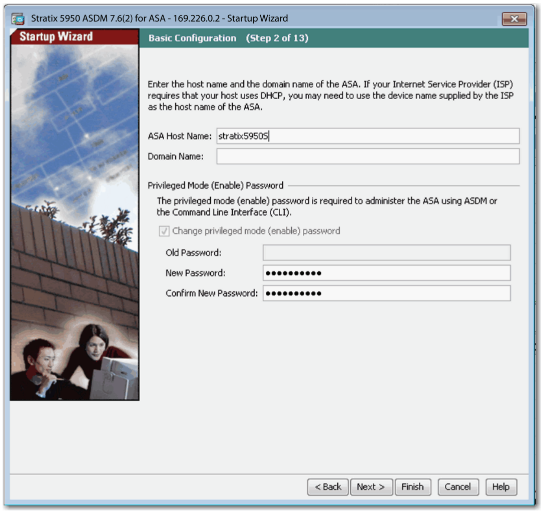
☑ Change privileged mode (enable) password

Old Password:

New Password: ••••••••••

Confirm New Password: ••••••••••

3. Provide password information.



Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard
Startup Wizard

Basic Configuration (Step 2 of 13)

Enter the host name and the domain name of the ASA. If your Internet Service Provider (ISP) requires that your host uses DHCP, you may need to use the device name supplied by the ISP as the host name of the ASA.

ASA Host Name: stratix5950S

Domain Name:

Privileged Mode (Enable) Password

The privileged mode (enable) password is required to administer the ASA using ASDM or the Command Line Interface (CLI).

☑ Change privileged mode (enable) password

Old Password:

New Password: ●●●●●●●●●●

Confirm New Password: ●●●●●●●●●●

4. On the Management IP address Configuration dialog box (Step 2of 13).

   a. Inline Mode Only:

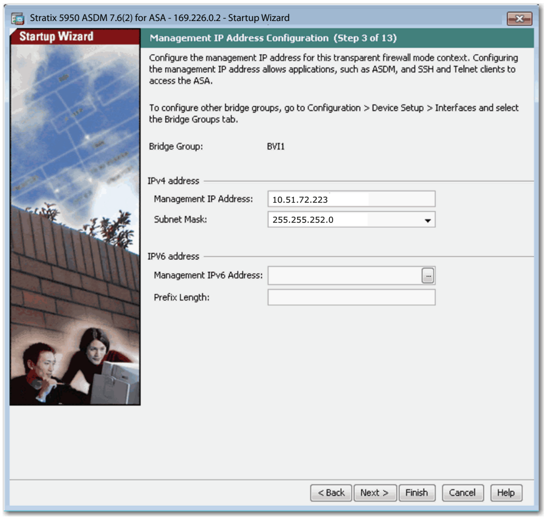
      Enter the IP address and Subnet Mask from the range of the network you want to monitor.

   b. SPAN Port Mode Only:

      Enter a temporary/dummy IP address that is not in the management network.

      The Subnet Mask must be changed to something other than 255.255.255.255. For example, IP Address = 2.2.2.2, Subnet Mask = 255.255.255.0

IMPORTANT This address is NOT the Management IP addresses in the Management network.



Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard
Startup Wizard

Management IP Address Configuration (Step 3 of 13)

Configure the management IP address for this transparent firewall mode context. Configuring the management IP address allows applications, such as ASDM, and SSH and Telnet clients to access the ASA.

To configure other bridge groups, go to Configuration > Device Setup > Interfaces and select the Bridge Groups tab.

Bridge Group: BVI1

IPv4 address

Management IP Address: 10.51.72.223

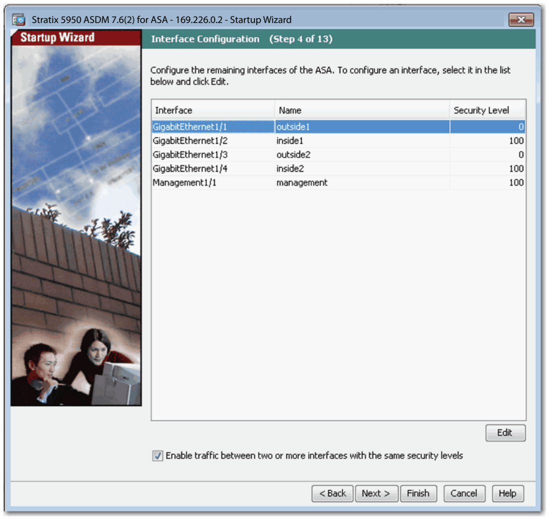
Subnet Mask: 255.255.252.0

IPV6 address

Management IPv6 Address:

Prefix Length:

5. On the Interface Configuration dialog box, edit the Management1/1 interface.



Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard

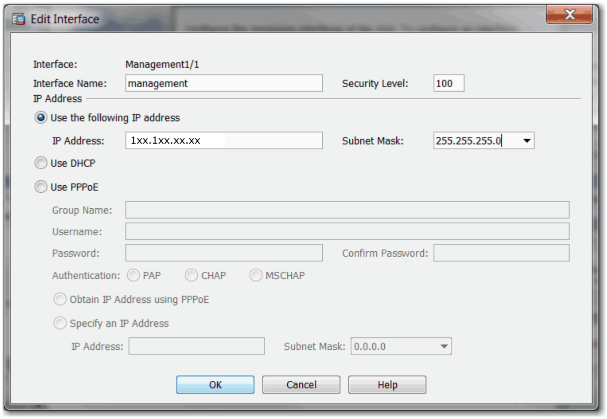
Interface Configuration (Step 4 of 13)

Configure the remaining interfaces of the ASA. To configure an interface, select it in the list below and click Edit.

Interface	Name	Security Level
GigabitEthernet1/1	outside1	0
GigabitEthernet1/2	inside1	100
GigabitEthernet1/3	outside2	0
GigabitEthernet1/4	inside2	100
Management1/1	management	100

☑ Enable traffic between two or more interfaces with the same security levels

6. Enter the ASA Management IP address that you obtained from your network administrator.



Edit Interface

Interface: Management1/1

Interface Name: management

Security Level: 100

IP Address

● Use the following IP address

IP Address: 1xx.1xx.xx.xx

Subnet Mask: 255.255.255.0

○ Use DHCP

○ Use PPPoE

Group Name:

Username:

Password:

Confirm Password:

Authentication: ○ PAP ○ CHAP ○ MSCHAP

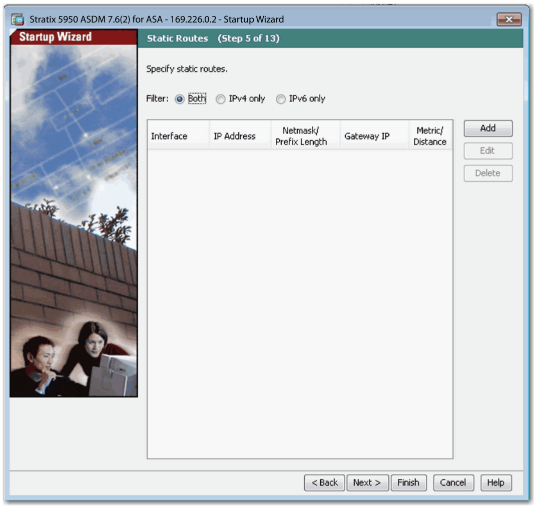
○ Obtain IP Address using PPPoE

○ Specify an IP Address

IP Address:

Subnet Mask: 0.0.0.0

7. Specify static routes and click Next.



Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard

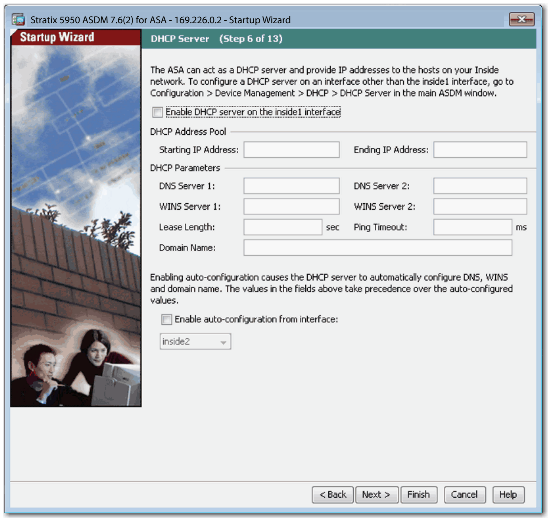
Static Routes (Step 5 of 13)

Specify static routes.

Filter: ● Both ○ IPv4 only ○ IPv6 only

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance

8. Decide to enable or not enable DHCP.



Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard

DHCP Server (Step 6 of 13)

The ASA can act as a DHCP server and provide IP addresses to the hosts on your Inside network. To configure a DHCP server on an interface other than the inside1 interface, go to Configuration > Device Management > DHCP > DHCP Server in the main ASDM window.

□ Enable DHCP server on the inside1 interface

DHCP Address Pool

Starting IP Address: Ending IP Address:

DHCP Parameters

DNS Server 1: DNS Server 2:

WINS Server 1: WINS Server 2:

Lease Length: sec Ping Timeout: ms

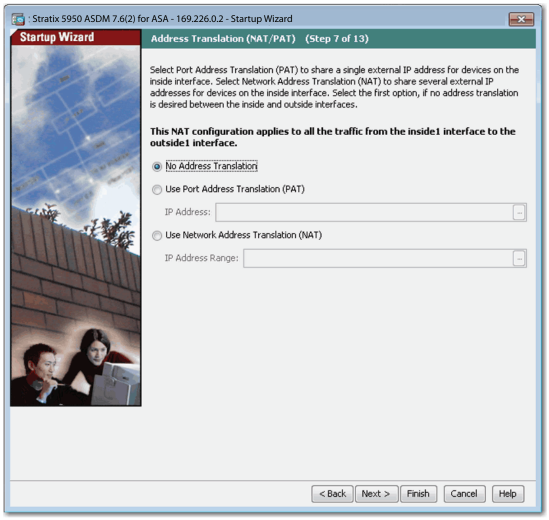
Domain Name:

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and domain name. The values in the fields above take precedence over the auto-configured values.

□ Enable auto-configuration from interface:

inside2

9. Select an Address Translation, if necessary, and then click Next.



Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard

Address Translation (NAT/PAT) (Step 7 of 13)

Select Port Address Translation (PAT) to share a single external IP address for devices on the inside interface. Select Network Address Translation (NAT) to share several external IP addresses for devices on the inside interface. Select the first option, if no address translation is desired between the inside and outside interfaces.

This NAT configuration applies to all the traffic from the inside1 interface to the outside1 interface.

● No Address Translation

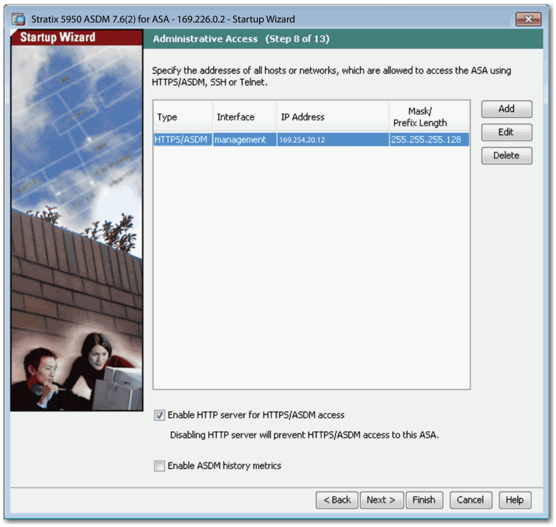
○ Use Port Address Translation (PAT)

IP Address:

○ Use Network Address Translation (NAT)

IP Address Range:

On the Administrative Access dialog box, edit the HTTPS/ASDM rule to allow web access to ASDM based on your management network configuration.



Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard

Startup Wizard

Administrative Access (Step 8 of 13)

Specify the addresses of all hosts or networks, which are allowed to access the ASA using HTTPS/ASDM, SSH or Telnet.

Type	Interface	IP Address	Mask/ Prefix Length
HTTPS/ASDM	management	169.254.20.12	255.255.255.128

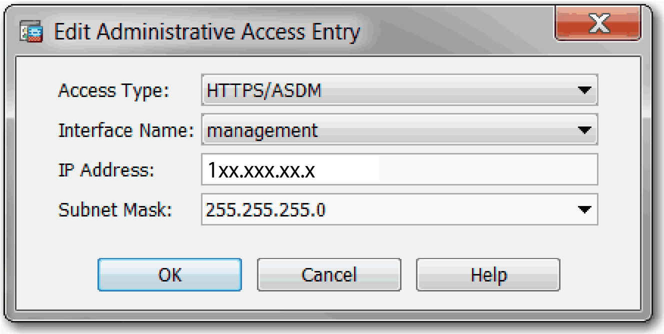
☑ Enable HTTP server for HTTPS/ASDM access

Disabling HTTP server will prevent HTTPS/ASDM access to this ASA.

☐ Enable ASDM history metrics

This edit can take a few minutes.

10. Identify Access Type, Interface name, and Enter IP Address and click OK.



Edit Administrative Access Entry

Access Type: HTTPS/ASDM

Interface Name: management

IP Address: 1xx.xxx.xx.x

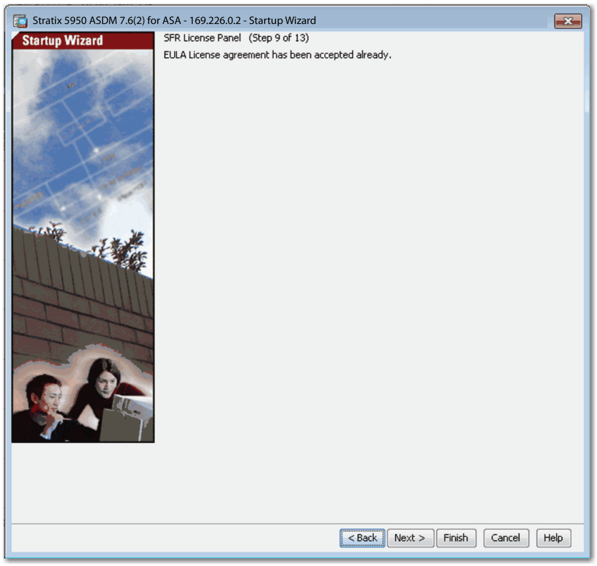
Subnet Mask: 255.255.255.0

11. On the ASA FirePOWER Basic Configuration dialog box, enter the SFR Management IP address information that you obtained from your network administrator.

12. Accept the Cisco End User License Agreement.

    In this example, the license has already been accepted.

13. Click Next.

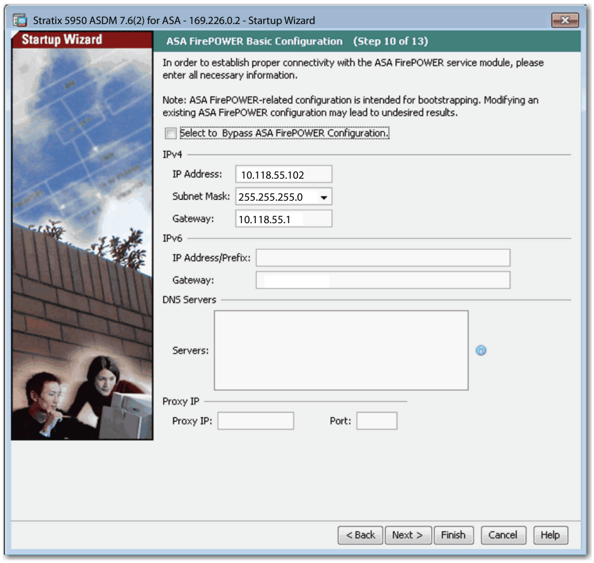


Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard

SFR License Panel (Step 9 of 13)

EULA License agreement has been accepted already.

14. Enter the necessary information and click Next.



Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard

ASA FirePOWER Basic Configuration (Step 10 of 13)

In order to establish proper connectivity with the ASA FirePOWER service module, please enter all necessary information.

Note: ASA FirePOWER-related configuration is intended for bootstrapping. Modifying an existing ASA FirePOWER configuration may lead to undesired results.

☐ Select to Bypass ASA FirePOWER Configuration.

IPv4

IP Address: 10.118.55.102

Subnet Mask: 255.255.255.0

Gateway: 10.118.55.1

IPv6

IP Address/Prefix:

Gateway:

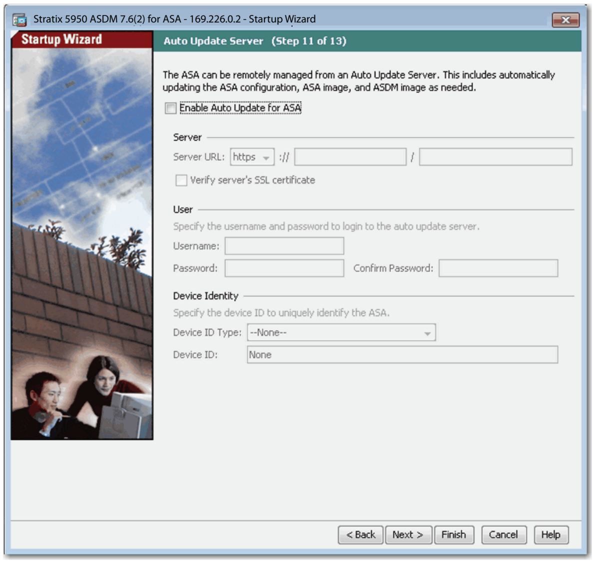
DNS Servers

Servers:

Proxy IP

Proxy IP: Port:

15. Enable Auto Update for ASA, if needed and click Next.



Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard

Startup Wizard

Auto Update Server (Step 11 of 13)

The ASA can be remotely managed from an Auto Update Server. This includes automatically updating the ASA configuration, ASA image, and ASDM image as needed.

□ Enable Auto Update for ASA

Server

Server URL: https :// /

□ Verify server's SSL certificate

User

Specify the username and password to login to the auto update server.

Username:

Password: Confirm Password:

Device Identity

Specify the device ID to uniquely identify the ASA.

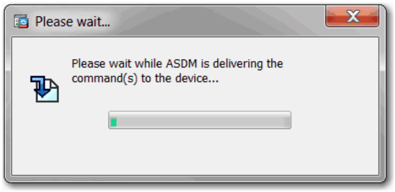
Device ID Type: --None--

Device ID: None

16. On the Startup Wizard Summary, click Finish.

The ‘Management IP Address’ listed in the ‘Configuration Summary’ is NOT the Management IP address in the Management network. This Management IP Address is the IP address of the network that you want to monitor.

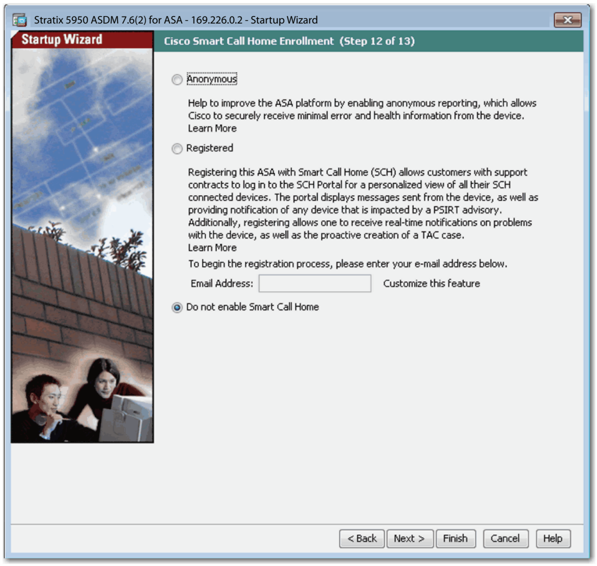
The wizard displays a wait message for a couple minutes.



Please wait...

Please wait while ASDM is delivering the command(s) to the device...

17. Enable Smart Call, if desired and click Next.



Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard

Startup Wizard

Cisco Smart Call Home Enrollment (Step 12 of 13)

○ Anonymous

Help to improve the ASA platform by enabling anonymous reporting, which allows Cisco to securely receive minimal error and health information from the device. Learn More

○ Registered

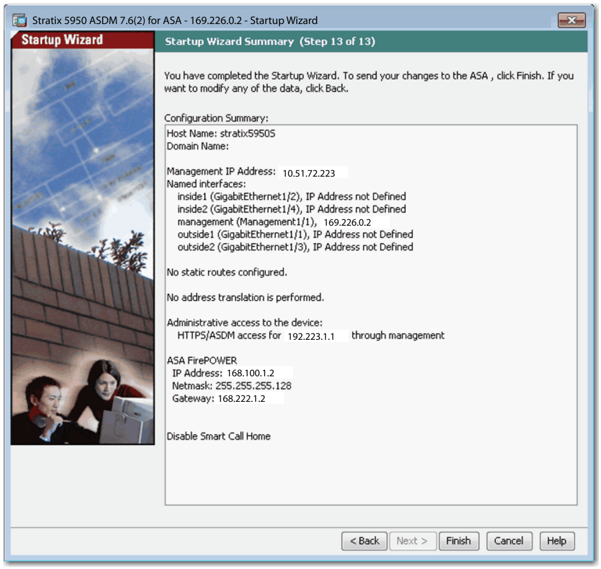
Registering this ASA with Smart Call Home (SCH) allows customers with support contracts to log in to the SCH Portal for a personalized view of all their SCH connected devices. The portal displays messages sent from the device, as well as providing notification of any device that is impacted by a PSIRT advisory. Additionally, registering allows one to receive real-time notifications on problems with the device, as well as the proactive creation of a TAC case. Learn More

To begin the registration process, please enter your e-mail address below.

Email Address: Customize this feature

● Do not enable Smart Call Home

18. Review your setup information. If you must change something, click Back and modify your settings.
19. When you are satisfied with the settings, click Finish.


Stratix 5950 ASDM 7.6(2) for ASA - 169.226.0.2 - Startup Wizard
Startup Wizard
< Back
Next >
Finish
Cancel
Help

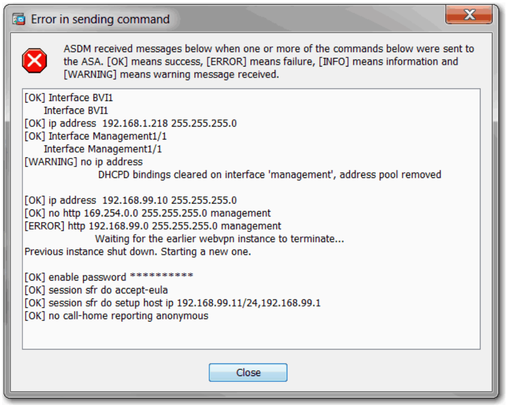
Startup Wizard Summary (Step 13 of 13)

You have completed the Startup Wizard. To send your changes to the ASA , click Finish. If you want to modify any of the data, click Back.

Configuration Summary:

```
Host Name: stratix5950S
Domain Name:

Management IP Address: 10.51.72.223
Named interfaces:
   inside1 (GigabitEthernet1/2), IP Address not Defined
   inside2 (GigabitEthernet1/4), IP Address not Defined
   management (Management1/1), 169.226.0.2
   outside1 (GigabitEthernet1/1), IP Address not Defined
   outside2 (GigabitEthernet1/3), IP Address not Defined

No static routes configured.

No address translation is performed.

Administrative access to the device:
   HTTPS/ASDM access for 192.223.1.1 through management

ASA FirePOWER
 IP Address: 168.100.1.2
 Netmask: 255.255.255.128
 Gateway: 168.222.1.2


Disable Smart Call Home
```

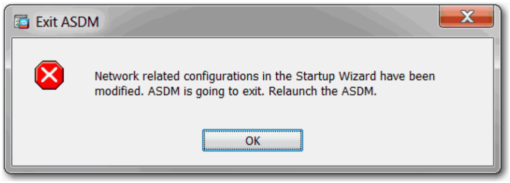
An error window can pop up.



ASDM received messages below when one or more of the commands below were sent to the ASA. [OK] means success, [ERROR] means failure, [INFO] means information and [WARNING] means warning message received.

```
[OK] Interface BVI1
     Interface BVI1
[OK] ip address  192.168.1.218 255.255.255.0
[OK] Interface Management1/1
     Interface Management1/1
[WARNING] no ip address
                 DHCPD bindings cleared on interface 'management', address pool removed

[OK] ip address  192.168.99.10 255.255.255.0
[OK] no http 169.254.0.0 255.255.255.0 management
[ERROR] http 192.168.99.0 255.255.255.0 management
                Waiting for the earlier webvpn instance to terminate...
Previous instance shut down. Starting a new one.

[OK] enable password **********
[OK] session sfr do accept-eula
[OK] session sfr do setup host ip 192.168.99.11/24,192.168.99.1
[OK] no call-home reporting anonymous
```

20. Click Close to ignore it.



Network related configurations in the Startup Wizard have been modified. ASDM is going to exit. Relaunch the ASDM.

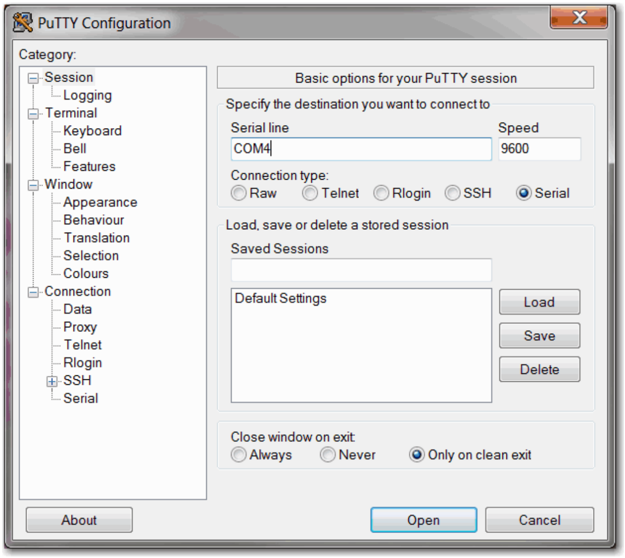
21. The wizard displays a message to wait while ASDM is loading the current configuration from your device.
22. Wait until loading is complete.
23. Eventually, the wizard displays the message, ‘Network related configurations in the Startup Wizard have been modified.’1
24. Click OK.

The ASDM software closes.

Configure FirePOWER Administrative Settings

To use PuTTY to connect to the serial port, follow these steps.

1. Run PuTTY and connect to the serial port of the device.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM4

Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

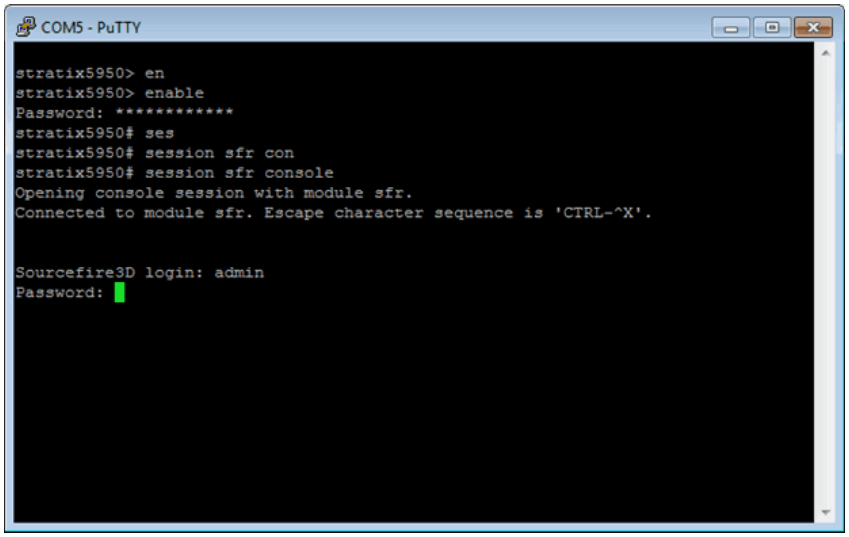
2. Click Open to start a command-line session.
3. At command line, press Enter.
4. Type: `stratix5950> enable`
5. Press Enter.
6. Enter the ASA password that was set in the Startup Wizard and press Enter.
7. Type: `stratix5950# session sfr console`
8. Press Enter.

9. Log in to FirePower with:

   username: `admin`

   Password: `Sourcefire`

   Passwords are case-sensitive.



```
stratix5950> en
stratix5950> enable
Password: ************
stratix5950# ses
stratix5950# session sfr con
stratix5950# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.


Sourcefire3D login: admin
Password:
```

10. Run `configure password` and change the password
11. Set the DNS servers that you obtained from your network administrator, for example:

    ```
    configure network dns servers [IP Address],
    [IP Address], [IP Address]
    ```
12. Run `exit`
13. Hold Control-Shift-6.
14. Release those keys, then press x.
15. Type `stratix5950# exit`

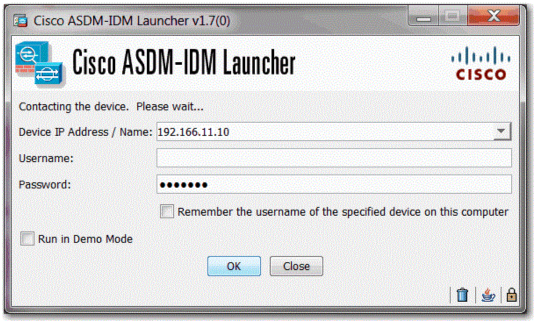
TIP To update the ASA, ASDM, FirePOWER software, and bootloader, see Chapter 9.

Configure the HTTPS Certificate Information

Follow these steps to configure the HTTPS certificate.

1. Disconnect the temporary connected network cable from your computer.
2. Change your NIC from DHCP to your normal network configuration.
3. Connect the network cable a switch in the Management network.
4. Run `Cisco ASDM-IDM Launcher`.
5. Connect using the ASA management IP address, and the new password that was set during the Startup Wizard.
6. Ignore the certificate warnings.

   ASDM launches.



Cisco ASDM-IDM Launcher v1.7(0)

Cisco ASDM-IDM Launcher

Contacting the device. Please wait...

Device IP Address / Name: 192.166.11.10

Username:

Password: •••••••

□ Remember the username of the specified device on this computer

□ Run in Demo Mode

7. Run Wizards -> ASDM Identity Certificate Wizard.
8. Select Simple Mode.
9. Then select Export Generated Identity Certificate.
10. Save the file as asa.cer.
11. Run Wizards -> ASDM Identity Certificate Wizard.
12. Select ASA FirePOWER Module.
13. Then select Export Generated Identity Certificate.
14. Save the file as sfr.cer.

    After this procedure, do the following:

1. Go to ASDM -> Save ASA Changes.
2. Go to ASDM -> Tools -> System Reload... -> Schedule Reload.
3. Close ASDM.
4. Open Java Control Panel -> Security -> Manage Certificates.
5. Select Certificate type as Secure Site.
6. Import asa.cer.
7. Import sfr.cer.

8. Wait until the EIP Mod status indicator on the Stratix 5950 security appliance is solid green, which takes about 5 minutes.

9. Run Cisco ASDM-IDM Launcher.

   No certificate warning dialogs are expected.

   ASDM opens.

Configure a Test Policy to Block CIP Administrative Traffic

Single Policy Restriction

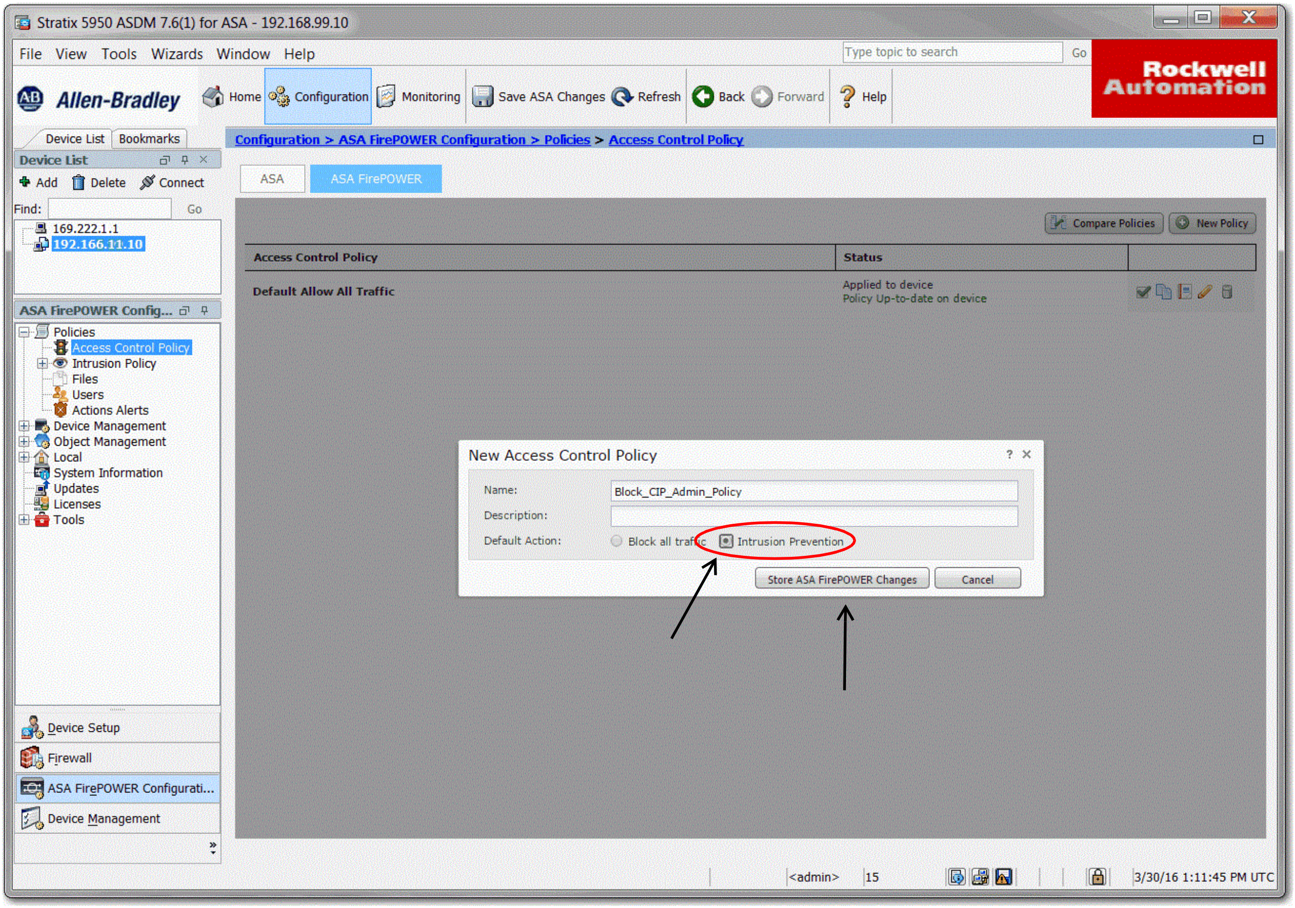
The ability to create policies was deprecated in the Stratix 5950 Version 6.4.0/ ASDM Version 7.12.1. With that release, you only get one policy: Default Allow All. You can modify the default policy, but you cannot create policies.

Configure a Test Policy

Configure a test policy to verify the expected behavior of CIP™ DPI functionality. This test policy verifies that the CIP RA Administrative traffic is blocked from passing through the device.

To configure a test policy to block CIP admin traffic, follow these steps.

1. Go to ASDM > Configuration >ASA FirePOWER Configuration >Policies > Access Control Policy > New Policy
2. Name the policy, for example, Block_CIP_Admin_Policy.
3. Change the Default Action to Intrusion Prevention.



Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy

Access Control Policy	Status
Default Allow All Traffic	Applied to device Policy Up-to-date on device

New Access Control Policy

Name: Block_CIP_Admin_Policy

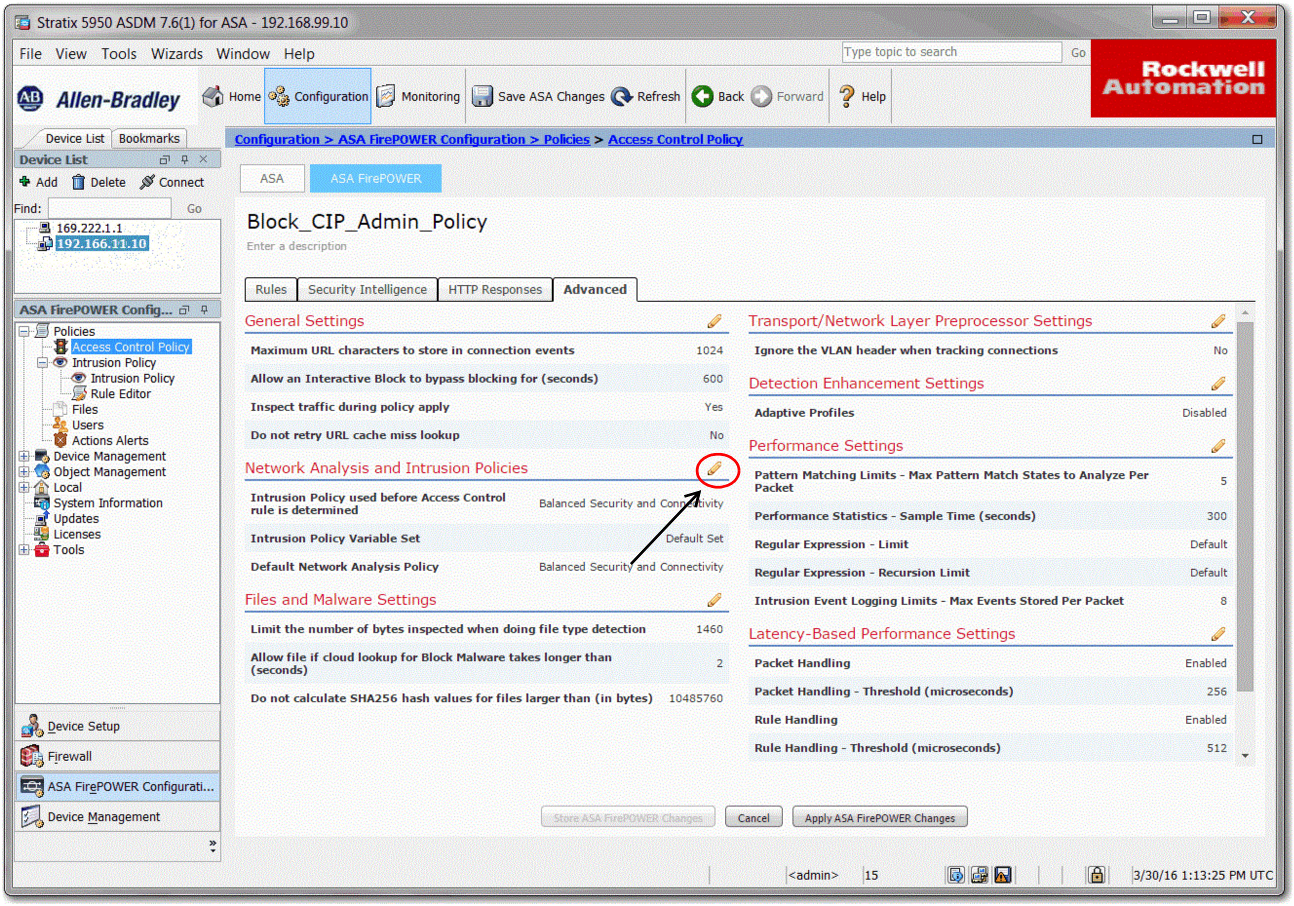
Description:

Default Action: ○ Block all traffic ● Intrusion Prevention

Store ASA FirePOWER Changes | Cancel

4. Click Store ASA FirePOWER Changes.

5. In the policy, select the Advanced tab.
6. Click the Pencil icon next to Network Analysis and Intrusion Policies.



Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy

Block_CIP_Admin_Policy

Enter a description

General Settings	
Maximum URL characters to store in connection events	1024
Allow an Interactive Block to bypass blocking for (seconds)	600
Inspect traffic during policy apply	Yes
Do not retry URL cache miss lookup	No

Network Analysis and Intrusion Policies	
Intrusion Policy used before Access Control rule is determined	Balanced Security and Connectivity
Intrusion Policy Variable Set	Default Set
Default Network Analysis Policy	Balanced Security and Connectivity

Files and Malware Settings	
Limit the number of bytes inspected when doing file type detection	1460
Allow file if cloud lookup for Block Malware takes longer than (seconds)	2
Do not calculate SHA256 hash values for files larger than (in bytes)	10485760

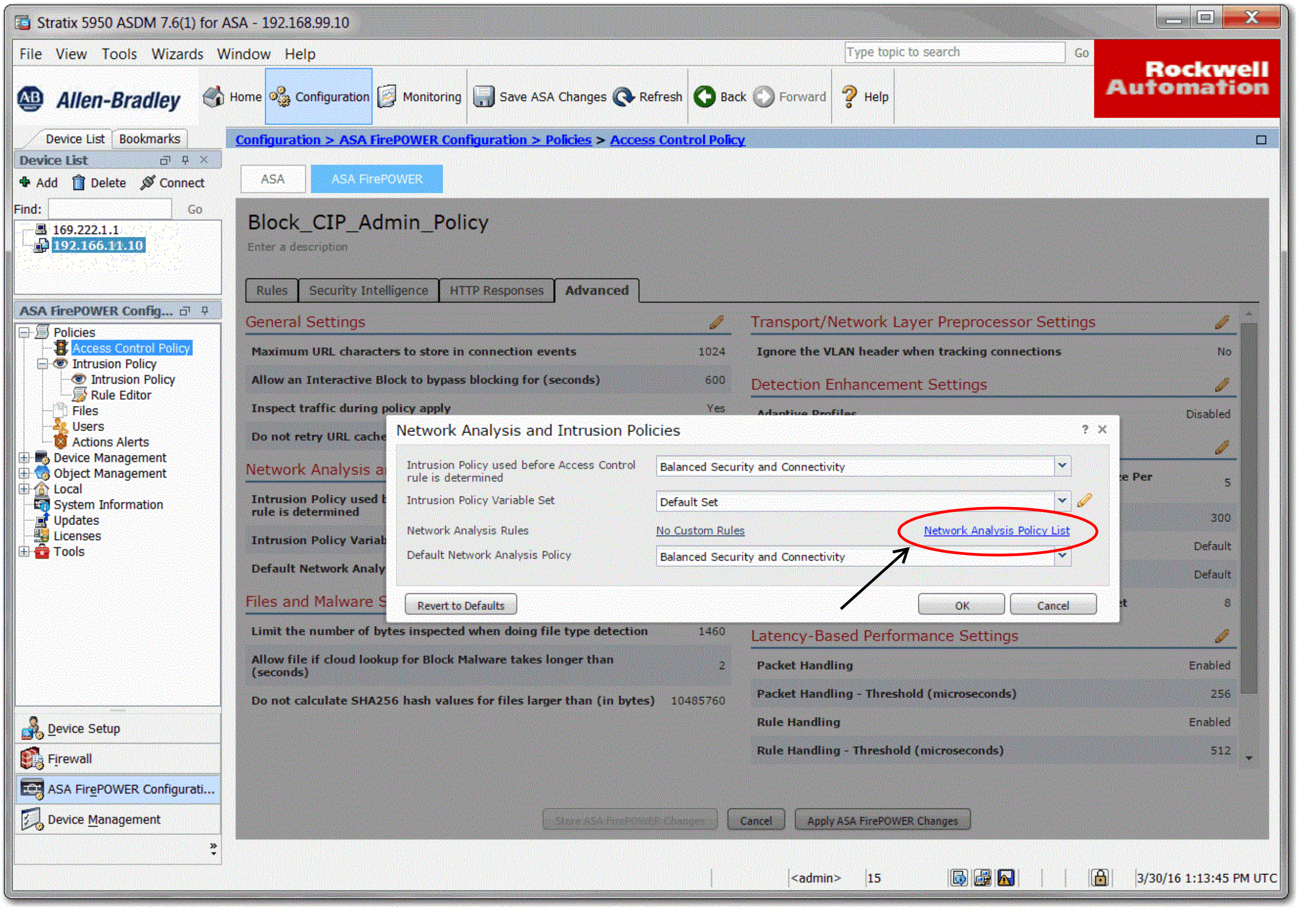
Transport/Network Layer Preprocessor Settings	
Ignore the VLAN header when tracking connections	No

Detection Enhancement Settings	
Adaptive Profiles	Disabled

Performance Settings	
Pattern Matching Limits - Max Pattern Match States to Analyze Per Packet	5
Performance Statistics - Sample Time (seconds)	300
Regular Expression - Limit	Default
Regular Expression - Recursion Limit	Default
Intrusion Event Logging Limits - Max Events Stored Per Packet	8

Latency-Based Performance Settings	
Packet Handling	Enabled
Packet Handling - Threshold (microseconds)	256
Rule Handling	Enabled
Rule Handling - Threshold (microseconds)	512

7. Click the Network Analysis Policy List link.



Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy

Block_CIP_Admin_Policy

Enter a description

General Settings

Maximum URL characters to store in connection events	1024
Allow an Interactive Block to bypass blocking for (seconds)	600
Inspect traffic during policy apply	Yes
Do not retry URL cache	

Network Analysis a

Intrusion Policy used b rule is determined	
Intrusion Policy Variab	
Default Network Analy	

Files and Malware S

Limit the number of bytes inspected when doing file type detection	1460
Allow file if cloud lookup for Block Malware takes longer than (seconds)	2
Do not calculate SHA256 hash values for files larger than (in bytes)	10485760

Transport/Network Layer Preprocessor Settings

Ignore the VLAN header when tracking connections	No

Detection Enhancement Settings

Adaptive Profiles	Disabled
e Per	5
	300
	Default
	Default
t	8

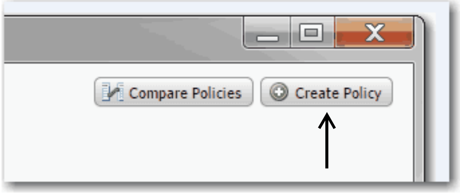
Latency-Based Performance Settings

Packet Handling	Enabled
Packet Handling - Threshold (microseconds)	256
Rule Handling	Enabled
Rule Handling - Threshold (microseconds)	512

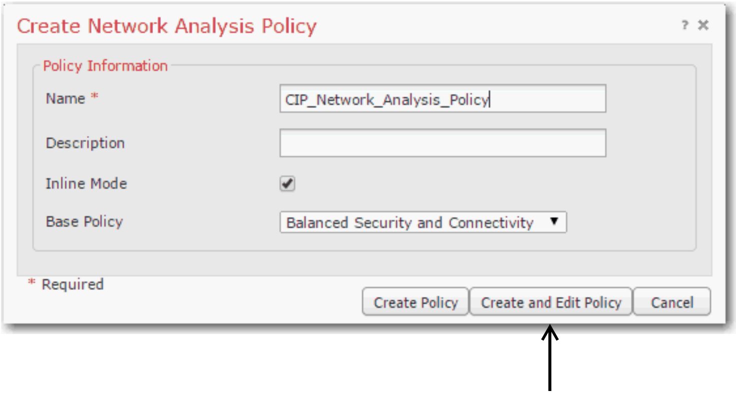
Network Analysis and Intrusion Policies

Intrusion Policy used before Access Control rule is determined	Balanced Security and Connectivity
Intrusion Policy Variable Set	Default Set
Network Analysis Rules	No Custom Rules Network Analysis Policy List
Default Network Analysis Policy	Balanced Security and Connectivity

8. Click Create Policy.



9. Name the policy and click Create and Edit Policy.



Create Network Analysis Policy

Policy Information

Name *: CIP_Network_Analysis_Policy

Description:

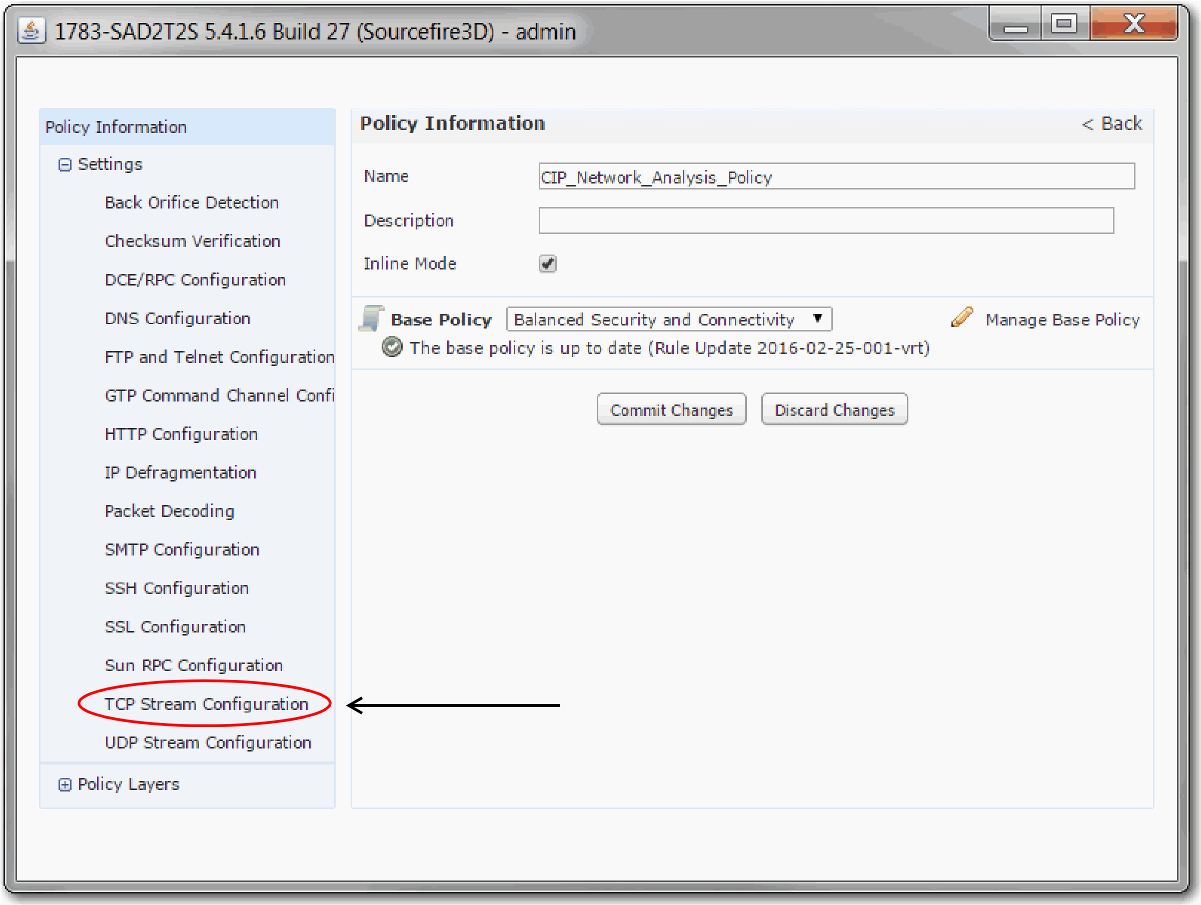
Inline Mode: ☑

Base Policy: Balanced Security and Connectivity

* Required

10. Wait while the policy is being created.

11. Select Policy Information -> Settings -> TCP Stream Configuration.



1783-SAD2T2S 5.4.1.6 Build 27 (Sourcefire3D) - admin

Policy Information

< Back

Name: CIP_Network_Analysis_Policy

Description:

Inline Mode: ☑

Base Policy: Balanced Security and Connectivity

Manage Base Policy

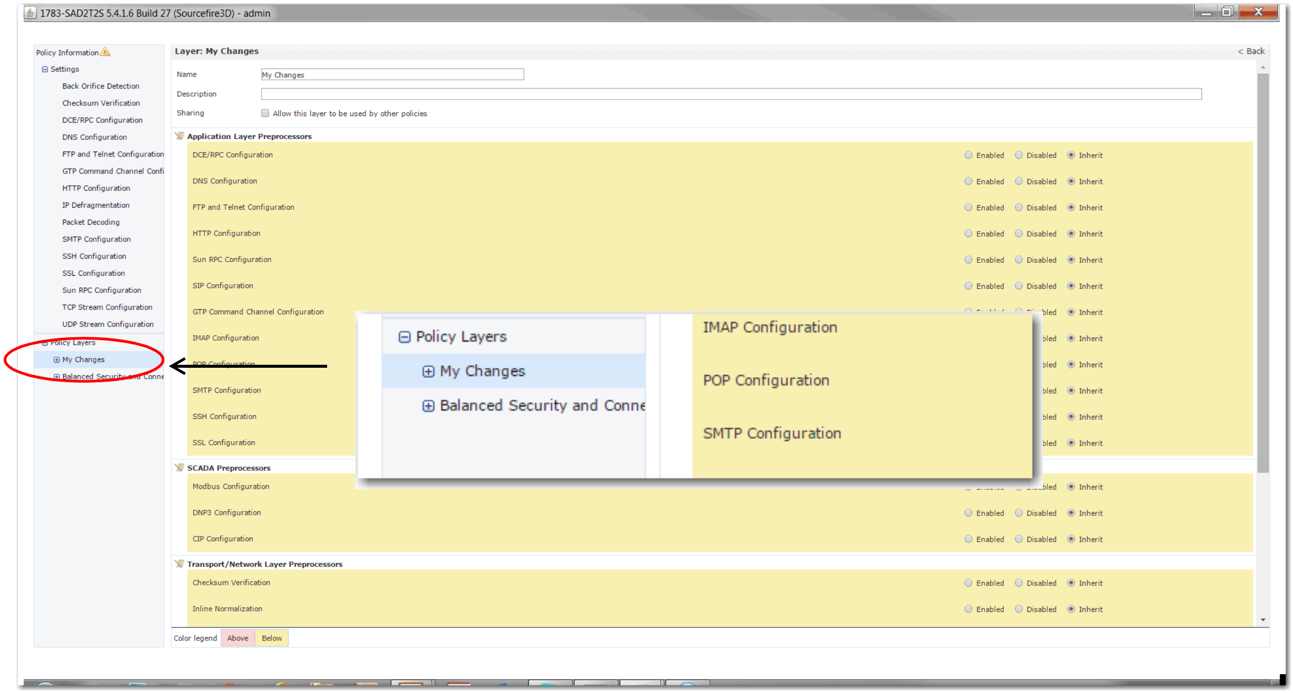
The base policy is up to date (Rule Update 2016-02-25-001-vrt)

12. Click TCP Stream Configuration

13. In the Perform Stream Reassembly on Both Ports field, scroll to the end of the line, and add 44818 to the list.

    Be sure to add the extra comma before 44818.

14. Select Policy Information -> Policy Layers -> My Changes



Layer: My Changes

Name: My Changes

Description:

Sharing: □ Allow this layer to be used by other policies

Application Layer Preprocessors

DCE/RPC Configuration	○ Enabled	○ Disabled	● Inherit
DNS Configuration	○ Enabled	○ Disabled	● Inherit
FTP and Telnet Configuration	○ Enabled	○ Disabled	● Inherit
HTTP Configuration	○ Enabled	○ Disabled	● Inherit
Sun RPC Configuration	○ Enabled	○ Disabled	● Inherit
SIP Configuration	○ Enabled	○ Disabled	● Inherit
GTP Command Channel Configuration	○ Enabled	○ Disabled	● Inherit
IMAP Configuration		bled	● Inherit
POP Configuration		bled	● Inherit
SMTP Configuration		bled	● Inherit
SSH Configuration		bled	● Inherit
SSL Configuration		bled	● Inherit

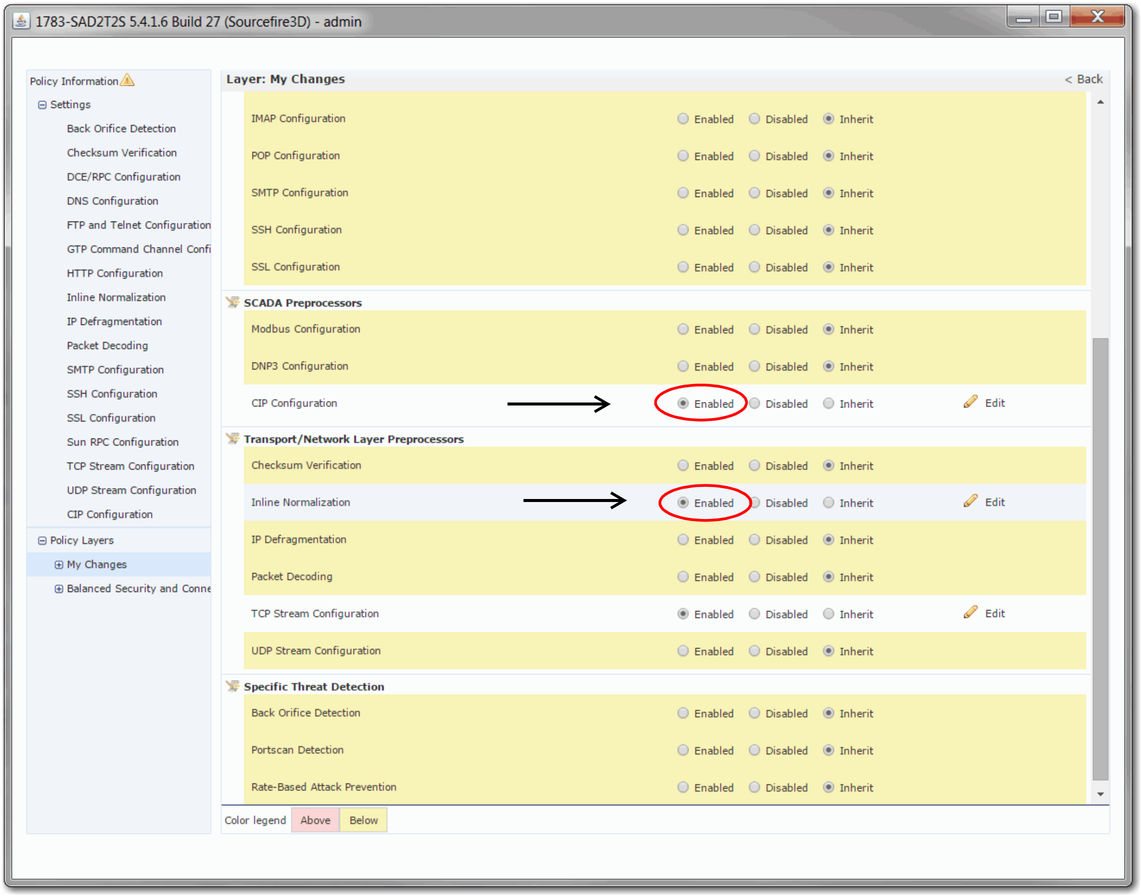
SCADA Preprocessors

Modbus Configuration	○ Enabled	○ Disabled	● Inherit
DNP3 Configuration	○ Enabled	○ Disabled	● Inherit
CIP Configuration	○ Enabled	○ Disabled	● Inherit

Transport/Network Layer Preprocessors

Checksum Verification	○ Enabled	○ Disabled	● Inherit
Inline Normalization	○ Enabled	○ Disabled	● Inherit

15. At SCADA Preprocessors, change CIP Configuration to Enabled.

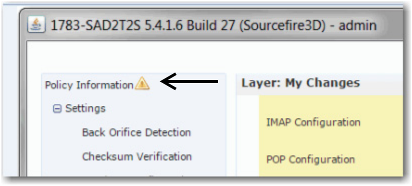


Layer: My Changes

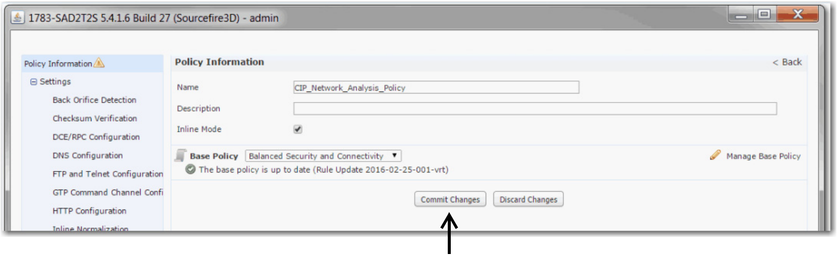
IMAP Configuration	○ Enabled	○ Disabled	● Inherit	
POP Configuration	○ Enabled	○ Disabled	● Inherit	
SMTP Configuration	○ Enabled	○ Disabled	● Inherit	
SSH Configuration	○ Enabled	○ Disabled	● Inherit	
SSL Configuration	○ Enabled	○ Disabled	● Inherit	
SCADA Preprocessors				
Modbus Configuration	○ Enabled	○ Disabled	● Inherit	
DNP3 Configuration	○ Enabled	○ Disabled	● Inherit	
CIP Configuration	● Enabled	○ Disabled	○ Inherit	Edit
Transport/Network Layer Preprocessors				
Checksum Verification	○ Enabled	○ Disabled	● Inherit	
Inline Normalization	● Enabled	○ Disabled	○ Inherit	Edit
IP Defragmentation	○ Enabled	○ Disabled	● Inherit	
Packet Decoding	○ Enabled	○ Disabled	● Inherit	
TCP Stream Configuration	● Enabled	○ Disabled	○ Inherit	Edit
UDP Stream Configuration	○ Enabled	○ Disabled	● Inherit	
Specific Threat Detection				
Back Orifice Detection	○ Enabled	○ Disabled	● Inherit	
Portscan Detection	○ Enabled	○ Disabled	● Inherit	
Rate-Based Attack Prevention	○ Enabled	○ Disabled	● Inherit	

16. At Transport/Network Layer Preprocessors, change Inline Normalization to Enabled.

17. Click Policy Information.



18. Click Commit Changes.



Policy Information

Name: CIP_Network_Analysis_Policy

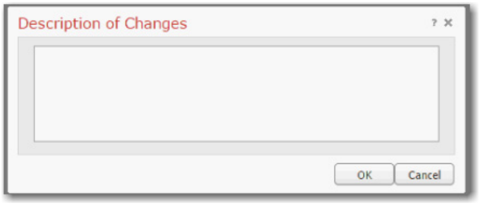
Description:

Inline Mode: ☑

Base Policy: Balanced Security and Connectivity

The base policy is up to date (Rule Update 2016-02-25-001-vrt)

19. Enter a description.

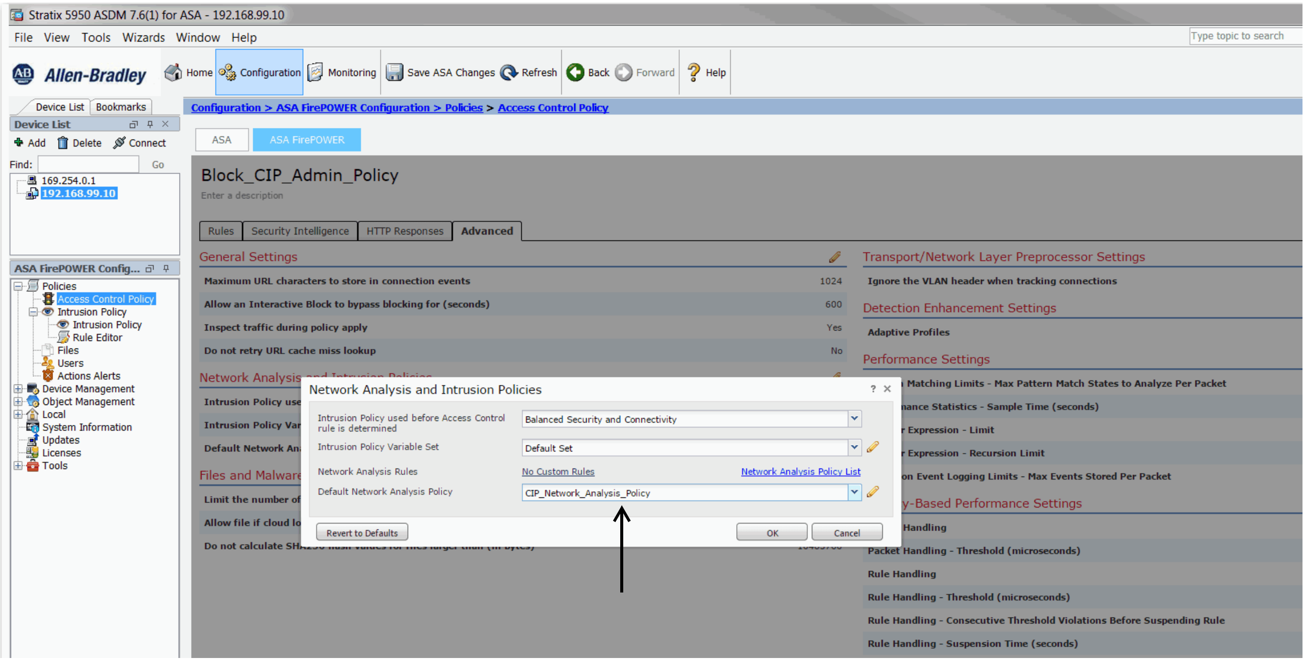


Description of Changes

20. Click OK.

21. In the Network Analysis and Intrusion Policies dialog box, change the Default Network Analysis Policy to the Network Analysis Policy that you created.

IMPORTANT **EVERY** time that you create a new Access Control Policy, this step **MUST** be done.



Block_CIP_Admin_Policy

Enter a description

General Settings

Maximum URL characters to store in connection events	1024
Allow an Interactive Block to bypass blocking for (seconds)	600
Inspect traffic during policy apply	Yes
Do not retry URL cache miss lookup	No

Network Analysis and Intrusion Policies

Intrusion Policy use

Intrusion Policy Var

Default Network An

Files and Malware

Limit the number of

Allow file if cloud lo

Do not calculate SHA256 hash values for files larger than (in bytes)

Transport/Network Layer Preprocessor Settings

Ignore the VLAN header when tracking connections

Detection Enhancement Settings

Adaptive Profiles

Performance Settings

Matching Limits - Max Pattern Match States to Analyze Per Packet

nance Statistics - Sample Time (seconds)

r Expression - Limit

r Expression - Recursion Limit

on Event Logging Limits - Max Events Stored Per Packet

y-Based Performance Settings

Handling

Packet Handling - Threshold (microseconds)

Rule Handling

Rule Handling - Threshold (microseconds)

Rule Handling - Consecutive Threshold Violations Before Suspending Rule

Rule Handling - Suspension Time (seconds)

Network Analysis and Intrusion Policies

Intrusion Policy used before Access Control rule is determined	Balanced Security and Connectivity
Intrusion Policy Variable Set	Default Set
Network Analysis Rules	No Custom Rules Network Analysis Policy List
Default Network Analysis Policy	CIP_Network_Analysis_Policy

22. Close the popup window that shows the new Network Analysis Policy that you created.

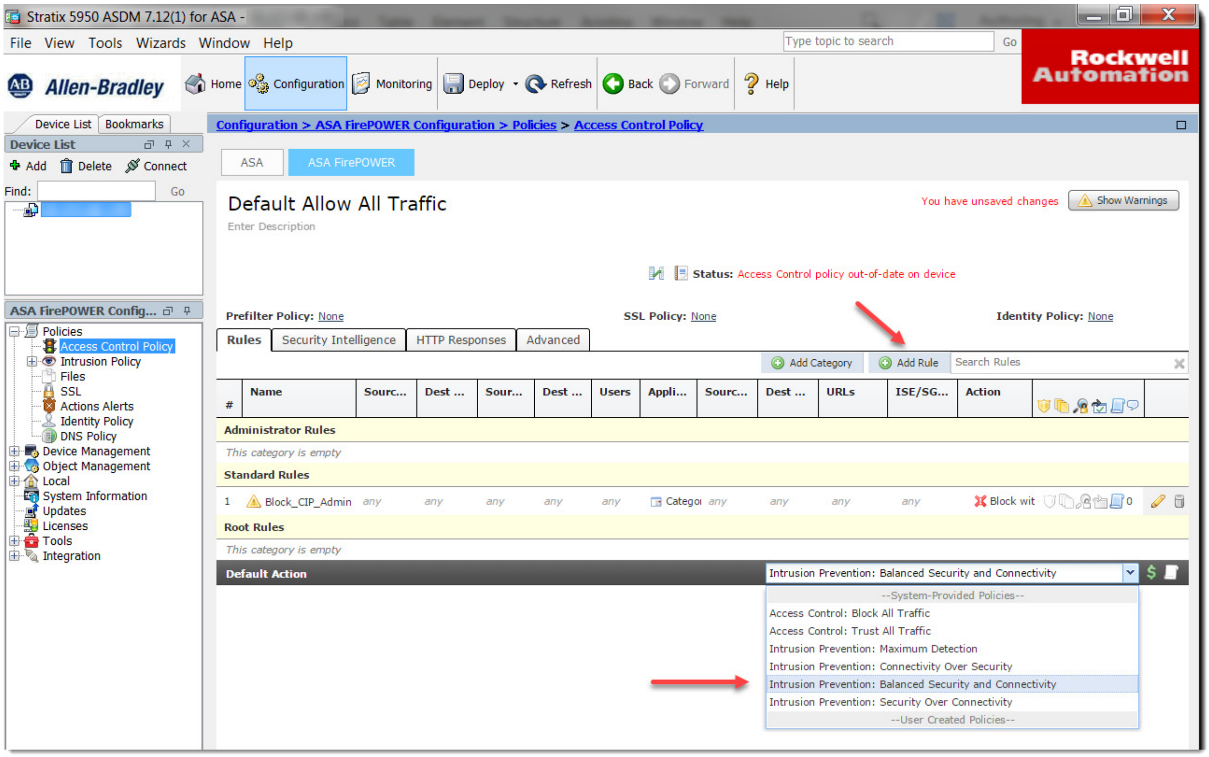
23. Click OK.

TIP Create the CIP Network Analysis Policy only once. If you create an Access Control Policy, you can use the existing CIP Network Analysis Policy.

Add a Rule

To add a rule, follow these steps.

1. From the Default Action pull-down menu, choose an Intrusion Prevention option. We recommend Balanced Security and Connectivity.
2. On the Rules tab, click Add Rule.



Stratix 5950 ASDM 7.12(1) for ASA -

Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy

Default Allow All Traffic

Enter Description

You have unsaved changes

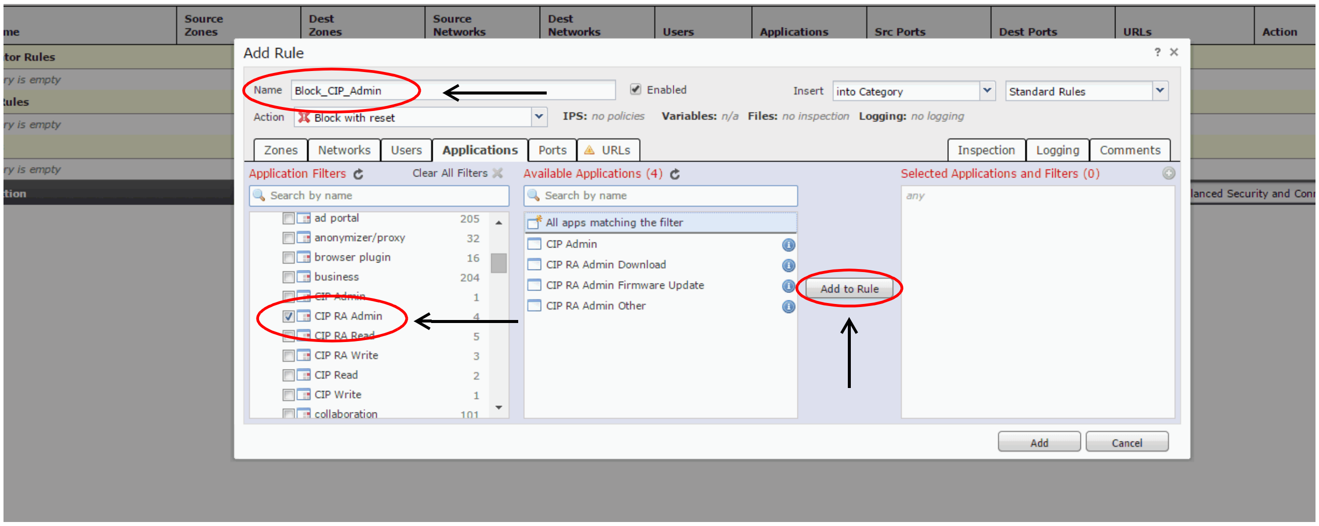
Status: Access Control policy out-of-date on device

Prefilter Policy: None SSL Policy: None Identity Policy: None

#	Name	Sourc...	Dest ...	Sour...	Dest ...	Users	Appli...	Sourc...	Dest ...	URLs	ISE/SG...	Action
Administrator Rules												
This category is empty												
Standard Rules												
1	Block_CIP_Admin	any	any	any	any	any	Categoı	any	any	any	any	Block wit
Root Rules												
This category is empty												

Default Action: Intrusion Prevention: Balanced Security and Connectivity

3. Set rule Name to Block_CIP_Admin.
4. From the Action pull-down, choose Block with reset.
5. On the Applications tab, under Application Filters>Categories, check CIP RA Admin, then click Add to Rule.



Add Rule

Name: Block_CIP_Admin

☑ Enabled

Insert: into Category — Standard Rules

Action: Block with reset

IPS: *no policies* Variables: *n/a* Files: *no inspection* Logging: *no logging*

Application Filters

□ ad portal	205
□ anonymizer/proxy	32
□ browser plugin	16
□ business	204
□ CIP Admin	1
☑ CIP RA Admin	4
□ CIP RA Read	5
□ CIP RA Write	3
□ CIP Read	2
□ CIP Write	1
□ collaboration	101

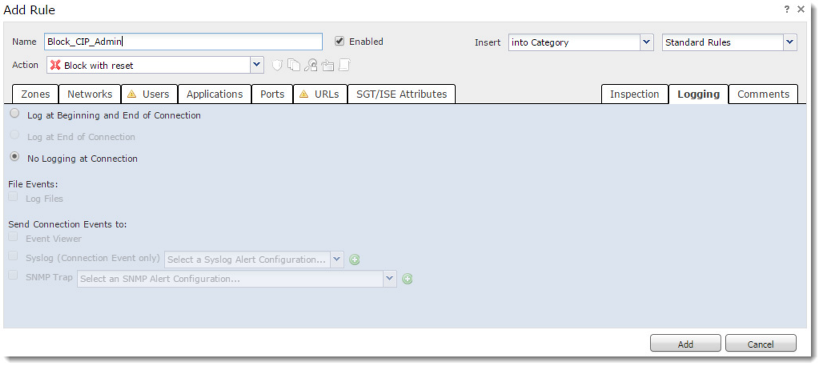
Available Applications (4)

- All apps matching the filter
- CIP Admin
- CIP RA Admin Download
- CIP RA Admin Firmware Update
- CIP RA Admin Other

Selected Applications and Filters (0)

any

6. Click the Logging tab.



Add Rule

Name: Block_CIP_Admin ☑ Enabled

Insert: into Category | Standard Rules

Action: Block with reset

○ Log at Beginning and End of Connection

○ Log at End of Connection

● No Logging at Connection

File Events:

□ Log Files

Send Connection Events to:

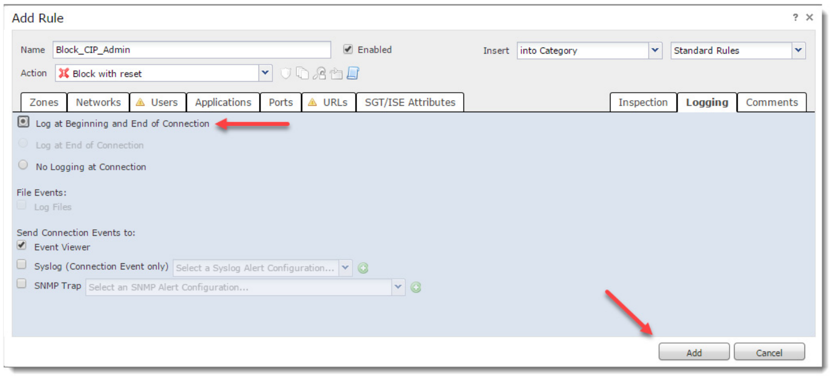
□ Event Viewer

□ Syslog (Connection Event only) Select a Syslog Alert Configuration...

□ SNMP Trap Select an SNMP Alert Configuration...

7. Click Log at Beginning and End of Connection.

8. Click Add.



Add Rule

Name: Block_CIP_Admin ☑ Enabled

Insert: into Category | Standard Rules

Action: Block with reset

● Log at Beginning and End of Connection

○ Log at End of Connection

○ No Logging at Connection

File Events:

□ Log Files

Send Connection Events to:

☑ Event Viewer

□ Syslog (Connection Event only) Select a Syslog Alert Configuration...

□ SNMP Trap Select an SNMP Alert Configuration...

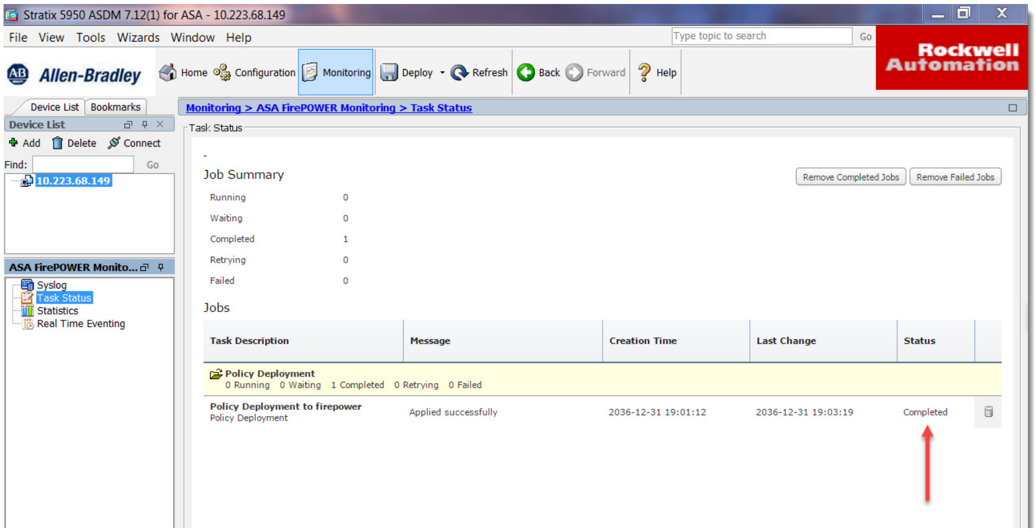
9. Click Store ASA FirePOWER Changes.

10. Click Apply All.

11. Click OK.

12. Go to ASDM > Monitoring > ASA FirePOWER Monitoring > Task Status.
13. Wait until the Apply Block_CIP_Admin_Policy task finishes, which takes about 2 minutes.

TIP The device ships in a Monitor Mode configuration. This configuration enables the device to show you what it would have blocked, if it was in a full blocking configuration, for test purposes. This test configuration only shows the first traffic that it would have blocked per TCP connection.



Job Summary

Running	0
Waiting	0
Completed	1
Retrying	0
Failed	0

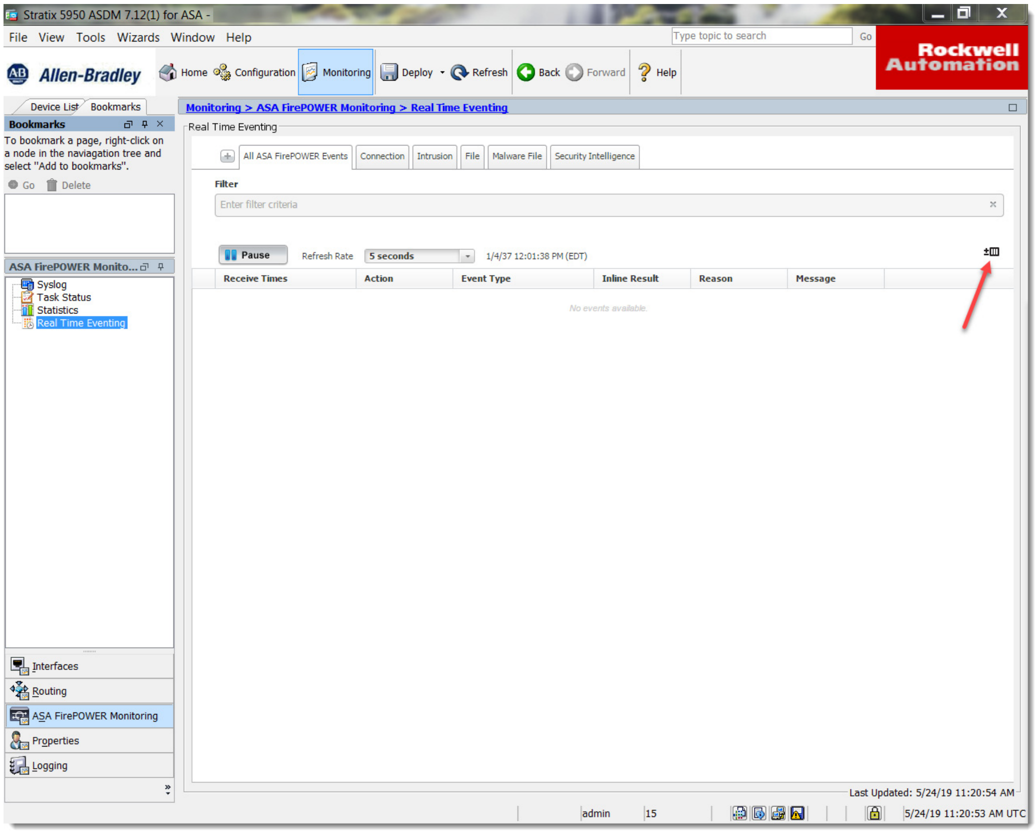
Jobs

Task Description	Message	Creation Time	Last Change	Status
Policy Deployment 0 Running 0 Waiting 1 Completed 0 Retrying 0 Failed				
Policy Deployment to firepower Policy Deployment	Applied successfully	2036-12-31 19:01:12	2036-12-31 19:03:19	Completed

Update Real Time Eventing View

Follow these steps to update the Real Time Eventing view.

1. Go to ASDM > Monitoring > Real Time Eventing > All ASA FirePOWER Events.
2. Click Add/Remove columns.



Bookmarks

To bookmark a page, right-click on a node in the naviagation tree and select "Add to bookmarks".

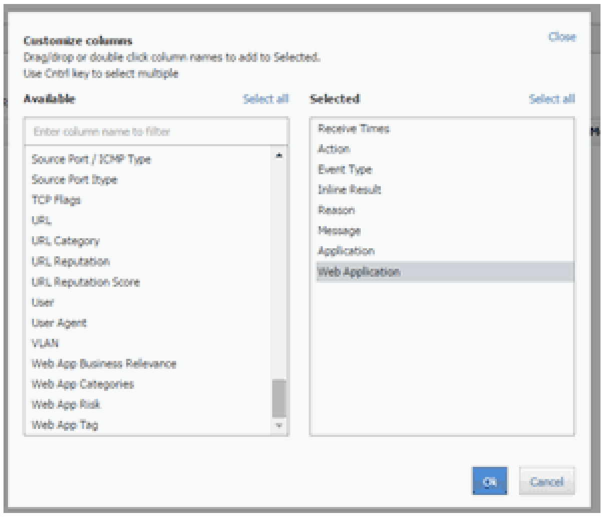
Refresh Rate: 5 seconds 1/4/37 12:01:38 PM (EDT)

No events available.

Last Updated: 5/24/19 11:20:54 AM

5/24/19 11:20:53 AM UTC

3. Drag Application, then Web Application from the left column to the right column.
4. Click OK.



Customize columns

Drag/drop or double click column names to add to Selected.
Use Cntrl key to select multiple

Available

Source Port / ICMP Type
Source Port Itype
TCP Flags
URL
URL Category
URL Reputation
URL Reputation Score
User
User Agent
VLAN
Web App Business Relevance
Web App Categories
Web App Risk
Web App Tag

Selected

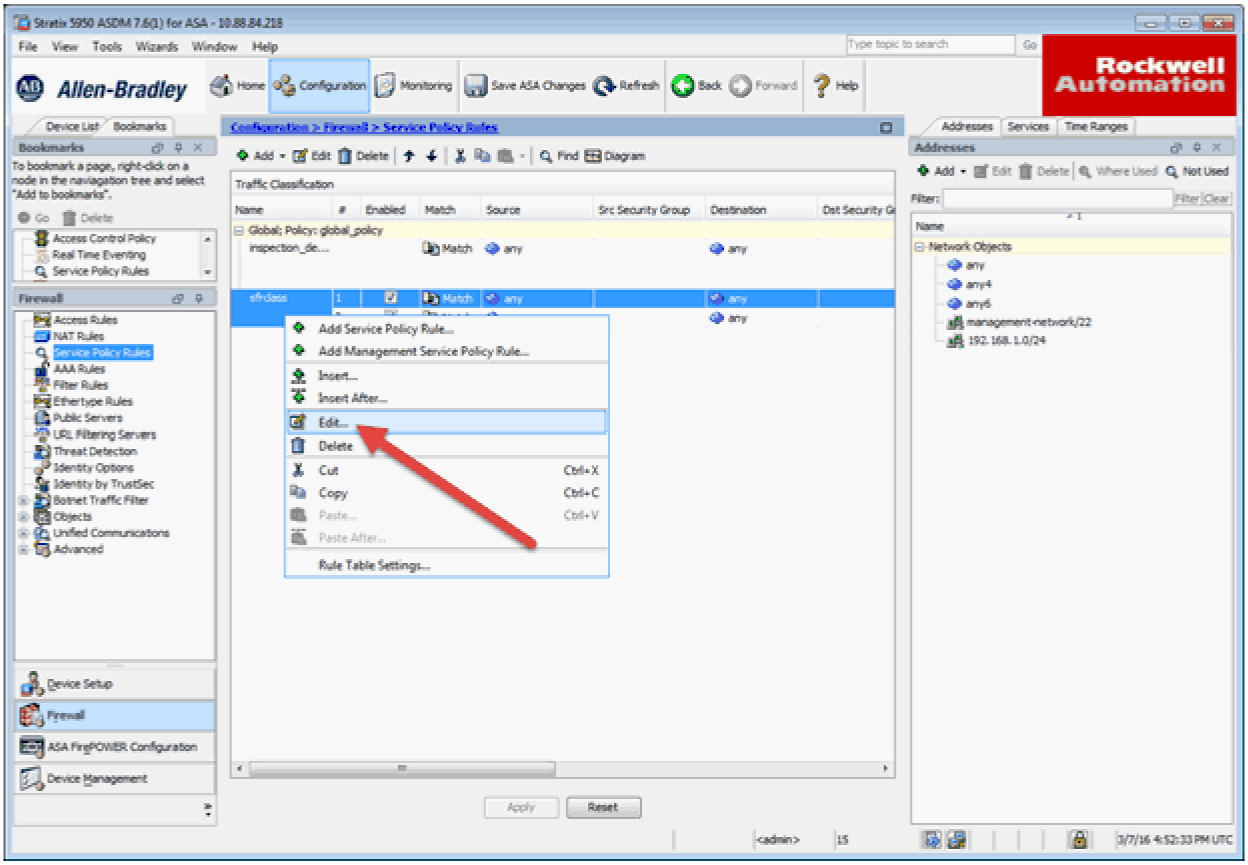
Receive Times
Action
Event Type
Inline Result
Reason
Message
Application
Web Application

Change the Device from Monitor Mode to a Full Blocking Configuration (Inline Mode Only)

The security appliance is configured from the factory in Monitor Mode configuration. This configuration enables the appliance to show you what it would have blocked if it was in a full blocking configuration, for test purposes.

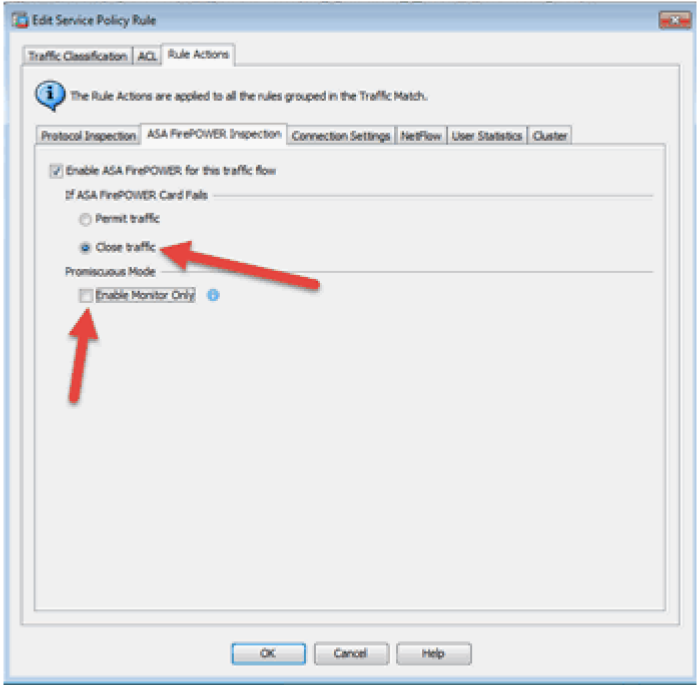
For testing the correct functionality of the CIP DPI configuration, it is easier to switch out of Monitor Mode into a full blocking configuration.

1. Go to ASDM>Configuration>Firewall>Service Policy Rules.
2. Edit the sfrclass rule.



3. On the Edit Service Policy Rule page, go to:
   Rule Actions>ASA FirePOWER Inspection.

4. Change the options to Close traffic and clear Enable Monitor Only.



The Rule Actions are applied to all the rules grouped in the Traffic Match.

☑ Enable ASA FirePOWER for this traffic flow

If ASA FirePOWER Card Fails

○ Permit traffic

● Close traffic

Promiscuous Mode

□ Enable Monitor Only

5. Click OK on the Edit Service Policy Rule.

6. Go to ASDM>Save ASA Changes.

7. Click Apply Changes.

8. Physically connect the 5950 device inline by connecting the network cables to port 1 and port 2 of the device.

   A test configuration could be:

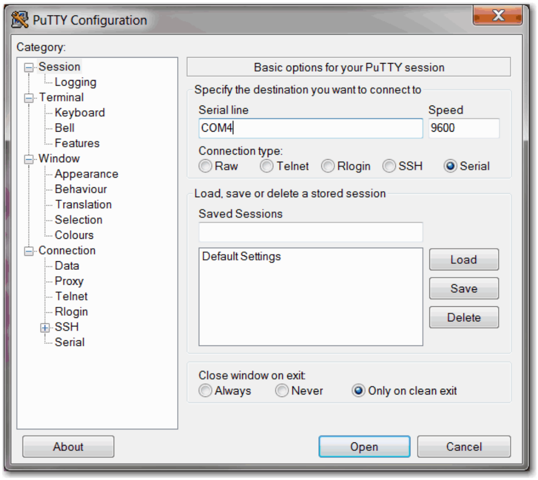
   a. PC>Network Cable>Stratix 5950 Port 1

   b. Stratix 5950 Port 2>Network Cable>1756-EN2TR

Configure SPAN Port Monitoring Settings

This section only applies to SPAN Port mode configuration only.

1. Run PuTTY and connect to the serial port of the device.



Specify the destination you want to connect to

Serial line: COM4 Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit

2. Click Open to start a command-line session.
3. At command line, press Enter.
4. Type: `stratix5950> enable`
5. Press Enter.
6. Enter the ASA password that was set in the Startup Wizard and press Enter.
7. `#configure terminal`
8. `interface BVI1`
9. `no ip address`
10. `interface GigabitEthernet1/1`
11. `no nameif`
12. `traffic-forward sfr monitor-only`
13. `no shutdown`
14. `no bridge-group 1`

> **TIP** This procedure is from Cisco, for more information go to http://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/firewall/asa-96-firewall-config/access-sfr.html

> **TIP** You can ignore any warnings about forwarded traffic being for demonstration purposes only, which is a supported production mode.

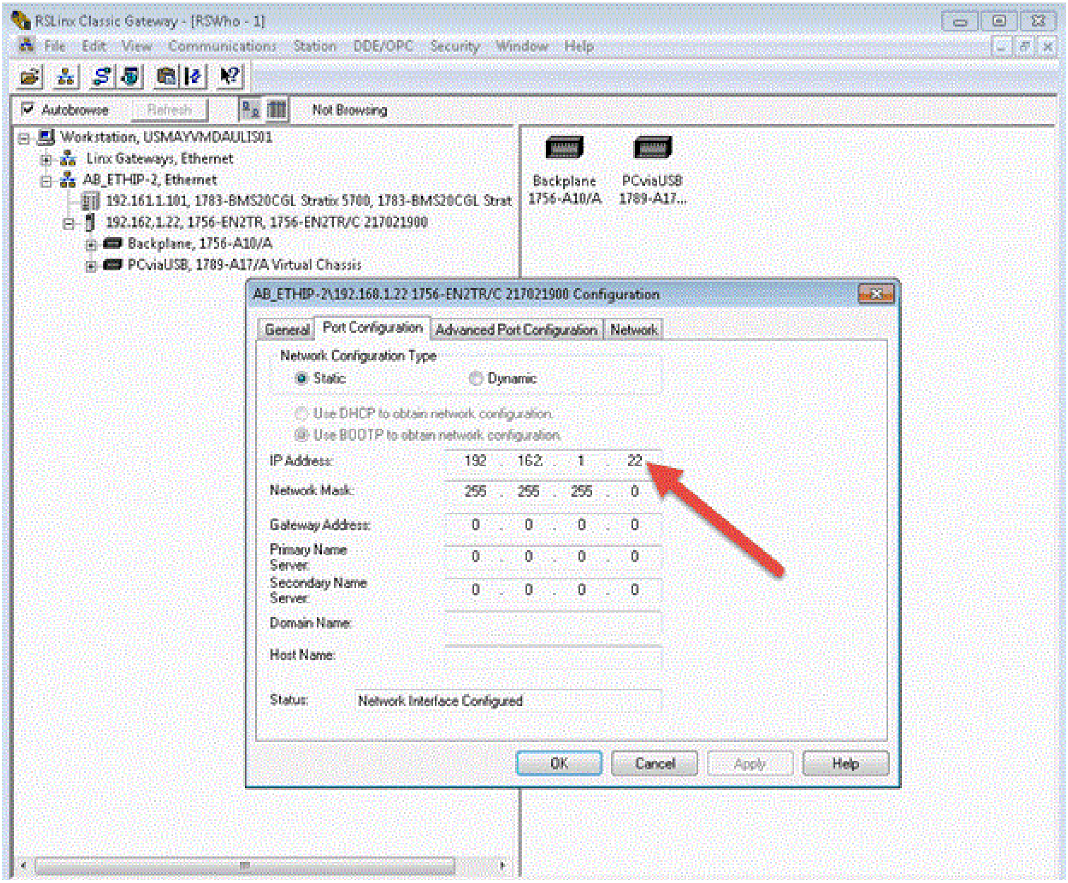
15. `write`
16. Physically connect port 1 of the device to another switch that has Port Mirroring (SPAN port) enabled for that port.

Change the IP Address of the Communication Module

Follow these steps to change the IP address on the 1756-ENT2R by using RSLinx® software.

1. Use RSLinx® Classic from your computer to attempt to change the IP address on the 1756-ENT2R.

   An IP address change via CIP is categorized as CIP Admin.


RSLinx Classic Gateway - [RSWho - 1]
File Edit View Communications Station DDE/OPC Security Window Help
Refresh
OK
Cancel
Apply
Help

☑ Autobrowse

Not Browsing

Workstation, USMAYVMDAULIS01
Linx Gateways, Ethernet
AB_ETHIP-2, Ethernet
192.161.1.101, 1783-BMS20CGL Stratix 5700, 1783-BMS20CGL Strat
192.162.1.22, 1756-EN2TR, 1756-EN2TR/C 217021900
Backplane, 1756-A10/A
PCviaUSB, 1789-A17/A Virtual Chassis

Backplane 1756-A10/A
PCviaUSB 1789-A17...

AB_ETHIP-2\192.168.1.22 1756-EN2TR/C 217021900 Configuration

General | Port Configuration | Advanced Port Configuration | Network

Network Configuration Type
● Static ○ Dynamic

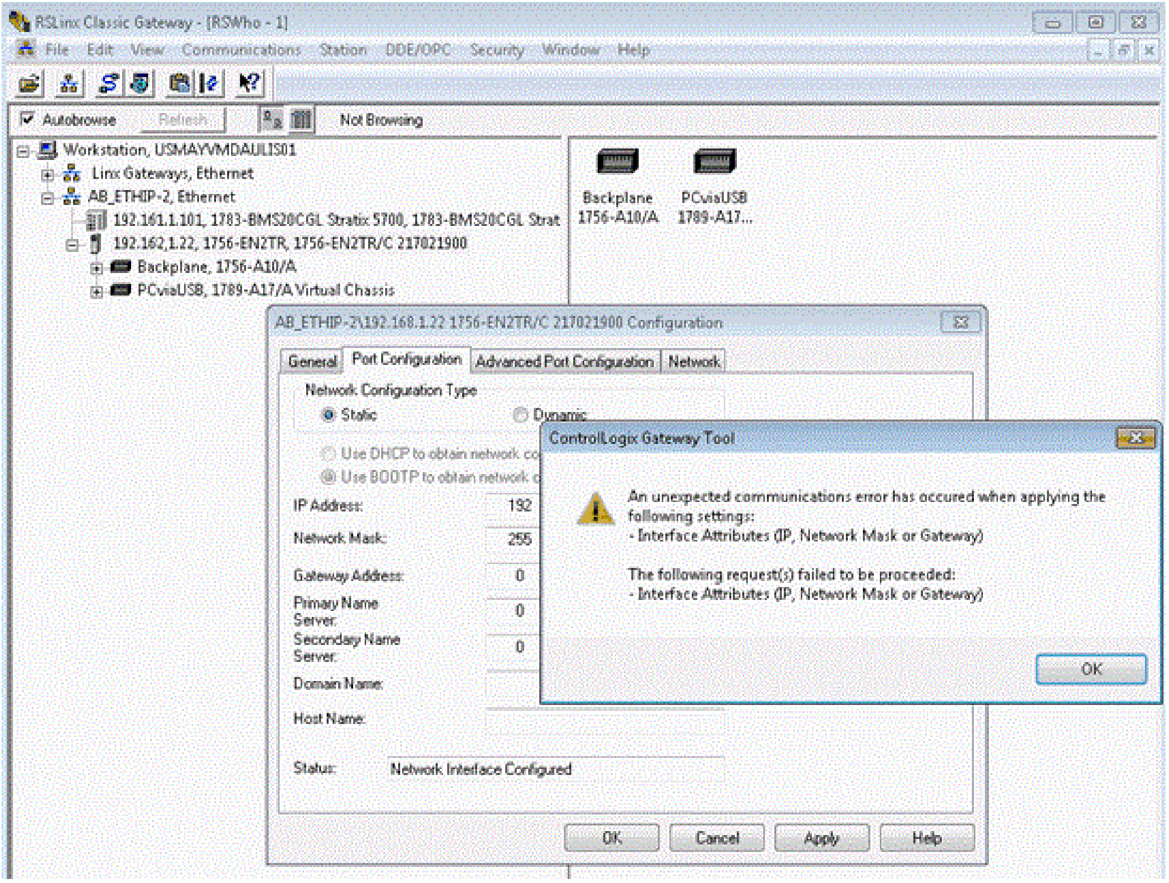
○ Use DHCP to obtain network configuration.
○ Use BOOTP to obtain network configuration.

IP Address: 192 . 162 . 1 . 22
Network Mask: 255 . 255 . 255 . 0
Gateway Address: 0 . 0 . 0 . 0
Primary Name Server: 0 . 0 . 0 . 0
Secondary Name Server: 0 . 0 . 0 . 0
Domain Name:
Host Name:

Status: Network Interface Configured

   RSLinx can report an error because the command did not succeed (Inline mode only).

2. Open up the 1756-EN2TR Module Configuration dialog again to confirm that the new IP address that you set was NOT applied (Inline mode only).



Workstation, USMAYVMDAULIS01
Linx Gateways, Ethernet
AB_ETHIP-2, Ethernet
192.161.1.101, 1783-BMS20CGL Stratix 5700, 1783-BMS20CGL Strat
192.162,1.22, 1756-EN2TR, 1756-EN2TR/C 217021900
Backplane, 1756-A10/A
PCviaUSB, 1789-A17/A Virtual Chassis

AB_ETHIP-2\192.168.1.22 1756-EN2TR/C 217021900 Configuration

Network Configuration Type

● Static ○ Dynamic

○ Use DHCP to obtain network co

● Use BOOTP to obtain network c

IP Address: 192

Network Mask: 255

Gateway Address: 0

Primary Name Server: 0

Secondary Name Server: 0

Domain Name:

Host Name:

Status: Network Interface Configured

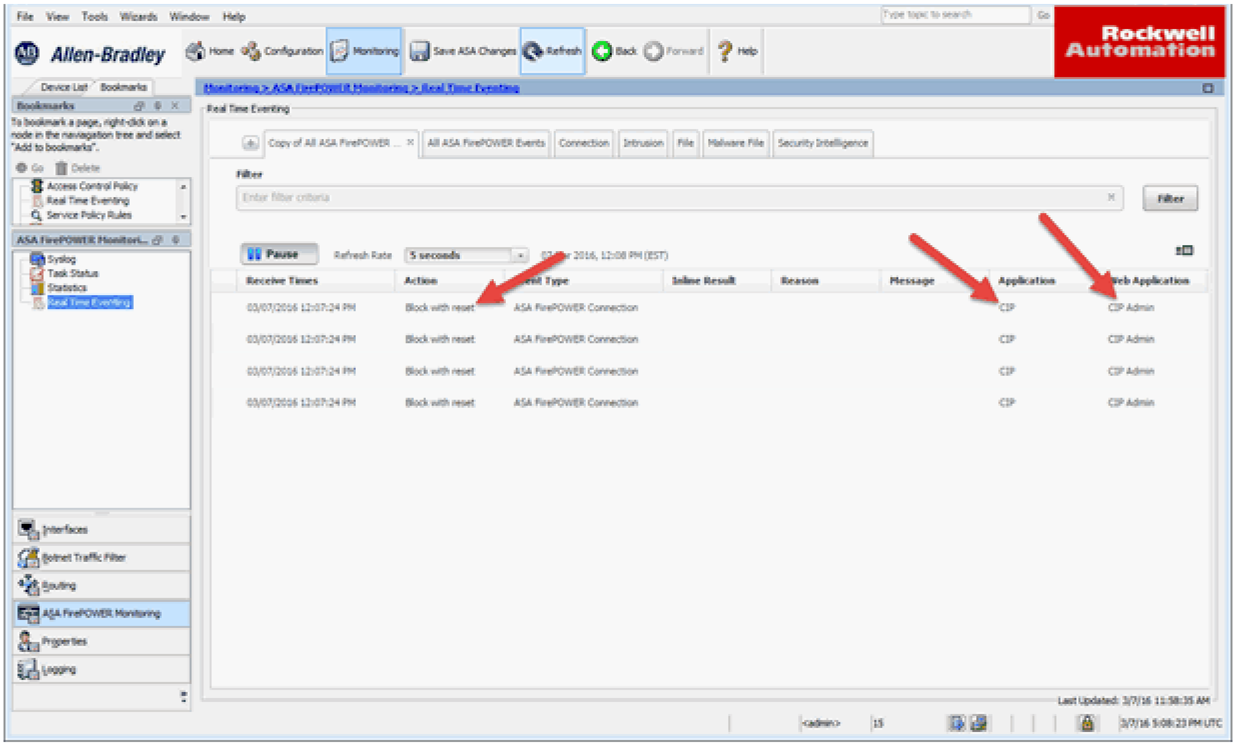
ControlLogix Gateway Tool

An unexpected communications error has occured when applying the following settings:
- Interface Attributes (IP, Network Mask or Gateway)

The following request(s) failed to be proceeded:
- Interface Attributes (IP, Network Mask or Gateway)

3. Go to ASDM>Monitoring>ASA FirePOWER Monitoring> Real Time Eventing.

4. Confirm that a log entry was added.



Receive Times	Action	...ent Type	Inline Result	Reason	Message	Application	...eb Application
03/07/2016 12:07:24 PM	Block with reset	ASA FirePOWER Connection				CIP	CIP Admin
03/07/2016 12:07:24 PM	Block with reset	ASA FirePOWER Connection				CIP	CIP Admin
03/07/2016 12:07:24 PM	Block with reset	ASA FirePOWER Connection				CIP	CIP Admin
03/07/2016 12:07:24 PM	Block with reset	ASA FirePOWER Connection				CIP	CIP Admin

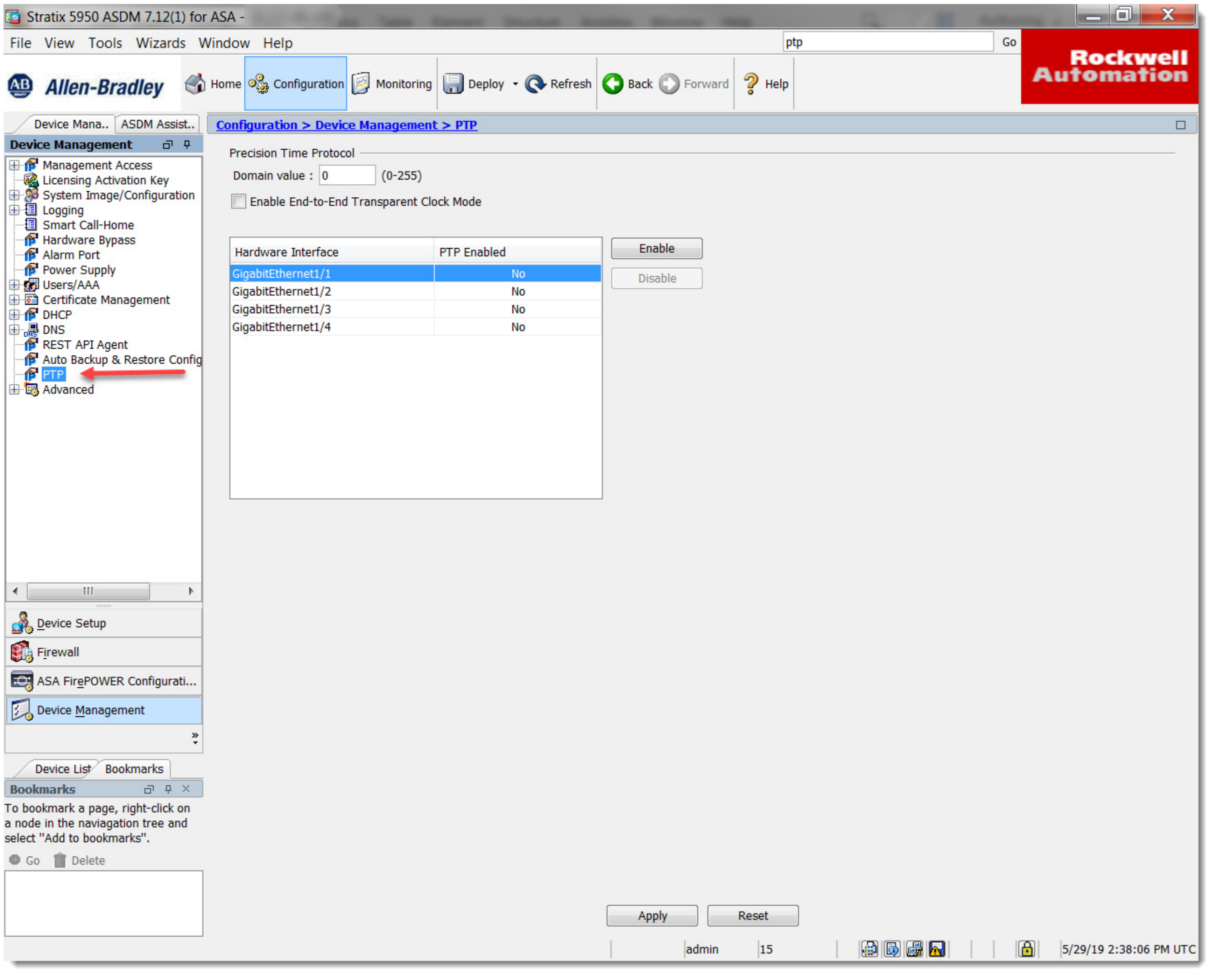
The Action is logged as Block with reset. The Application is logged as CIP and the Web Application is logged as CIP Admin.

Configure Precision Time Protocol (PTP)

PTP synchronizes the clocks of various devices in a packet-based network.

To enable PTP, follow these steps.

1. From ASDM Home, click Configuration.
2. Under Device Management, click PTP. Precision Time Protocol is displayed.
3. Type the Domain value.
4. Check Enable End-to-End Transparent Clock Mode.
5. Select a Hardware Interface, and then click Enable.
6. Click Apply.



Configuration > Device Management > PTP

Precision Time Protocol

Domain value : 0 (0-255)

□ Enable End-to-End Transparent Clock Mode

Hardware Interface	PTP Enabled
GigabitEthernet1/1	No
GigabitEthernet1/2	No
GigabitEthernet1/3	No
GigabitEthernet1/4	No

Table 5 - Precision Time Protocol (PTP)

Field	Description
Domain value	Type the domain number for all ports on the device, 0…255. Zero is the default value.
Enable End-to-End Transparent Clock Mode	Check to enable end-to-end transparent mode on all PTP-enabled interfaces. A transparent clock compensates for its delays by measuring the residence times and updating the `correctionField` in the PTP packet.

Notes:

Chapter 4

Monitor the Security Appliance

This chapter contains information that is required to monitor the Stratix® 5950 security appliance.

Status Indicators

This table describes the Stratix 5950 security appliance status indicators.

Table 6 - Stratix 5950 Security Appliance Status Indicators

Indicator	Status	Description
EIP ModStatus	The System status indicator shows the power status of the appliance.	
	Off	Power to the appliance is off or is not properly connected.
	Solid green	The appliance is operating properly. When ASA and FirePOWER® Software boots up, the system status indicator turns solid green.
	Flashing green	Standby. The appliance is going through the startup (boot phase) sequence. If you have not configured the security appliance, the module status indicator is flashing green. This status indicator is in this state until ASA and FirePOWER successfully boots up.
	Solid red	The appliance is not working properly. If the security appliance has detected a nonrecoverable major fault, the module status indicator is steady red. Major faults 1 = Secure boot failure of BIOS 2 = ROMMON self-check failure
	Flashing green/red	Self-test During the security appliance power-up test, the module status indicator is flashes green/red. After power-up, the status indicator is in this state until secure boot check is completed.
Ports and Management		
	Off	No Link (default)
	Solid green	Port link with no activity
	Flashing green	The appliance transmits and receives data.
	Flashing amber	Ports 1 and 2 or 3 and 4 flash amber together - those two ports are bypassed, and system is up.

Table 6 - Stratix 5950 Security Appliance Status Indicators

Indicator	Status	Description
Power Inputs		
	Off	Power to the appliance is off or is not properly connected.
	Solid green	Power is present on the associated circuit. (Hardware controlled)
Alarm Monitoring, Alarm Out		
	Off	The Alarm Out not configured or the system is off (Default).
	Solid red	System has detected a minor alarm report of a power-supply dual failure.
Alarm Monitoring, Alarm In 1 and 2		
	Off	The Alarm In not configured or the system is off (Default).
Ethernet Ports: Link Status		
	Off	No link
	Solid green	Link is up
	Flashing green	The appliance transmits and receives data.
	Solid amber	Fault, implies no link Ports 1 and 2 (copper/fiber) and ports 3 and 4 (copper only) fast blink amber together — Those ports are in bypass mode.

Centralized Management

Overview

Local management can get cumbersome when we must manage many IFWs in the network. A centralized management enables consistent policy enforcement and quick troubleshooting of security incidents, with offered summarized reports across the security deployment. A centralized interface helps organizations to scale efficiently and manage a wide range of security devices with improved visibility.

As explained in earlier sections, the IFW has two components: the firewall and FirePOWER® module. Each component is managed separately. FireSIGHT™ Management Center manages the FirePOWER component, and Cisco® Security Manager (CSM) manages the firewall component. The following sections provide an overview of each application.

FireSIGHT Management Center

The Cisco FireSIGHT Management Center manages the FirePOWER module of the IFW. FireSIGHT Management Center is the administrative nerve center for a number of security products that incorporate FirePOWER technology. It provides complete and unified management of firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection. The Management Center is the centralized point for event and policy management for the IFW platform.

The FireSIGHT Management Center provides extensive intelligence about the users, applications, devices, threats, and vulnerabilities that exist in your network. It uses this information to analyze your network vulnerabilities and provides tailored recommendations on which security incidents to investigate.

Figure 18 shows examples of the types of data that can be gathered via FireSIGHT Management Center.

Figure 18 - FireSIGHT Management Center

The FireSIGHT Management Center discovers real-time information about changed network resources and operations to provide a full contextual basis for making informed decisions. The FireSIGHT Management Center delivers a fine level of detail that includes:

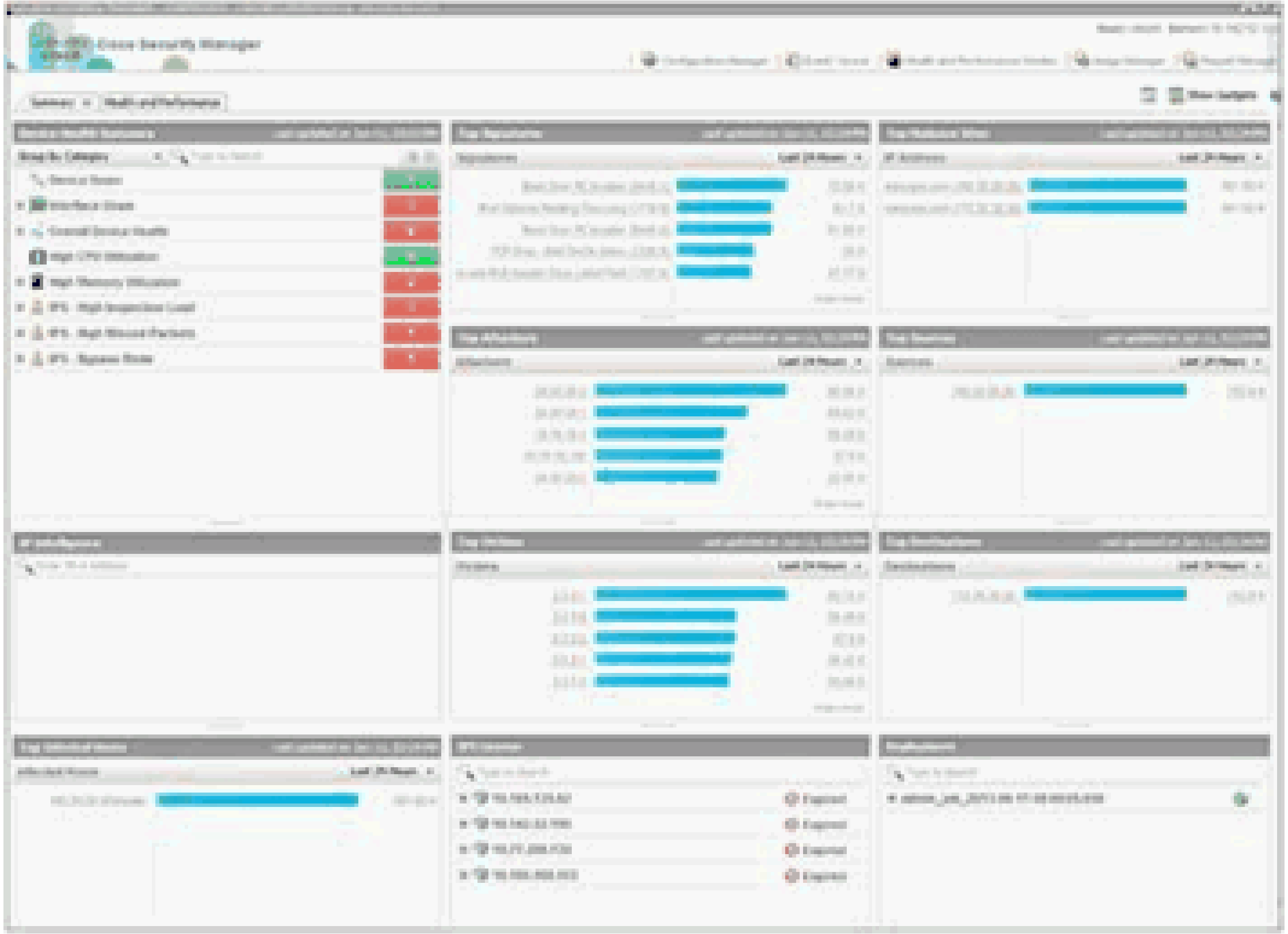
- Trends and high-level statistics that help managers and executives understand their security posture at a given moment in time and how it is changing, for better or worse.
- Event detail, compliance, and forensics that provide an understanding of what happened during a security incident to improve defenses, support breach containment efforts, and aid in legal enforcement actions.
- Workflow data that can be easily exported to other solutions to improve incident response management.

For more information on the FireSIGHT Management Center, see http://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html.

Cisco Security Manager (CSM)

The Cisco Security Manager (CSM) provides scalable, centralized management for the firewall component of the IFW. With CSM, administrators can gain visibility and maintain policy compliance across the network. Designed for operational efficiency, CSM also includes a powerful suite of automated capabilities, such as health and performance monitoring, software image management, automatic conflict detection, and integration with ticketing systems. Figure 19 shows an overview of CSM.

Figure 19 - Cisco Security Manager Overview



CSM provides the following functions:

- Policy and object management
  - Helps enable reuse of security rules and objects.
  - Facilitates process compliance and error-free deployments.
  - Improves ability to monitor security threats.
- Event management
  - Supports syslog messages that are created by Cisco security devices.
  - Facilitates viewing of real-time and historical events.
  - Provides rapid navigation from events to source policies.
  - Includes pre-bundled and customizable views for firewall, intelligent protection switching (intrusion prevention systems), and VPN.

- Reporting and troubleshooting
  - Provides system and custom reports.
  - Offers export and scheduled email delivery of reports in CSV or PDF format.
  - Provides advanced troubleshooting with tools such as ping, traceroute, and packet tracer.
- Image management
  - Provides direct, simplified upgrade of firewall software images via an intuitive wizard.
  - Offers scheduling of image upgrade jobs during network maintenance windows.
  - Imports images from the Cisco online software website or from a local file system.
  - Provides automated updates that can be performed on each firewall individually or run in groups.
- Health and performance monitoring (HPM)
  - Adds visibility around health and performance of firewalls, intrusion prevention systems (intrusion prevention systems), and VPNs.
  - Offers ability to set thresholds on various parameters.
  - Provides alerts when predefined thresholds are reached.
- API access
  - Shares information with other essential network services such as compliance and advanced security analysis systems.
  - Provides direct access to data from any security device that is managed by Cisco Security Manager via external firewall compliance systems.
  - Is compatible with various security compliance vendors such as Tufin, Algosec, and Skybox.
- Other functionalities
  - Provides insight into Talos™ Security Intelligence and Research Group (Talos) recommendations.
  - Helps administrators fine-tune their environments before signature updates are deployed.

For more information on the Cisco Security Manager, see http://www.cisco.com/c/en/us/products/security/security-manager/index.html

Management Recommendations

The following aspects of managing the IFW must be considered before deployment.

- Local management that uses Adaptive Security Device Manager (ASDM) is recommended for small deployments only (no more than five IFW devices).
- Centralized management is recommended for most deployments due to ease of manageability, policy consistency, quick troubleshooting, scalability, and robust logging.
- Cisco and Rockwell Automation recommend positioning the centralized management server in Level 3 Site Operations within the Industrial Zone.
- When the FirePOWER module of the IFW is being managed by the FireSIGHT Management Center, local (ASDM) configuration of the FirePOWER module is not supported.
- FireSIGHT Management Center and Cisco Security Manager generally support communication with the IFW via its dedicated management interface only.

Integration of New Firewalls

The following tasks are required to migrate a locally managed firewall to a centralized management system.

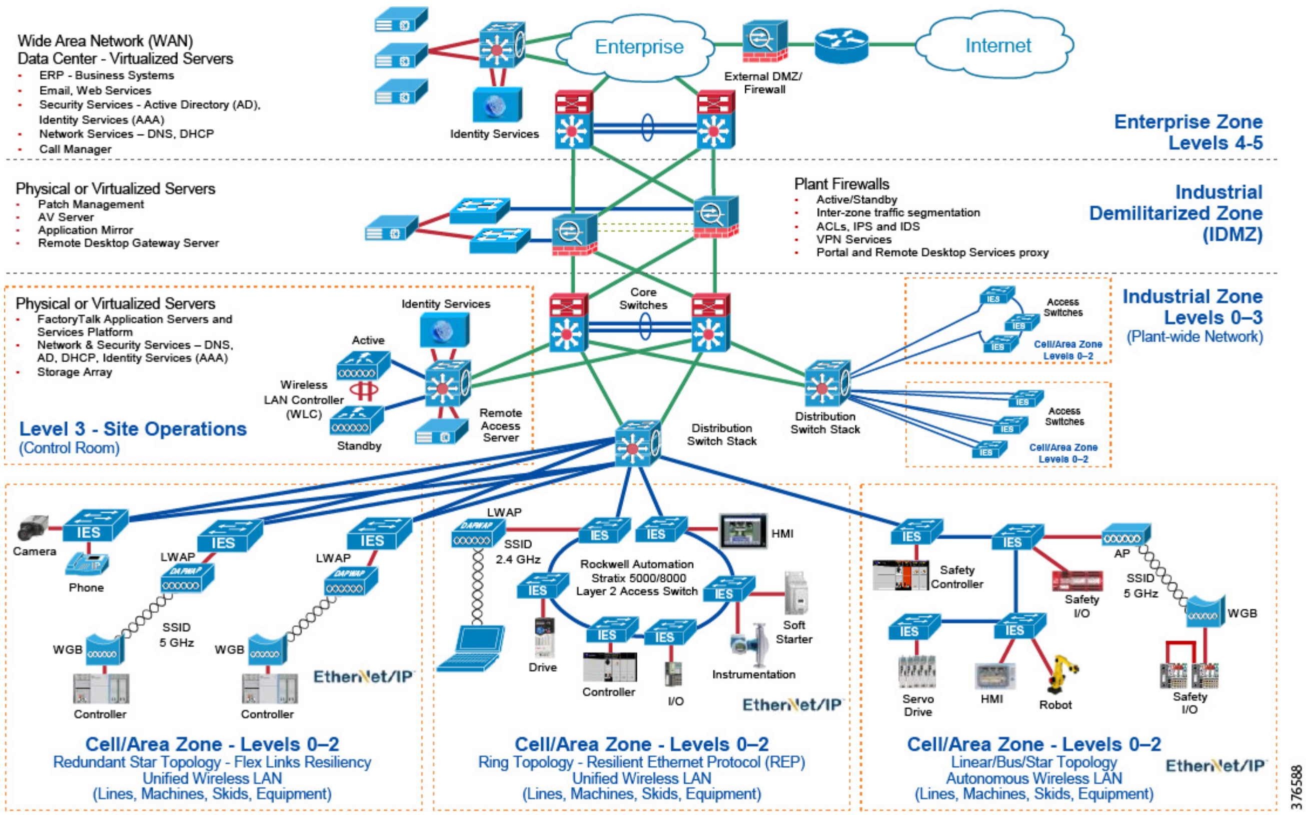
- In ASDM, configure the FireSIGHT Management Center as a remote manager.
- Change the management IP addresses for both the firewall and FirePOWER module to unique IP addresses within the management network.
- Connect the dedicated management interface to the management network.
- Add required licenses within FireSIGHT Management Center.
- Add the IFW in the centralized management application (FirePOWER and/or Cisco Security Manager).

IMPORTANT Locally configured FirePOWER policies are lost when you migrate from local management to FireSIGHT Management Center. Confirm that the current policies are exported and backed up, if needed, before the device is migrated.

Centralized Management

This figure describes the centralized management approach.

Figure 20 - Centralized Management


Wide Area Network (WAN)
Data Center - Virtualized Servers
- ERP - Business Systems
- Email, Web Services
- Security Services - Active Directory (AD), Identity Services (AAA)
- Network Services – DNS, DHCP
- Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Enterprise Zone Levels 4-5
Physical or Virtualized Servers
- Patch Management
- AV Server
- Application Mirror
- Remote Desktop Gateway Server
Plant Firewalls
- Active/Standby
- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
- FactoryTalk Application Servers and Services Platform
- Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
- Storage Array
Identity Services
Active
Wireless LAN Controller (WLC)
Standby
Remote Access Server
Core Switches
Level 3 - Site Operations
(Control Room)
Distribution Switch Stack
Distribution Switch Stack
IES
Access Switches
Cell/Area Zone Levels 0–2
Industrial Zone Levels 0–3
(Plant-wide Network)
Access Switches
Cell/Area Zone Levels 0–2
Camera
IES
Phone
LWAP
LWAP
WGB
SSID 5 GHz
WGB
Controller
Controller
EtherNet/IP
LWAP
SSID 2.4 GHz
Rockwell Automation Stratix 5000/8000 Layer 2 Access Switch
HMI
Drive
Controller
I/O
Soft Starter
Instrumentation
EtherNet/IP
Safety Controller
AP
SSID 5 GHz
Safety I/O
WGB
Servo Drive
HMI
Robot
Safety I/O
EtherNet/IP
Cell/Area Zone - Levels 0–2
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
Cell/Area Zone - Levels 0–2
Ring Topology - Resilient Ethernet Protocol (REP)
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Autonomous Wireless LAN
(Lines, Machines, Skids, Equipment)
376588

Hardware Bypass

The Stratix® 5950 security appliance has hardware bypass relay support between data port pairs 1 and 2 (copper/fiber) and 3 and 4 (on copper only). There are two instances where a bypass can be triggered.

- Power failure of the system
- The bypass mode is enabled manually through CLI command

Power Failure of the System

When power failure occurs, the system hard-wires the data ports if you have configured it to do so. All traffic can pass freely from internal- to external ports and vice versa. Upon power restoration, the system software monitors the start-up progress and only disables the bypass when the system is ready (Firewall and FirePOWER® are ready to process packets). An event can be sent out to the management system to indicate that the bypass status after power is restored.

Enable the Hardware Bypass by Using CLI Commands

Once you issue a command, the system immediately enables bypass, and ASA no longer receives traffic from the paired ports and all Firewall/VPN. The IPS function does not take effect until you issue commands to disable bypass. A critical event is sent to the management system to indicate that no protection is provided by the system.

The `enable sfr boot delay` feature default is set to on. Therefore, the system disables the bypass when both ASA and SFR modules are ready to process packets after the system boots.

When power is restored, the system stays in bypass mode if you specifically have it configured to do so. All traffic can pass from internal- to external ports and vice versa until you manually disable the bypass. An event/trap is sent to the management system to indicate that the system still continues bypass after power is restored.

The hardware on the Stratix 5950 security appliance restricts pairing to ports 1 and 2 or ports 3 and 4. Port 1 cannot be paired with 3, invalid pairs are (1, 3) / (1, 4) / (2, 3) / (2, 4). Valid pairs are (1, 2) and (3, 4) only.

ASA has CLI commands to allow the following:

- Allows you to configure bypass behavior when power fails or power-up conditions
- Allow you to enable/disable bypass manually (immediately)
- Allow you to check bypass settings and status by show commands

Default State of the Hardware Bypass

The default hardware bypass feature is enabled.

ASA CLI Commands for Hardware Bypass

The following ASA CLI commands have been added to support the hardware bypass feature.

```
show hardware-bypass
```

This CLI command displays the status of the bypass on particular port set. The status details the state of the relays on power fail and sticky as well.

CLI shows the following:

```
Gigabitethernet 1/1-1/2

-------------------------------

  L1-bypass port12 is enable/disable

  L1-bypass port12 on power fail is enable/disable

  L1-bypass port12 on power up is enable/disable

Gigabitethernet 1/3-1/4

-------------------------------

  L1-bypass port34 is enable/disable

  L1-bypass port34 on power fail is enable/disable

  L1-bypass port34 on power up is enable/disable
```

```
[no] hardware-bypass gigabitethernet {1/1-1/2|1/3-1/4}
[sticky]
```

This CLI command is used to enable or disable the bypass mode when power fails and sticky mode. A drop in the input 12V supply below a lower limit can trigger power failure events.

```
[no] hardware-bypass manual gigabitethernet {1/1-1/2|1/3-1/
4}
```

This CLI command is used to control the bypass. Means to enable or disable the bypass mode when power is on.

Limitations of Hardware Bypass

You must carefully consider enabling the bypass feature and its interoperability with other features. Here are some considerations to keep in mind.

- When using port security, the Stratix 5950 security appliance acts as another MAC address on the link. You must enable one more MAC allowed on the port of the switch than expected.
- A Stratix 5950 security appliance cannot be placed on a link with Port Security enabled. In general, placement of the appliance on a link with Port Security enabled affects the following.
  - Port Security limits on the number and value of MAC addresses on that link. These limits could be a manual CLI configuration
  - Any Smartport configuration that automatically sets Port Security configuration, for example, Automation Device, Desktop for Automation.
- Bypass mode is supported only in transparent mode. No CLI commands are available in the routed mode to configure bypass.
- Bridge-groups must contain g1/1, g1/2, or g1/3 and g3/4 for them to work properly when bypass is configured. If a bridge-group is defined with some ports bypass enabled and other ports bypass disabled, then there would be packet drops from/to ports for which bypass is enabled
- Disable the bypass feature when using subinterfaces and EtherChannel features.
- You have to disable the bypass feature to use HA and vice versa.
- After bypass is disabled and ASA starts to process packets, all TCP sessions have to be reinitiated like FTP and Telnet sessions. UDP and single packets can still pass. The ongoing FTP session packets are dropped mid-way once ASA starts to process packets. CIP™ connected messages and unconnected packets have the same behavior and are dropped in ASA.

Hardware Bypass CLI

The following are the CLI commands to support hardware bypass feature.

```
show hardware-bypass
```

This CLI displays the status of the bypass on a particular port set. The status details the state of the relays on powerfail, sticky and manual as well.

```
stratix5950# show hardware-bypass

                          Status           Powerdown        Powerup

Gigabitethernet 1/1-1/2   Enable/Disable   Enable/disable   Enable/Disable

Gigabitethernet 1/3-1/4   Enable/Disable   Enable/Disable   Enable/Disable
```

```
[no] hardware-bypass gigabitethernet {1/1-1/2|1/3-1/4}
[sticky]
```

This CLI command is used to enable or disable the bypass mode during power down and power up.

```
Hardware Bypass Behavior During Power Down
```

To enable hardware bypass mode when power is lost to the appliance the following CLI is used.

```
stratix5950# conf t

stratix5950(config) #hardware-bypass gigabitethernet 1/1-1/2
```

To disable hardware bypass mode when power is lost and power up to the appliance the following CLI is used.

```
stratix5950# conf t

stratix5950(config) #no hardware-bypass gigabitethernet 1/1-
1/2

  "Hardware Bypass Behavior During Power Up
```

When hardware bypass is enabled with the power up option, traffic continues to flow on the bypass port pair even after the system boots up. To enable bypass on power-up, we must also enable for power fail because the hardware supports power up along with power fail option. The option of power-up only is not supported in the hardware.

To enable hardware bypass mode with the power down and power up option, the following CLI is used.

```
stratix5950 # conf t
```

```
stratix5950(config)#hardware-bypass gigabitethernet 1/1-1/2
sticky
```

This command would disable both power up and power down for ports 1 and 2. The following CLI is used:

```
stratix5950(config)#no hardware-bypass gigabitethernet 1/1-
1/2
```

```
[no] hardware-bypass manual gigabitethernet {1/1-1/2|1/3-1/
4}
```

This CLI command is used to enable/disable the bypass feature when the appliance is powered and able to run. This CLI command does not depend on the power fail or power up option that is discussed in earlier sections.

To enable hardware bypass mode with the manual option, the following CLI is used.

```
stratix5950# hardware-bypass manual gigabitethernet 1/1-1/2
```

When hardware bypass is disabled with the manual option, the traffic stops on the bypass port pair immediately and flow through physical interfaces.

To disable hardware bypass mode with the manual option, the following CLI is used.

```
stratix5950# no hardware-bypass manual gigabitethernet 1/1-
1/2
```

```
  "[no] hardware-bypass boot-delay module sfr
```

This CLI command is used to enable/disable bypass operation delay based on SFR boot status. If it is turned on, the bypass only turns off if SFR module is full up. If it is not turned on, the bypass is turned off once the ASA module is ready. If bypass is not enabled, this command does not have any impact.

For a listing of Cisco® documentation, see Additional Resources on page 8.

Notes:

CIP Inspection

IMPORTANT In order for any Common Industrial Protocol (CIP™) access control policy or CIP intrusion policy to work properly, the Network Analysis Policy must be properly configured to inspect CIP traffic.

CIP Preprocessor

The ASA FirePOWER® module has a software component and the Network Analysis Policy rules engine that is called a preprocessor. The preprocessor is responsible to handle the interpretation of the packet before the rules engine handles the packet. The IFW has a CIP preprocessor that interprets the CIP protocol, which allows the system administrator to author policy rules related to the CIP protocol actions.

CIP is an open protocol that encompasses a comprehensive suite of messages and services for industrial automation applications. CIP is used to communicate to ControlLogix processors and I/O subsystems for control, process control, safety, motion control, real-time information and network management. The IFW with the CIP preprocessor can inspect a packet that contains the CIP protocol and determine whether to permit or deny the traffic based on the preconfigure policy rules.

Two types of CIP DPI rule categories have been added to the IFW:

- CIP Generic—Related to the open CIP standard.
- Rockwell Automation specific CIP—CIP protocol extensions specific to Rockwell Automation products.

The CIP open standards define a generic set of commands in the CIP protocol. The IFW defines security policies as they relate to the CIP open standard. The list of supported CIP generic rules are:

Table 7 - CIP Generic Rules

CIP Generic Rule	Description
CIP Admin	ODVA-specified commands that change the state of a device.
CIP Infrastructure	ODVA-specified commands that are core functions. For example, configuring sessions and connections.
CIP Malformed	Malformed data according to specification.
CIP Read	ODVA-specified commands that read data from a device.
CIP Unknown	CIP command was unable to be categorized to any other CIP application.
CIP Write	ODVA-specified commands that write data into a device.

It is common for a vendor to extend a standard to support the vendor-specific requirements not covered in the open standard. These extensions are often proprietary, which is why additional preprocessors are required for vendor-specific protocol extensions.

The CIP generic or open standard rules have been extended by Rockwell Automation to support Rockwell Automation devices. The CIP extensions that have been added to the IFW are:

Table 8 - CIP Extensions

CIP Extensions	Description
CIP RA Admin Download	Rockwell Automation commands that perform a project download.
CIP RA Admin Firmware Update	Rockwell Automation commands that perform a firmware update.
CIP RA Infrastructure	Rockwell Automation commands that commands that are core functions.
CIP RA Read Tag	Rockwell Automation commands that read tag values from a device.
CIP RA Write Tag	Rockwell Automation commands that write tag values into a device.

CIP Access Control Policies

CIP application categories are recommended as a way to configure CIP rules in access control policies. CIP application categories provide high-level groupings of various kinds of CIP applications to create simpler rules and policies.

You can use the following CIP application categories in access control policy rules.

Table 9 - Access Control Policy Application Categories

Application Category	Description
CIP RA Admin	Actions that change the state of the device via CIP. Use standard and Rockwell Automation-specific methods, such as CIP Reset. • ControlFlash or any tool that updates RA firmware in a standard way. • Usage of the Logix Designer application that goes online with a device; for example, Go Online, Download, or Upload. • Use of RSLinx™ software to change a Networking property of a module, such as: IP address, Netmask, Gateway, DNS server, Domain name, Hostname, Speed, Duplex Mode, Interface Speed.
CIP RA Read	Actions that read values/attributes via CIP, via the use of standard and Rockwell Automation-specific methods. For example, RSLinx software browse, or the HMI reading a tag.
CIP RA Write	Actions that set values/attributes via CIP, which do not fall under `CIP RA Admin’, which uses standard and Rockwell Automation-specific methods. For example, the HMI setting a tag value, RSLinx changes various properties of a device (properties that do not fall under CIP RA Admin).
CIP Admin	Actions that change the state of the device via CIP, with the use of standard methods, such as CIP Reset.
CIP Read	Actions that read values/attributes via CIP, with the use of standard methods.
CIP Write	Actions that set values/attributes via CIP, which do not fall under "CIP Admin", with the use of standard methods.

CIP Access Control Policy Rule Limitations

We only recommended to use CIP access control policy rules to block specific CIP traffic. Access control rules that you configure to log connections do not generate events for specified CIP applications. And access-control rules that you do not configure to log connections can generate events for CIP applications. We recommended that you use an access-control policy default action of Intrusion Prevention.

The CIP preprocessor does not support an access-control policy default action of Access Control: Trust All Traffic. This default action could produce undesirable behavior, including not dropping traffic triggered by CIP applications specified in intrusion rules and access-control policy rules.

The CIP preprocessor does not support an access-control policy default action of access control: Block All Traffic, which could produce undesirable behavior, including blocked CIP applications that you do not expect to be blocked.

The CIP preprocessor does not support application visibility for CIP applications, including network discovery.

CIP Intrusion Policies

Through advanced configuration, you can specify detailed CIP protocol parameters for the most granular level of traffic identification. These parameters are specified through IDS preprocessor rules. This configuration requires a high level of CIP-specific knowledge.

Table 10 - CIP Protocol Parameters

IDS Keyword	Description	Parameter Range
cip_attribute	Matches the last CIP Attribute ID in a Request Path of a CIP Message Router Request.	0…0xFFFF
cip_class	Matches the last CIP Class ID in a Request Path of a CIP Message Router Request.	0…0xFFFF
cip_conn_path_class	Matches the last CIP Class ID in a Connection Path of a CIP Forward Open Request.	0…0xFFFF
cip_instance	Matches the last CIP Instance ID in a Request Path of a CIP Message Router Request.	0…0xFFFFFFFF
cip_req	Matches a CIP request (CIP Message Router Request).	No data allowed
cip_rsp	Matches a CIP response (CIP Message Router Response).	No data allowed
cip_service	Matches the CIP Service of a CIP Message Router Request/ Response format.	0…0x7F
cip_status	Matches the General Status of a CIP Message Router Response.	0…0xFF
enip_command	Matches the Command in an EtherNet/IP™ Encapsulation Packet.	0…0xFFFF
enip_req	Matches an EtherNet/IP™ command request.	No data allowed
enip_rsp	Matches an EtherNet/IP command response.	No data allowed

The following pre-defined CIP preprocessor rules are available:

Table 11 - Pre-defined CIP Preprocessor Rules

Rule Name	Description
CIP_MALFORMED	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 can flag this rule.
CIP_NON_CONFORMING	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 could flag this rule.
CIP_CONNECTION_LIMIT	CIP connection limit per TCP connection exceeded. Least recently used connection removed.
CIP_REQUEST_LIMIT	CIP concurrent unconnected request limit per TCP connection exceeded. Oldest request removed.

Firewall Modes

ASA software provides the firewall features such as ACL, NAT, VPN, and overall system and platform management. FirePOWER® software provides the IPS features, application control, network discovery, and network AMP functionality.

The ASA runs in two different firewall modes:

- Routed
- Transparent

In routed mode, the ASA is considered to be a router hop in the network.

In transparent mode, the ASA acts like a 'bump in the wire,' or a 'stealth firewall,' and is not considered a router hop. The ASA connects to the same network on its inside and outside interfaces.

FirePOWER module can operate in two modes: inline mode and passive mode. The following figures provide overview of traffic flow in these two modes.

Figure 21 - Traffic Flow under Inline Mode

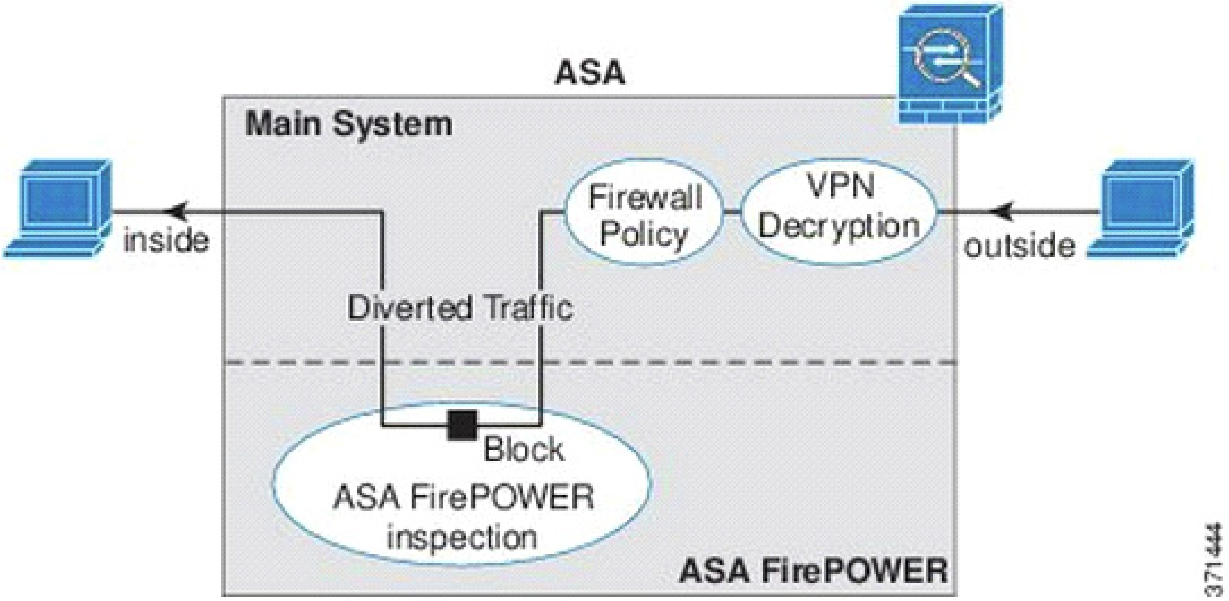
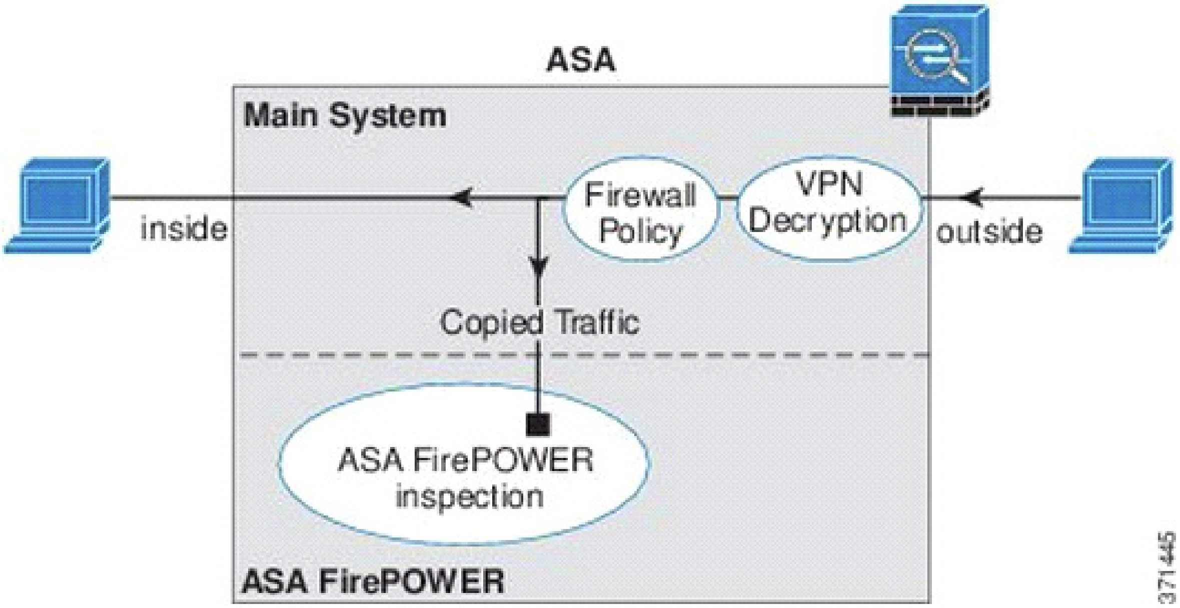


Figure 22 - Traffic Flow under Passive (Monitor Only) Mode



The Stratix® 5950 security appliance runs with these defaults:

- ASA in Transparent Mode
- SFR configured to be inline Passive mode with No Drop Actions (not in SPAN/TAP/Passive Mode)

Industrial Firewall Deployment Considerations

The IFW can be deployed in various modes, depending on policy enforcement and risk tolerance level. It is possible to place it in an inline or passive location in the network. When located inline, the IFW is inserted into the network segment and can operate in two modes: transparent or routed. When in a passive location, the IFW is separate from the network segment and only receives a copy of the traffic. The following sections provide details and considerations for each supported deployment mode of the IFW.

TIP Use the Multiport Automation Device Smartport role for any inline installs.

Inline Transparent Mode

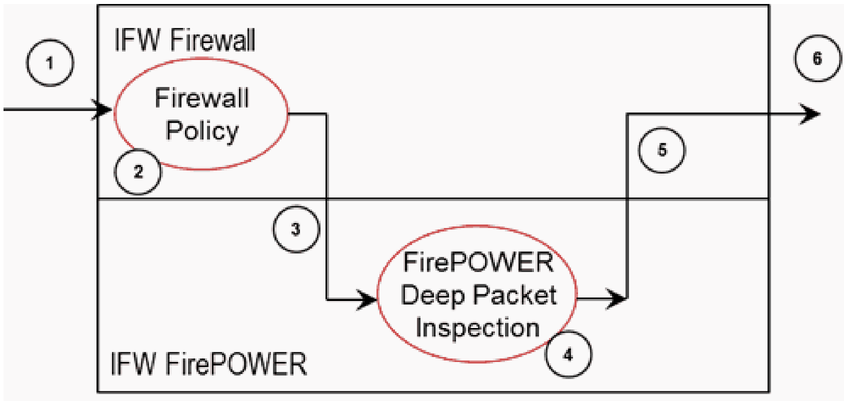
The IFW operates in transparent mode by default. In transparent mode, the IFW acts like a ‘bump in the wire,’ and is not considered a router hop (connects to the same network on its inside and outside interfaces). There can be two variations of this deployment.

In an inline deployment, the actual traffic is sent to the IFW FirePOWER module, whose policy affects what happens to the traffic. After dropping undesired traffic and other actions that are applied by policy, the traffic is returned to the firewall for further processing.

In inline transparent mode, traffic goes through the firewall checks before being forwarded to the FirePOWER module. The module blocks traffic that is not allowed for a certain application. All other traffic is forwarded through the firewall.

Figure 23 shows the traffic flow when using the IFW in inline transparent mode.

Figure 23 - IFW Traffic Flow for Inline Transparent Mode



As shown in the figure, traffic flows through the IFW as follows:

1. Traffic enters the IFW.
2. Firewall policies are applied.
3. Traffic is sent to the FirePOWER module.
4. The FirePOWER module applies its security policy to the traffic, and takes appropriate actions.
5. Valid traffic is sent back to the firewall; the FirePOWER module could block some traffic according to its security policy.
6. Traffic exits the IFW.

Inline Transparent Monitor-only Mode

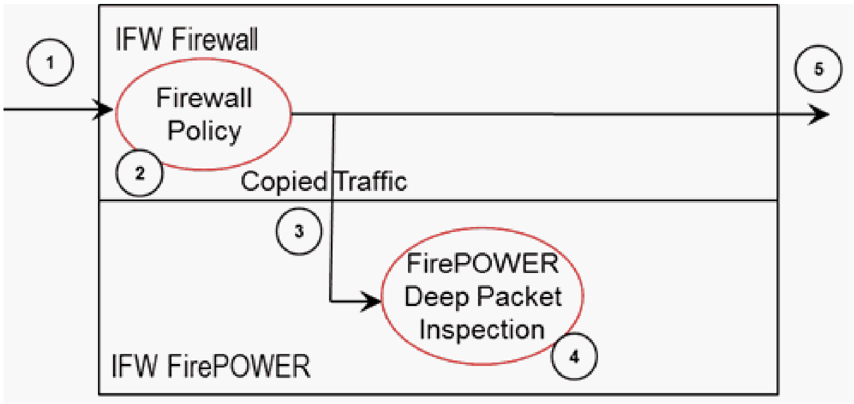
In an inline monitor-only deployment, a copy of the traffic is sent to the IFW FirePOWER module, but it is not returned to the firewall. Inline monitor-only mode indicates what the IFW FirePOWER module can do to traffic, and allows you to evaluate the content of the traffic, without impacting the network. However, in this mode, the firewall applies its policies to the traffic, so traffic can be dropped due to access rules, TCP normalization, and so forth.

TIP You cannot configure both inline monitor-only mode and normal inline mode simultaneously on the ASA. Only one type of security policy is allowed.

Inline transparent monitor-only mode sends a duplicate stream of traffic to the IFW FirePOWER module for monitoring purposes only. The module applies the security policy to the traffic and logs what it could do if it were operating in inline transparent mode. For example, traffic could be marked 'would have dropped', in events. You can use this information for traffic analysis and to help you decide if inline transparent mode is desirable.

Figure 24 shows the traffic flow when using the IFW in inline transparent monitor-only mode.

Figure 24 - IFW Traffic Flow for Inline Transparent Monitor-only Mode



As shown in the figure, traffic flows through the IFW as follows:

1. Traffic enters the IFW.
2. Firewall policies are applied.
3. Copied traffic is sent to the FirePOWER module.
4. The FirePOWER module applies its security policy to the traffic, and logs events only.
5. Traffic exits the IFW.

Inline Routed Mode

In routed mode, the ASA is considered to be a router hop in the network.

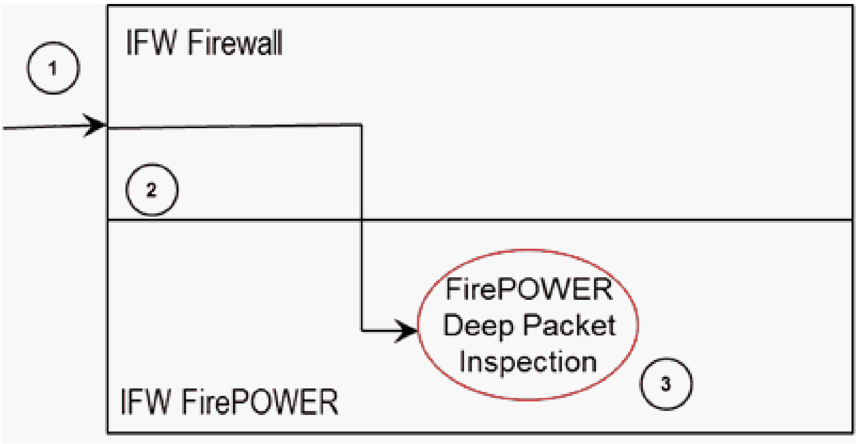
- Routed mode operates in layer 3 router mode.
- Each interface has IP addresses assigned and other typical layer 3 attributes are assigned.
- With two subnets active, CAN'T put the box into bypass mode.
- Only Active/Standby Mode - No data traffic in link
- Remote access to ISA directly.
- For routed mode, the following types of traffic are allowed through, by default:
  - Unicast IPv4 and IPv6 traffic from a higher security interface to a lower security interface.
- Broadcast and multicast traffic is blocked even if you allow it in an access rule, including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay).

Passive Monitor-only Mode

If you want to help prevent any possibility of the IFW to impact traffic, you can configure a traffic-forwarding interface and connect it to a SPAN port on a switch. In this mode, all traffic is sent directly to the IFW FirePOWER module without firewall processing. The traffic is 'black holed,' in that nothing is returned from the module, nor does the IFW send the traffic out any interface.

In passive monitor-only mode, the module applies the security policy to the traffic and indicates what it could do if it were operating in inline transparent mode. For example, traffic could be marked 'would have dropped' in events.

Figure 25 - IFW Traffic Flow for Passive Monitor-only Mode shows the traffic flow when IFW is in passive monitor-only mode



As shown in the figure, traffic flows through the IFW as follows:

1. Traffic enters the IFW on the traffic-forwarding interface.
2. All traffic is sent directly to the FirePOWER module.
3. The FirePOWER module applies its security policy to the traffic, and logs events only.

Deployment Recommendations

Placement and deployment of the IFW depends on the desired function of the device in the industrial network. When you place the IFW inline with traffic flow, you can monitor the traffic and/or take desired actions, such as blocking. If you place the IFW outside of the traffic flow, you can only monitor the traffic.

Regardless of where the IFW is placed, Cisco® and Rockwell Automation recommend configuring the device in monitor-only (IDS) mode during the initial deployment stages. This strategy allows for applications, endpoints, and other communication data to be monitored on the network over a time. IPS policies can be crafted over time that can have the desired effect on targeted traffic without inadvertently affecting other traffic. Once the network traffic is characterized and the policies are tested, an IFW, deployed inline, can be placed into its normal (IPS) mode, which helps protect the network. If the risk of inadvertent effects on network traffic outweighs the benefits of IPS for a particular deployment, the IFW can be placed as a passive listener. However, the IFW must be physically relocated to be inline with the network segment if an IPS function is desired in the future.

When placed inline, the IFW can be deployed in transparent or routed mode. Cisco and Rockwell Automation generally recommend deploying the IFW in transparent mode (default) unless routing functionality is needed.

In summary, the deployment recommendations for the IFW are:

- Inline transparent mode - deployments where the ability to help protect the network is more important than traffic affected by potential 'false positives'. Always place the IFW in monitor-only mode during the initial deployment, then transition to full IPS mode during a maintenance window.

- Inline routed mode - same as transparent mode, but deployments where routing functionality is also required.

- Passive monitor-only mode - deployments where uninterrupted connectivity is more important than active network protection. The IFW remains in monitor-only mode with no possibility of running in full IPS mode unless it is moved to be inline in the network segment.

Industrial Firewall Use Cases

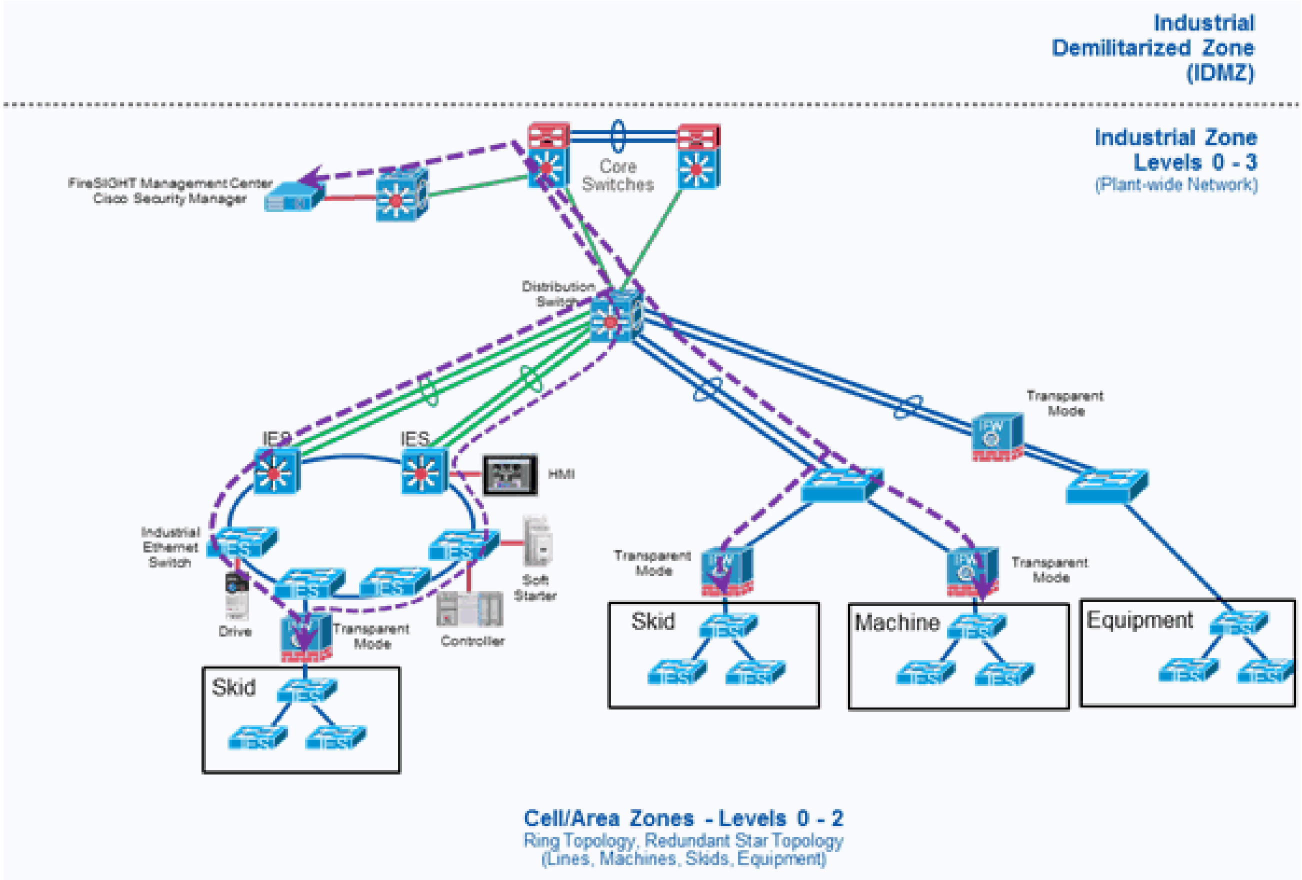
The IFW is used to separate networks with different security requirements and is also strategically placed within a network to monitor and log traffic. In this section, several architectures and their use cases are discussed.

Machine/Skid Protection

The machine/skid protection use case is used to separate a machine, skid, or unit from a higher-level network. This protection could be to support different security requirements between the larger network and the machine/skid or to restrict ingress and egress traffic.

As shown in Figure 26, the Transparent Mode firewalls are placed between a larger network and a grouping of automation equipment that act as a machine, skid, or unit.

Figure 26 - Industrial Firewall Placement for Machine/Skid Protection



In each case, the IFW acts as an ingress and egress point to the machine/skid where traffic can be monitored or controlled through firewall or DPI security policies.

Considerations

Before implementing the IFW in a machine/skid protection architecture, it is recommended that the designer understands and documents the following.

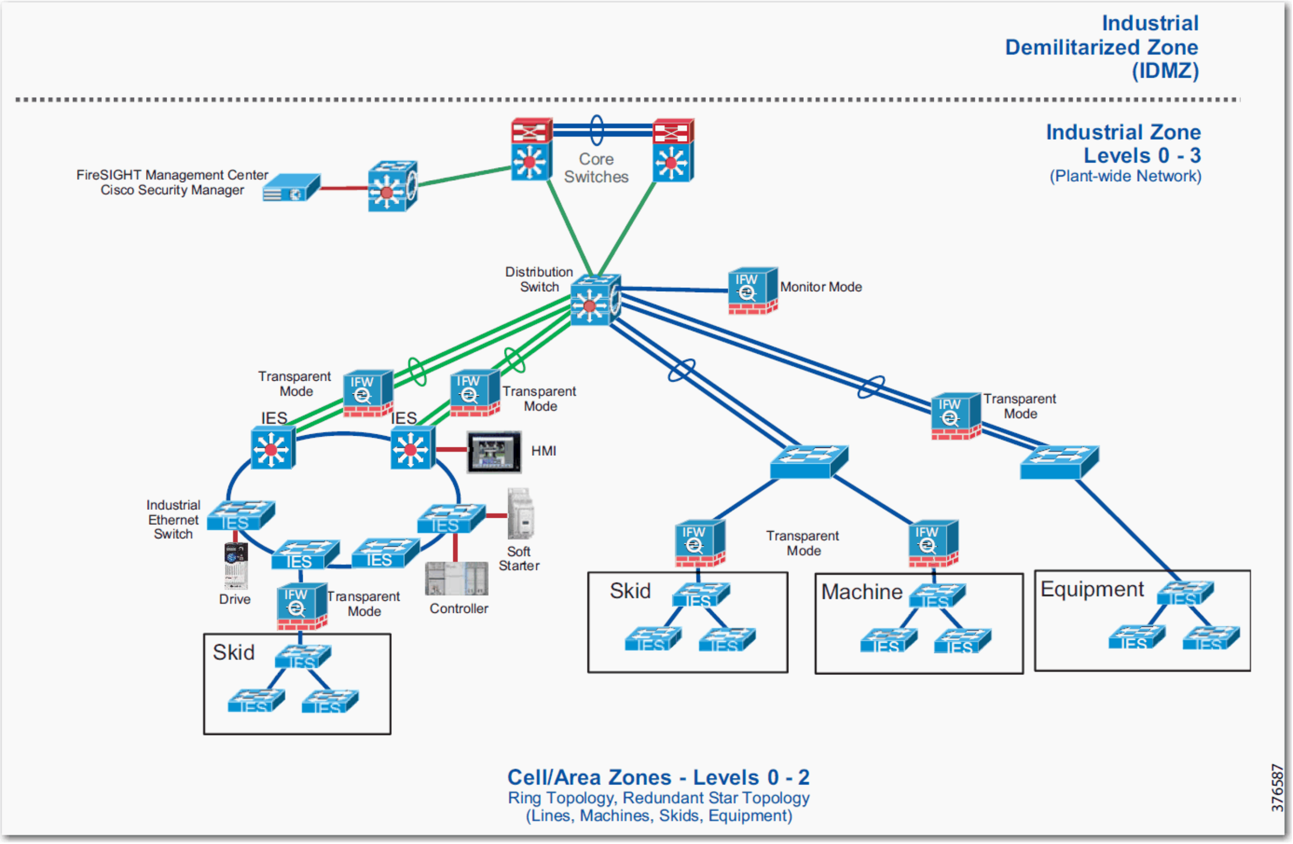
- Ingress and egress traffic source and destination host communications. For example, IP addresses of controllers, HMI, engineering workstations, and all communications that enter or leave the machine/skid must be known so firewall and DPI security policies can be configured.
- Ingress and egress traffic source and destination protocols must be known to configure the firewall and DPI rules.
- Ingress and egress traffic volume.
- Redundancy and availability requirements. For example, when considering high availability, one must regard the security considerations while in hardware bypass mode.

Redundant Star Cell/Area Zone Protection

When a redundant star network configuration is required to meet redundancy requirements, the IFW can have an architecture that supports redundant Layer 2 EtherChannel links.

In Figure 27, the IFW is placed between the distribution switch and the plant floor equipment.

Figure 27 - Industrial Firewall Placement for Redundant Star Cell/Area Zone Protection


Industrial Demilitarized Zone (IDMZ)
Industrial Zone Levels 0 - 3
(Plant-wide Network)
FireSIGHT Management Center
Cisco Security Manager
Core Switches
Distribution Switch
IFW
Monitor Mode
Transparent Mode
IES
HMI
Industrial Ethernet Switch
Drive
Controller
Soft Starter
Skid
Machine
Equipment
Cell/Area Zones - Levels 0 - 2
Ring Topology, Redundant Star Topology
(Lines, Machines, Skids, Equipment)
376587

This architecture is typically used when the IFW monitors or blocks traffic at a higher level in the network architecture and a redundant star network is designed or deployed.

Considerations

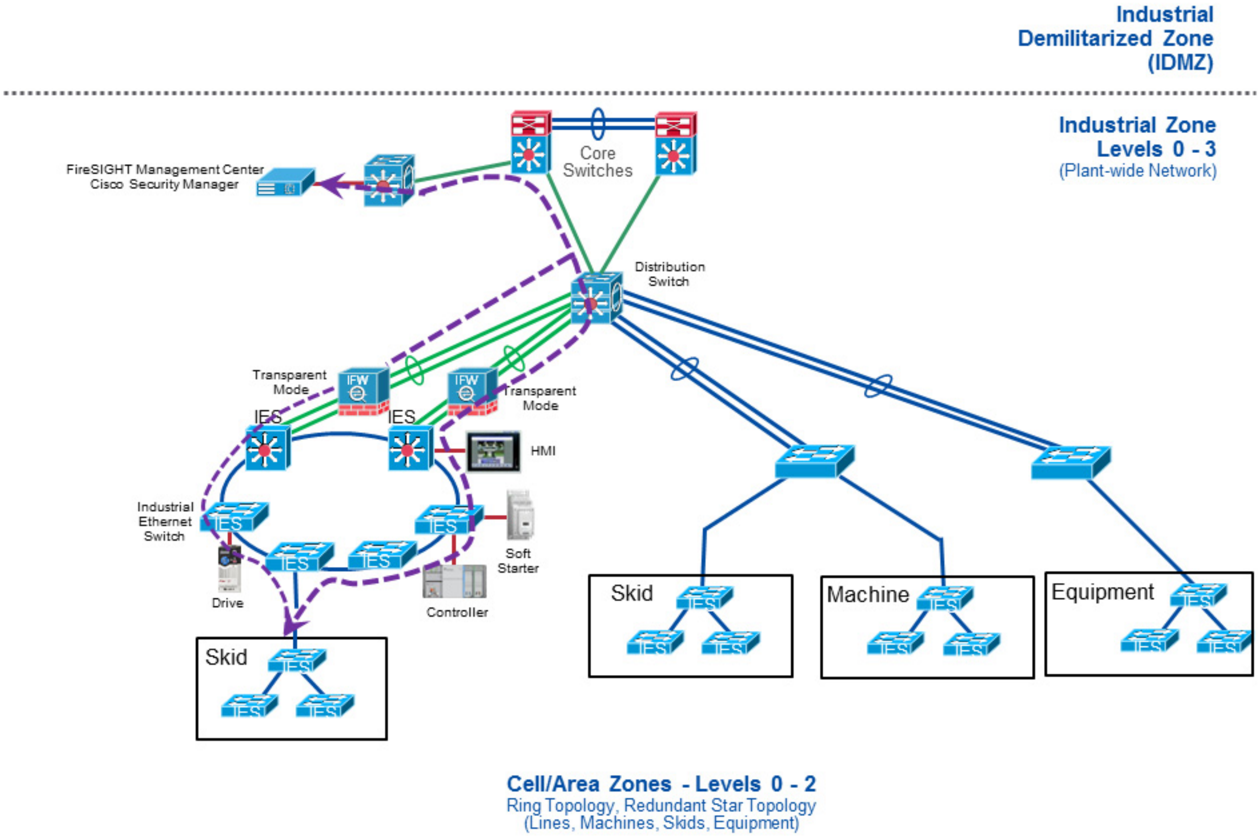
Before implementing the IFW in a redundant star architecture, it is recommended that the designer understands and documents the following.

- Ingress and egress traffic source and destination host communications. For example, IP addresses of controllers, HMI, engineering workstations, and all communications that enter or leave the machine/skid must be known so firewall and DPI security policies can be configured.
- Ingress and egress traffic source and destination protocols must be known to configure the firewall and DPI rules.
- Ingress and egress traffic volume.
- Redundancy and availability requirements. For example, when the IFW is configured with trunk ports, then hardware bypass mode is not available in this architecture.

Ring Cell/Area Zone Protection

The ring cell/area zone protection use case is used to monitor and apply security policies to a ring. As shown in Figure 28, two Transparent Mode firewalls are placed between the distribution switches and the ring.

Figure 28 - Industrial Firewall Placement for Ring Cell/Area Zone Protection



The IFWs are not acting as an active/standby firewall pair in this configuration, but they simply provide firewall and, possibly, DPI functionality on both ingress points of the network ring.

Considerations

Before implementing the IFW in a ring cell/area zone protection architecture, it is recommended that the designer understands and documents:

- Ingress and egress traffic source and destination host communications.

  For example, IP addresses of controllers, HMI, engineering workstations, and all communications that enter or leave the machine/skid must be known so firewall and DPI security policies can be configured.

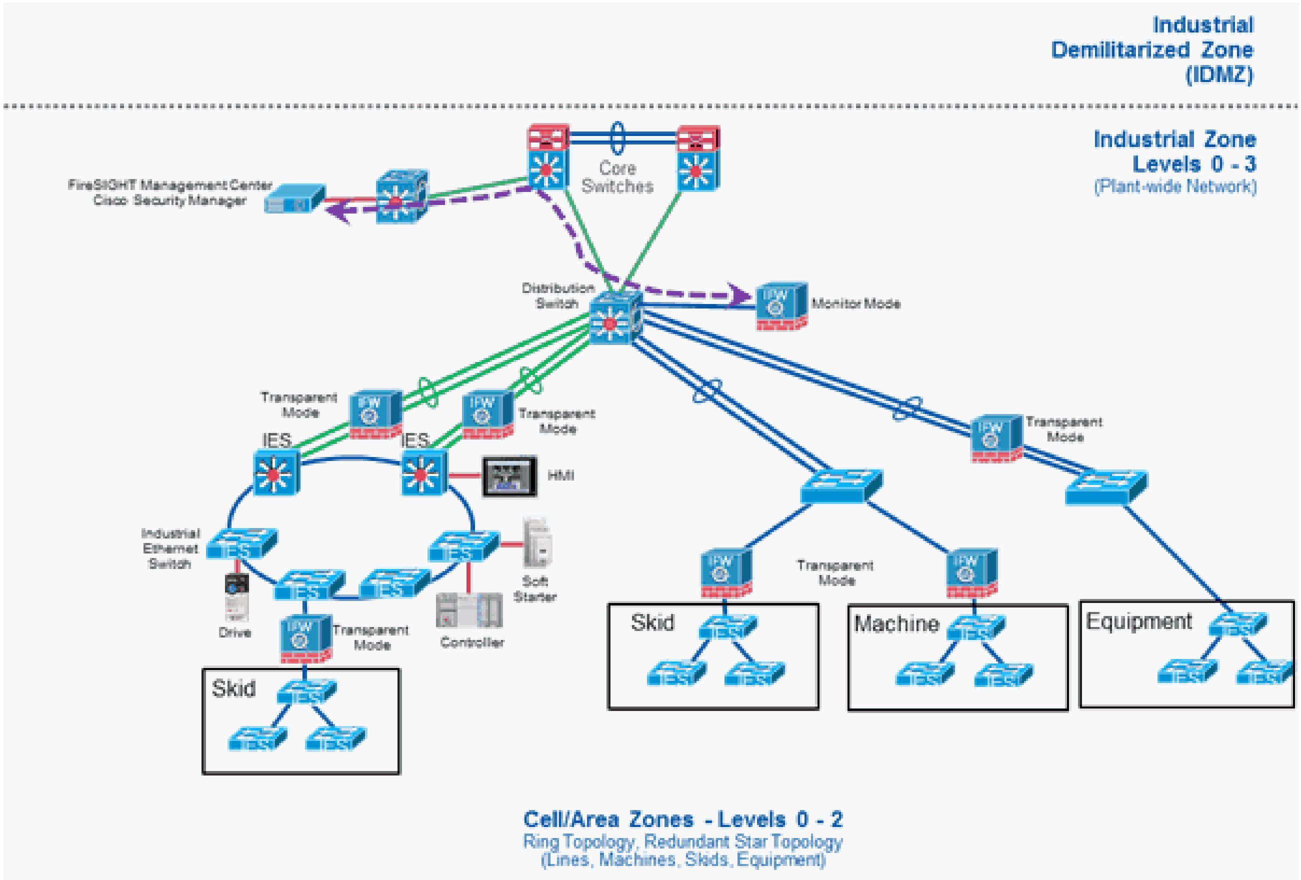
- Ingress and egress traffic source and destination protocols must be known to configure the firewall and DPI rules.
- Ingress and egress traffic volume.
- Redundancy and availability requirements. In this use case, the ports are configured for Layer 3 EtherChannel. Hardware bypass is not available in this architecture.

Cell/Area Zone Monitoring

The cell/area zone monitor mode use case is used to monitor traffic of interest without placing the IFW directly inline of a controller, skid, machine, or cell/area zone of interest. The IFR is connected to a switch that has visibility to the traffic that is required to be monitored. A span session or port mirror is created to send the traffic of interest to the IFW.

Figure 29 illustrates this use case.

Figure 29 - Industrial Firewall Placement for Cell/Area Zone Monitoring



Considerations

Before implementing the IFW as a monitor, it is recommended that the designer understand and document:

- Ingress and egress traffic volume

Notes:

Chapter 9

Update the Device

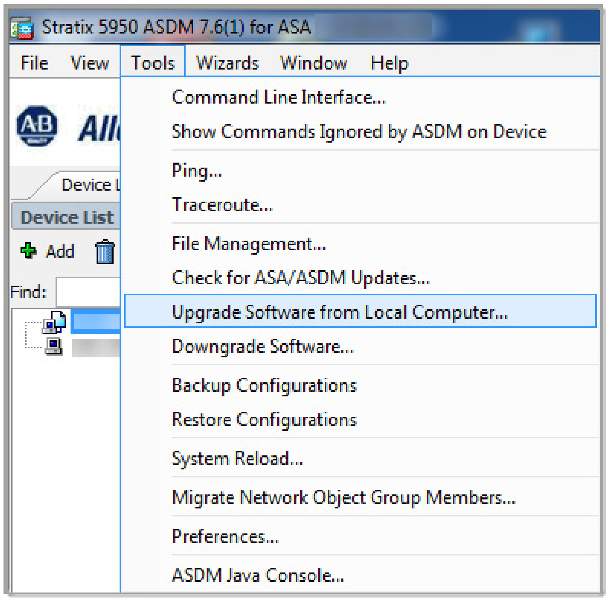
To update the Stratix® 5950 security appliance, complete these procedures:

1. Upgrade the ASA security device manager (ASDM).
2. Upgrade the adaptive security appliance (ASA).
3. Back up the controls license.
4. Install the Sourcefire® (SFR) update.
5. Restore the controls license.
6. Upgrade the bootloader.

Upgrade ASDM Software

To upgrade the ASDM software, follow these steps.

1. Obtain the latest ASDM image from the Rockwell Automation support site: https://compatibility.rockwellautomation.com.
2. From the Tools menu, choose Upgrade Software from Local Computer.


Stratix 5950 ASDM 7.6(1) for ASA
File
View
Tools
Wizards
Window
Help
Command Line Interface...
Show Commands Ignored by ASDM on Device
Ping...
Traceroute...
File Management...
Check for ASA/ASDM Updates...
Upgrade Software from Local Computer...
Downgrade Software...
Backup Configurations
Restore Configurations
System Reload...
Migrate Network Object Group Members...
Preferences...
ASDM Java Console...
Device List
Add
Find:

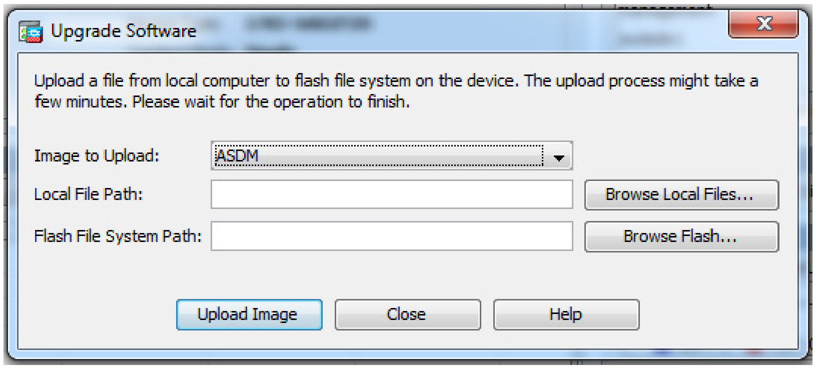
3. From the Image to Upload pull-down menu, choose ASDM.
4. To find the ASDM software image on the local personal computer, click Browse Local Files.

   The file name appears in the Local File Path field.
5. (Optional). To change the file name, click Browse Flash.

IMPORTANT	We recommend that you do not change the file name.

   The Browse Flash dialog box appears with the Local File System Path populated automatically. If the file name does not appear, enter it manually in the File Name field, and then click OK.
6. Click Upload Image.

   ASDM uploads the file.


Upgrade Software

Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish.

Image to Upload: ASDM

Local File Path:

Flash File System Path:

Table 12 - Upgrade Software Configuration Descriptions

Field	Description
Image to Upload	• ASA—Adaptive security appliance. • ASDM—Cisco® device management software for the ASA platform.
Local File Path	The path to the location of the file on your local personal computer.
Flash File System Path	The path to the system designed for the flash device.

7. When the ASDM dialog box indicates that the image was uploaded and prompts you to set the ASDM image, click Yes.

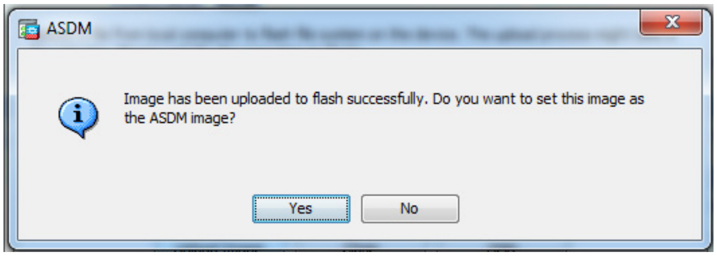
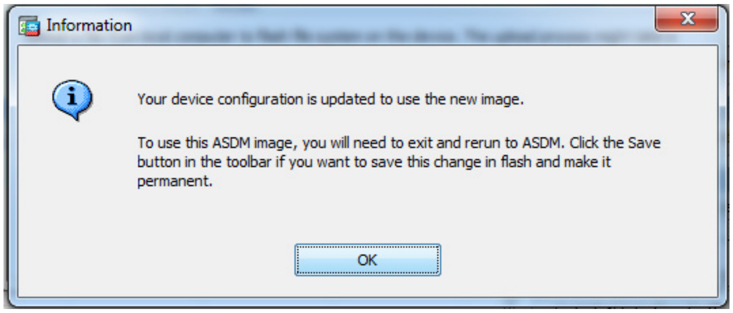


Image has been uploaded to flash successfully. Do you want to set this image as the ASDM image?

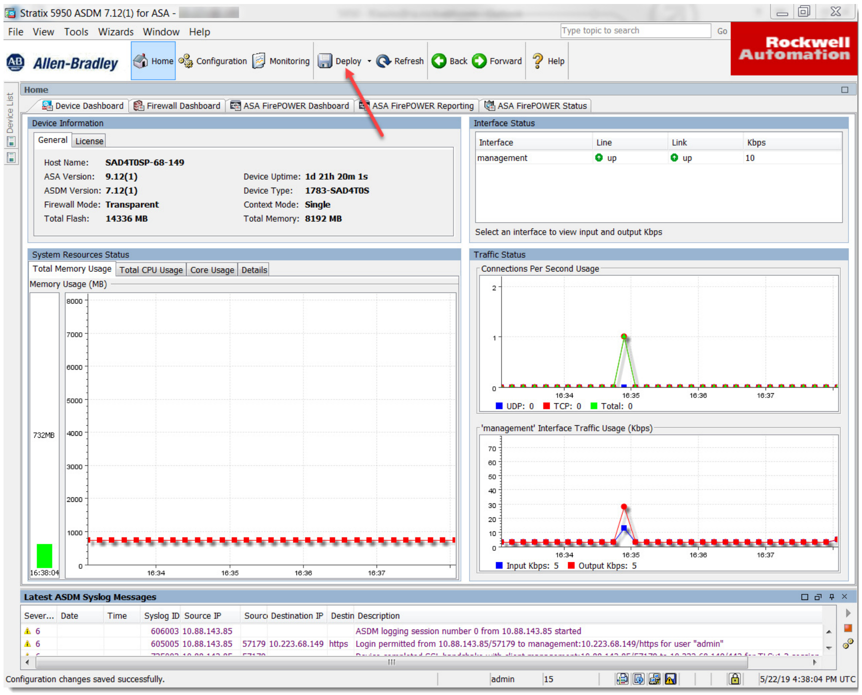
8. When the Information dialog box indicates that the configuration is updated with the new image, click OK.



Your device configuration is updated to use the new image.

To use this ASDM image, you will need to exit and rerun to ASDM. Click the Save button in the toolbar if you want to save this change in flash and make it permanent.

9. Click Deploy near the top-middle of the ASDM home dialog box.



Stratix 5950 ASDM 7.12(1) for ASA - [redacted]

Host Name: SAD4T0SP-68-149
ASA Version: 9.12(1)
ASDM Version: 7.12(1)
Firewall Mode: Transparent
Total Flash: 14336 MB
Device Uptime: 1d 21h 20m 1s
Device Type: 1783-SAD4T0S
Context Mode: Single
Total Memory: 8192 MB

Interface	Line	Link	Kbps
management	up	up	10

Select an interface to view input and output Kbps

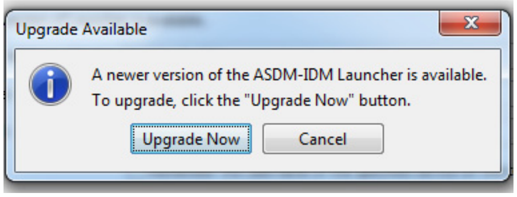
Sever...	Date	Time	Syslog ID	Source IP	Sourc	Destination IP	Destin	Description
6			606003	10.88.143.85				ASDM logging session number 0 from 10.88.143.85 started
6			605005	10.88.143.85	57179	10.223.68.149	https	Login permitted from 10.88.143.85/57179 to management:10.223.68.149/https for user "admin"

Configuration changes saved successfully. admin 15 5/22/19 4:38:04 PM UTC

10. Exit ASDM.

11. Reopen ASDM and update it on your local personal computer.

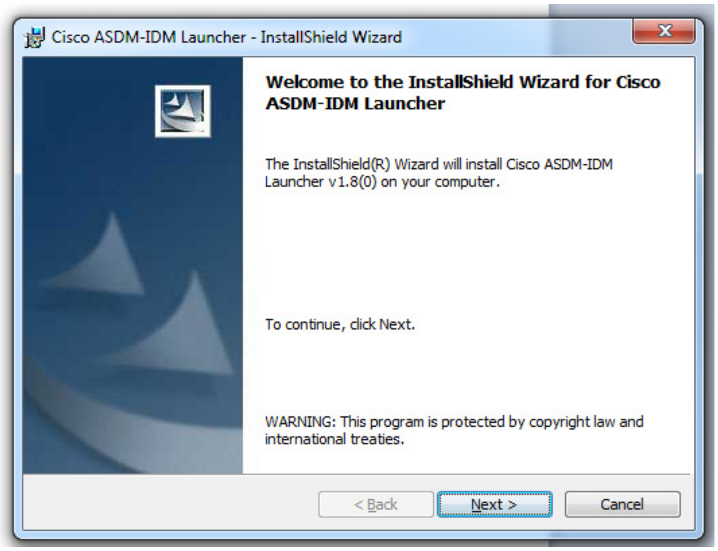
    a. Click Upgrade Now.



Upgrade Available

A newer version of the ASDM-IDM Launcher is available.
To upgrade, click the "Upgrade Now" button.

    b. On the InstallShield Wizard Welcome dialog box, click Next.



Cisco ASDM-IDM Launcher - InstallShield Wizard

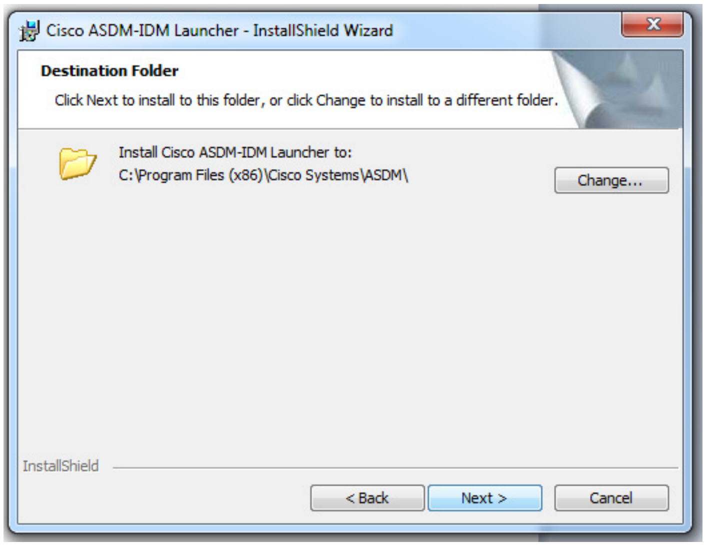
Welcome to the InstallShield Wizard for Cisco ASDM-IDM Launcher

The InstallShield(R) Wizard will install Cisco ASDM-IDM Launcher v1.8(0) on your computer.

To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

c. On the Destination Folder dialog box, click Next.



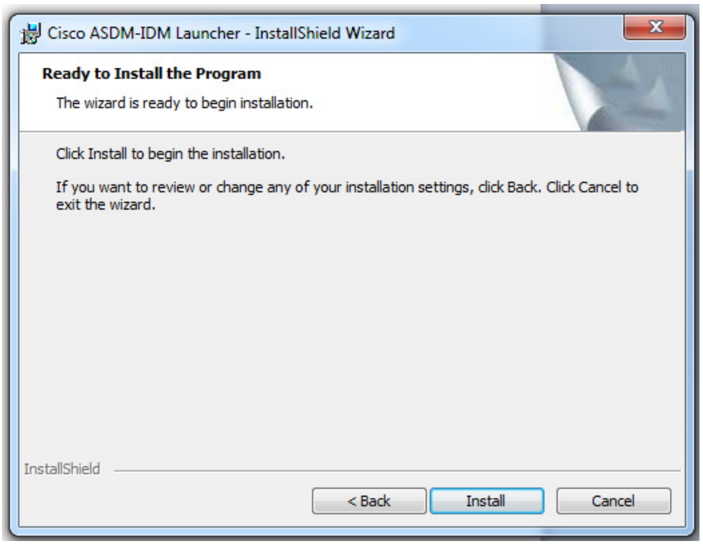
Cisco ASDM-IDM Launcher - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Cisco ASDM-IDM Launcher to:
C:\Program Files (x86)\Cisco Systems\ASDM\

d. On the Ready to Install the Program dialog box, click Install.



Cisco ASDM-IDM Launcher - InstallShield Wizard

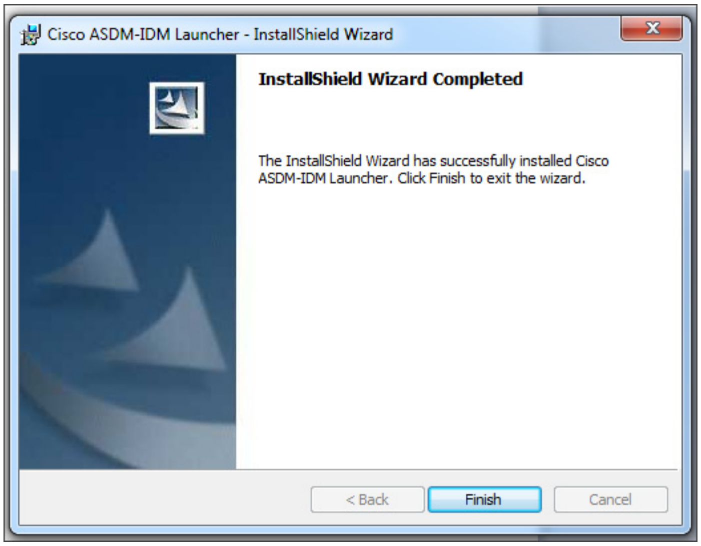
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

e. On the InstallShield Wizard Completed dialog box, click Finish.



InstallShield Wizard Completed

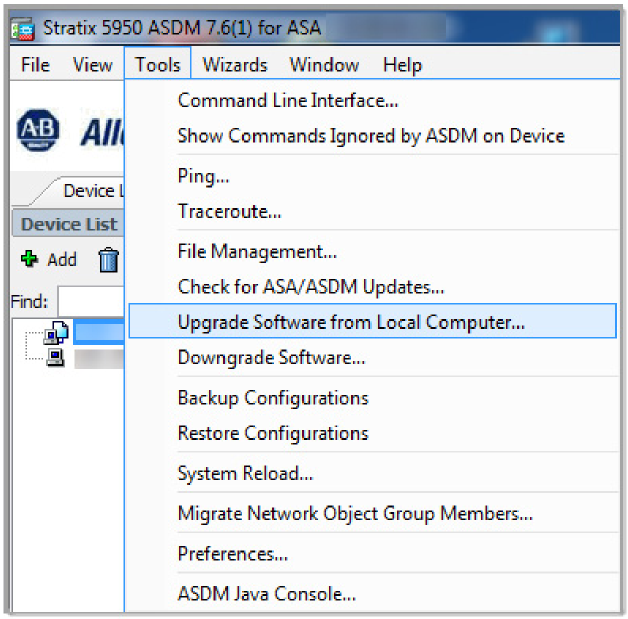
The InstallShield Wizard has successfully installed Cisco ASDM-IDM Launcher. Click Finish to exit the wizard.

12. Reconnect to the device with the newly upgraded ASDM.

Upgrade ASA Software

From the ASDM home page, follow these steps to upgrade the ASA software.

1. Obtain the latest ASA image from the Rockwell Automation support site: https://compatibility.rockwellautomation.com.
2. Choose Tools > Upgrade Software from Local Computer.



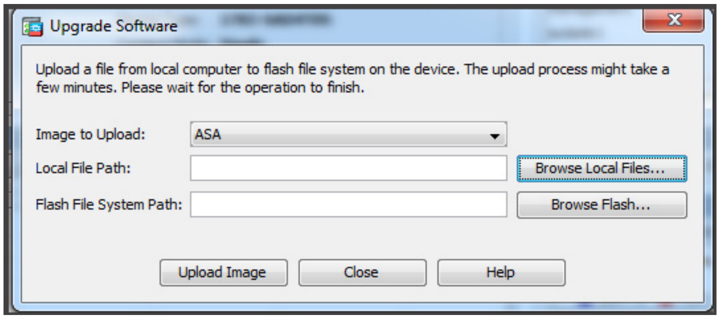
3. In the Upgrade Software dialog box, choose ASA from the Image to Upload pull-down menu.
4. To find the ASA software image on your local personal computer, click Browse Local Files. The file name appears in the Local File Path field.

5. (Optional). To change the file name, click Browse Flash.

IMPORTANT	We recommend that you do not change the file name.

The Browse Flash dialog box appears with the file name populated automatically. If the file name does not populate automatically, enter it manually in the File Name field, and then click OK.

6. Click Upload Image. ASDM uploads the file.



Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish.

Image to Upload: ASA

Local File Path:

Flash File System Path:

Field	**Description**
Image to Upload	• ASA—Adaptive security appliance • ASDM—Cisco device management software for ASA platform
Local File Path	The path to the location of the file on your local personal computer.
Flash File System Path	The path to the location on device flash.

The ASA dialog box indicates that the image was uploaded and prompts whether you want the image set as the restart image.

7. To make this the ASA image, click Yes.

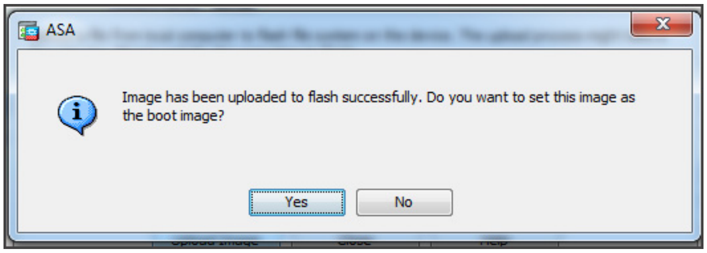
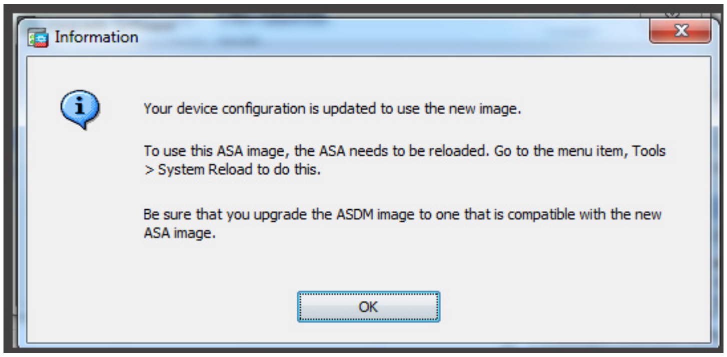


Image has been uploaded to flash successfully. Do you want to set this image as the boot image?

8. At the Information prompt, click OK.



Your device configuration is updated to use the new image.

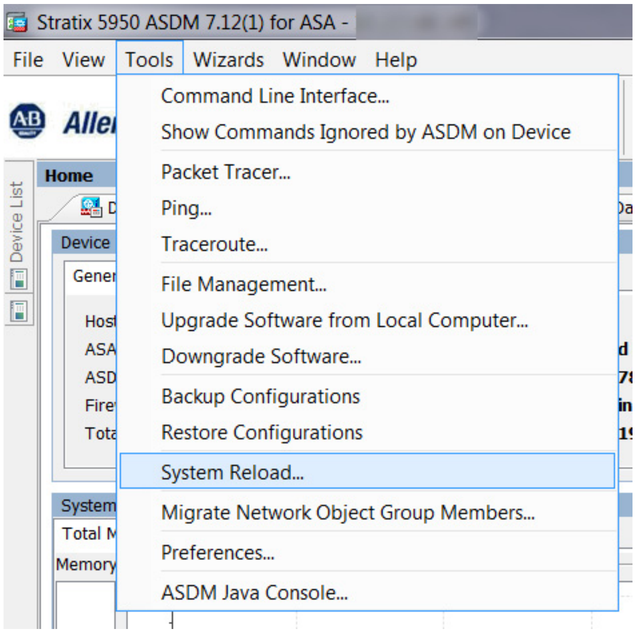
To use this ASA image, the ASA needs to be reloaded. Go to the menu item, Tools > System Reload to do this.

Be sure that you upgrade the ASDM image to one that is compatible with the new ASA image.

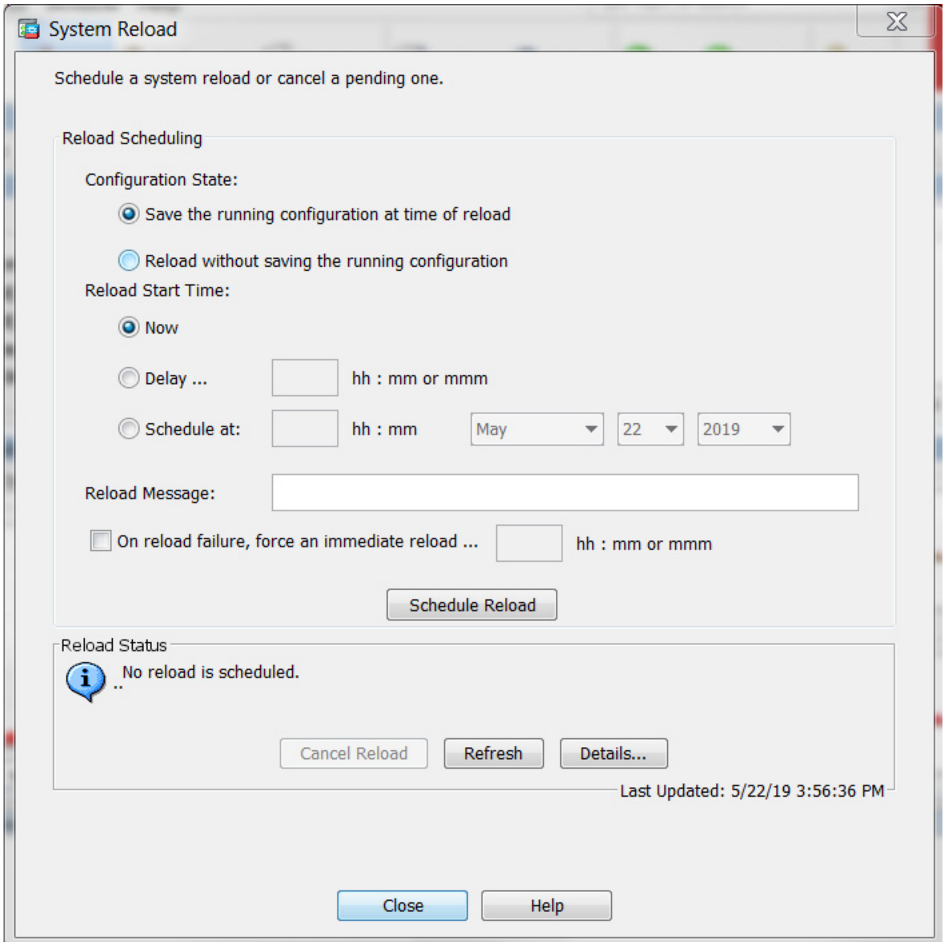
9. Click Close in the Upload Image from Local personal computer dialog box.

10. Reload the device:

    a. From the ASDM home dialog box, choose Tools > System Reload to reload the device.



b. The System Reload dialog box appears. Click Schedule Reload.



System Reload

Schedule a system reload or cancel a pending one.

Reload Scheduling

Configuration State:

● Save the running configuration at time of reload

○ Reload without saving the running configuration

Reload Start Time:

● Now

○ Delay ... hh : mm or mmm

○ Schedule at: hh : mm May 22 2019

Reload Message:

□ On reload failure, force an immediate reload ... hh : mm or mmm

Reload Status

No reload is scheduled.

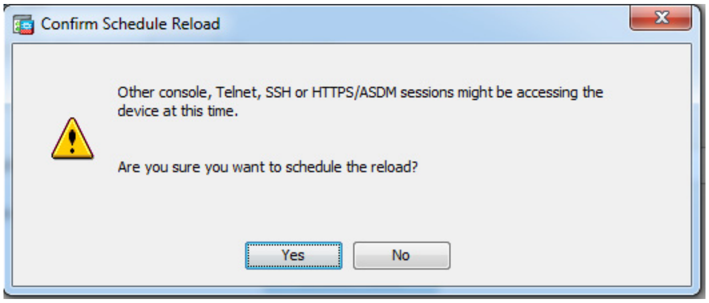
Last Updated: 5/22/19 3:56:36 PM

Table 13 - System Reload Configuration Fields

Field	Description
Save the running configuration at time of reload	Saves the running configuration when the system reloads.
Reload without saving the running configuration	Reloads the running configuration without saving it.
Now	Restart the device immediately.
Delay	Number of hours and minutes from now to reload the device.
Schedule at	The time and date to reload the device.
Reload Message	The message to be displayed when the system is about to restart.
On reload failure, force an immediate reload after	Specifies whether the device forces a reload immediately if a scheduled reload fails. Also, specifies the maximum hold time, which is the amount of time that the security appliance waits to notify other subsystems before a shutdown or restart. A forced shutdown/reboot occurs after this time elapses.

c. Click Yes on the Confirm Schedule Reload dialog box.

The device turns off.

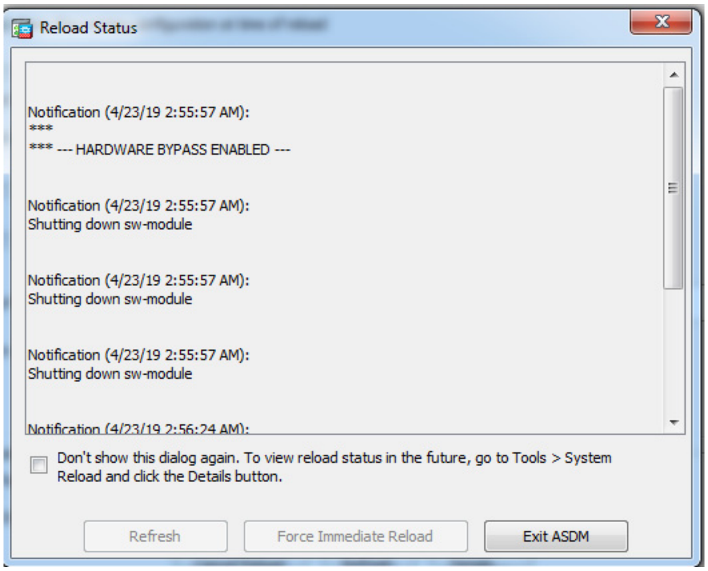


Other console, Telnet, SSH or HTTPS/ASDM sessions might be accessing the device at this time.

Are you sure you want to schedule the reload?

The Reload Status dialog box displays the restart process.

d. Click Exit ASDM.



```
Notification (4/23/19 2:55:57 AM):
***
*** --- HARDWARE BYPASS ENABLED ---


Notification (4/23/19 2:55:57 AM):
Shutting down sw-module


Notification (4/23/19 2:55:57 AM):
Shutting down sw-module


Notification (4/23/19 2:55:57 AM):
Shutting down sw-module


Notification (4/23/19 2:56:24 AM):
```

□ Don't show this dialog again. To view reload status in the future, go to Tools > System Reload and click the Details button.

e. Restart ASDM once the ASA reboots, which takes a few minutes.

To know when the ASA is ready, ping the IP address.

Back Up Controls License

Before updating your software, you must back up your controls license. To back up your controls license from the command line, follow these steps.

1. Access the SFR command line interface.
   If you are using a console cable, the CLI defaults to ASA. In this case, use the command `session sfr console`, and then press Enter to access ASA. If you use SSH to connect directly to SFR, then you do not need to use this command.

   Log in to SFR with your configured username and password.
   If you did not configure a password, the SFR 5.4 defaults are username=`admin`, password=`Sourcefire`.
   The SFR 6.4 defaults are username=`admin`, password=`Admin123`.

2. Type `expert` to change to the Linux console.
   The prompt changes, and the full Linux command structure is available.

3. Type `sudo -i`, and then type the same password that you used in Step 2, again at the prompt, which gives you root access and elevates your permission level.
4. Type `cd /etc/sf/license.d` to navigate to the controls license folder.
5. Type `cat *.lic` to display your entire license.

IMPORTANT Save the output of your controls license in a text file for later use.

Install the SFR 6.4.0 Update

Follow these instructions to install the SFR 6.4.0 update, which is completed entirely through CLI.

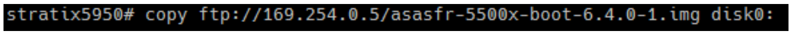
1. Log in to the console for the ASA.
2. Back up your SFR configuration.

   Updating SFR to 6.4 from 5.4 causes you lose the ability to have multiple policies. Therefore, you cannot back up from a file. Either record the current active policy to hard copy, or copy and paste the information electronically. Back up your rules through SFR in ASDM. To back up the network configuration, type `show module SFR`.

IMPORTANT Record the IP address, Network mask, Gateway, and NTP Server details as this process deletes that information. Otherwise, you are forced to regenerate the information.

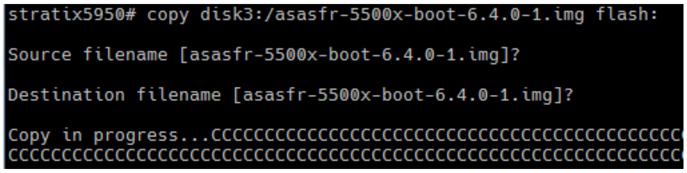
3. Copy the ASA SFR boot image to disk0 via FTP, HTTP, TFTP, or SD card.

Figure 30 - Example of Command to Copy Boot Image from FTP



```
stratix5950# copy ftp://169.254.0.5/asasfr-5500x-boot-6.4.0-1.img disk0:
```

Figure 31 - Example of Command to Copy Boot Image from SD Card



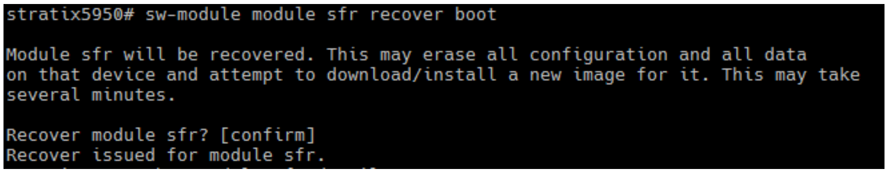
```
stratix5950# copy disk3:/asasfr-5500x-boot-6.4.0-1.img flash:

Source filename [asasfr-5500x-boot-6.4.0-1.img]?

Destination filename [asasfr-5500x-boot-6.4.0-1.img]?

Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
```

4. Once the image is copied to disk0, change the pointer and tell it to boot from that image:

   Type `sw-module module sfr recover configure image disk0:asasfr-5500x-boot-6.4.0-1.img`.

5. Boot the new image.

   You are prompted for confirmation.



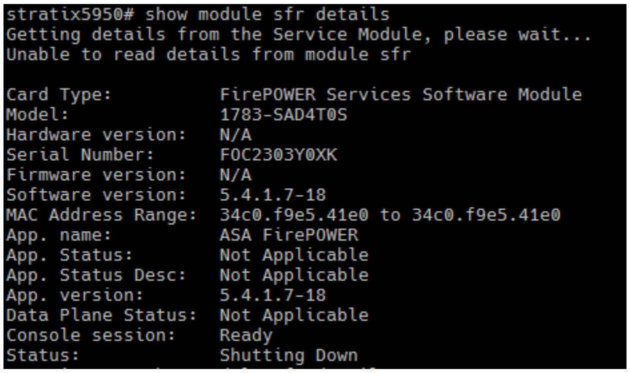
```
stratix5950# sw-module module sfr recover boot

Module sfr will be recovered. This may erase all configuration and all data
on that device and attempt to download/install a new image for it. This may take
several minutes.

Recover module sfr? [confirm]
Recover issued for module sfr.
```

6. To confirm that you want to recover the module, press Enter.

   The system begins to shut down.

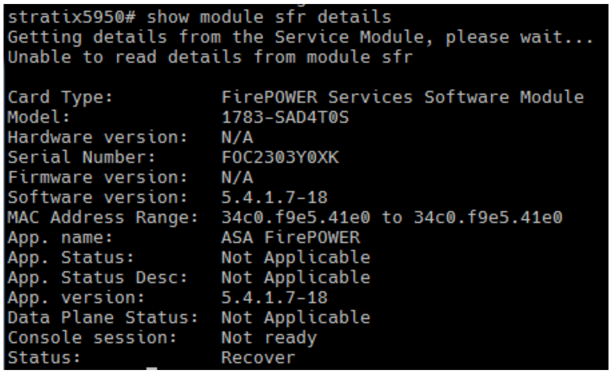
7. (Optional). If you issue a `show module sfr details` command, you see three states, depending on time elapsed:

   - Ready/Shutting Down indicates that this is the session/status lines.



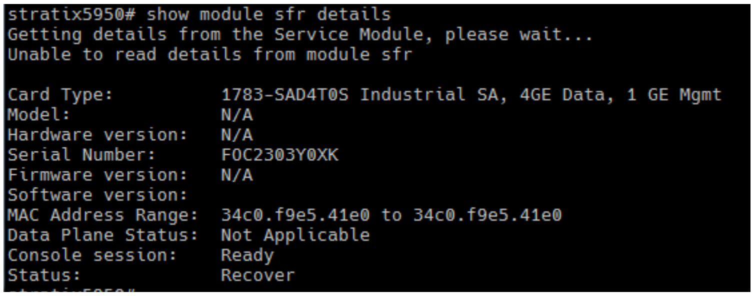
```
stratix5950# show module sfr details
Getting details from the Service Module, please wait...
Unable to read details from module sfr

Card Type:          FirePOWER Services Software Module
Model:              1783-SAD4T0S
Hardware version:   N/A
Serial Number:      FOC2303Y0XK
Firmware version:   N/A
Software version:   5.4.1.7-18
MAC Address Range:  34c0.f9e5.41e0 to 34c0.f9e5.41e0
App. name:          ASA FirePOWER
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       5.4.1.7-18
Data Plane Status:  Not Applicable
Console session:    Ready
Status:             Shutting Down
```

   - Not ready/Recover indicates that the device is booting.



```
stratix5950# show module sfr details
Getting details from the Service Module, please wait...
Unable to read details from module sfr

Card Type:          FirePOWER Services Software Module
Model:              1783-SAD4T0S
Hardware version:   N/A
Serial Number:      FOC2303Y0XK
Firmware version:   N/A
Software version:   5.4.1.7-18
MAC Address Range:  34c0.f9e5.41e0 to 34c0.f9e5.41e0
App. name:          ASA FirePOWER
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       5.4.1.7-18
Data Plane Status:  Not Applicable
Console session:    Not ready
Status:             Recover
```

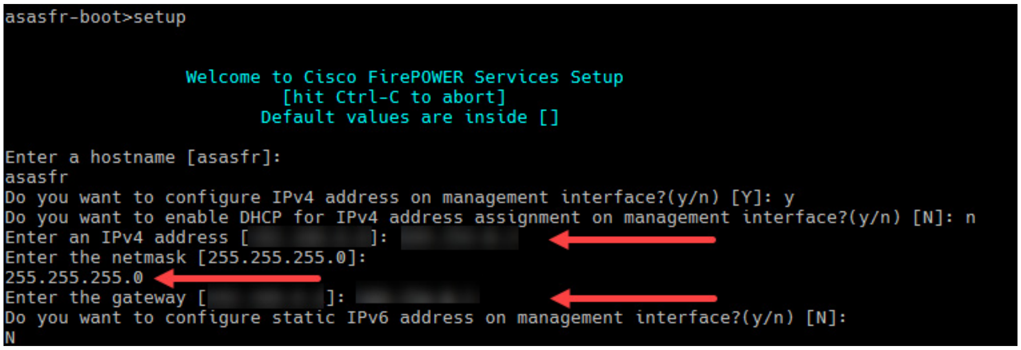
   - Ready/Recover indicates that the device is ready for a console session and to be configured



```
stratix5950# show module sfr details
Getting details from the Service Module, please wait...
Unable to read details from module sfr

Card Type:          1783-SAD4T0S Industrial SA, 4GE Data, 1 GE Mgmt
Model:              N/A
Hardware version:   N/A
Serial Number:      FOC2303Y0XK
Firmware version:   N/A
Software version:
MAC Address Range:  34c0.f9e5.41e0 to 34c0.f9e5.41e0
Data Plane Status:  Not Applicable
Console session:    Ready
Status:             Recover
```

The Ready/Recover status can take up to 5 minutes to display.

8. Type `Session SFR console`.
9. Log in with username=`admin`, password=`Admin123`. This installation is new, and it requires the default password. This password is changed in later steps.
10. Type `setup` to configure the SFR.
11. Type the IP address, Network mask, and Gateway details you recorded in step 1.



```
asasfr-boot>setup

                   Welcome to Cisco FirePOWER Services Setup
                             [hit Ctrl-C to abort]
                          Default values are inside []

Enter a hostname [asasfr]:
asasfr
Do you want to configure IPv4 address on management interface?(y/n) [Y]: y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [N]: n
Enter an IPv4 address [[redacted]]: [redacted]
Enter the netmask [255.255.255.0]:
255.255.255.0
Enter the gateway [[redacted]]: [redacted]
Do you want to configure static IPv6 address on management interface?(y/n) [N]:
N
```

12. When prompted to apply the changes, Type `y`.

    If you use a ping to validate your network connectivity, you must press CTRL-C to interrupt. Otherwise, it continues to ping.

13. At this point, copy over and install SFR (which takes 2 hours).
    This can be done from FTP, TFTP, or HTTP, but not from an SD card.
    The system indicates that it is verifying, downloading, and extracting, which takes a few minutes on a direct link.
    Type `system install noconfirm ftp://FTP_IP_ADDRESS/asasfr-sys-6.44.0-102.pkg`

    About 20 to 30 minutes into the two-hour process, the system indicates, “Finished extracting, will issue a reboot”.

IMPORTANT Do not power off your system. This restart is for the SFR side only.

The system upgrades and populates the new system image for about 20 minutes, and then there is another restart of the SFR.

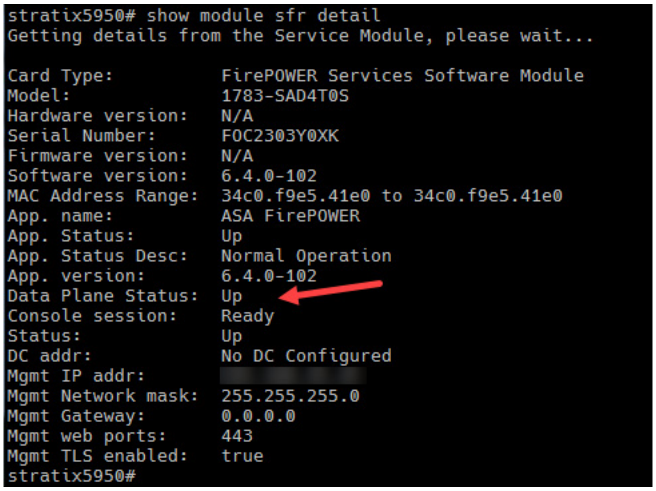
IMPORTANT Do not restart your system. This restart is for the SFR side only.

Another restart of the SFR occurs several minutes later. If you press a key, you receive a message that the system was terminated, and then the ASA command prompt returns. The system indicates “status up” when complete, usually about 2 hours.

IMPORTANT Do not power off the system during those 2 hours.

14. To return data, such as IP addresses, type `show module sfr detail`.

    Important data includes 'Data Plane Status: UP' and 'Console session: Ready'.



```
stratix5950# show module sfr detail
Getting details from the Service Module, please wait...

Card Type:          FirePOWER Services Software Module
Model:              1783-SAD4T0S
Hardware version:   N/A
Serial Number:      FOC2303Y0XK
Firmware version:   N/A
Software version:   6.4.0-102
MAC Address Range:  34c0.f9e5.41e0 to 34c0.f9e5.41e0
App. name:          ASA FirePOWER
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       6.4.0-102
Data Plane Status:  Up
Console session:    Ready
Status:             Up
DC addr:            No DC Configured
Mgmt IP addr:       [redacted]
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       0.0.0.0
Mgmt web ports:     443
Mgmt TLS enabled:   true
stratix5950#
```

15. To return to the SFR, type `session SFR console`.

    You are prompted for the username and password.

16. Log in with `username=admin`, `password=Admin123`.

    The EULA appears.

17. To advance screens, press the space bar.

18. To accept the EULA, press Enter.

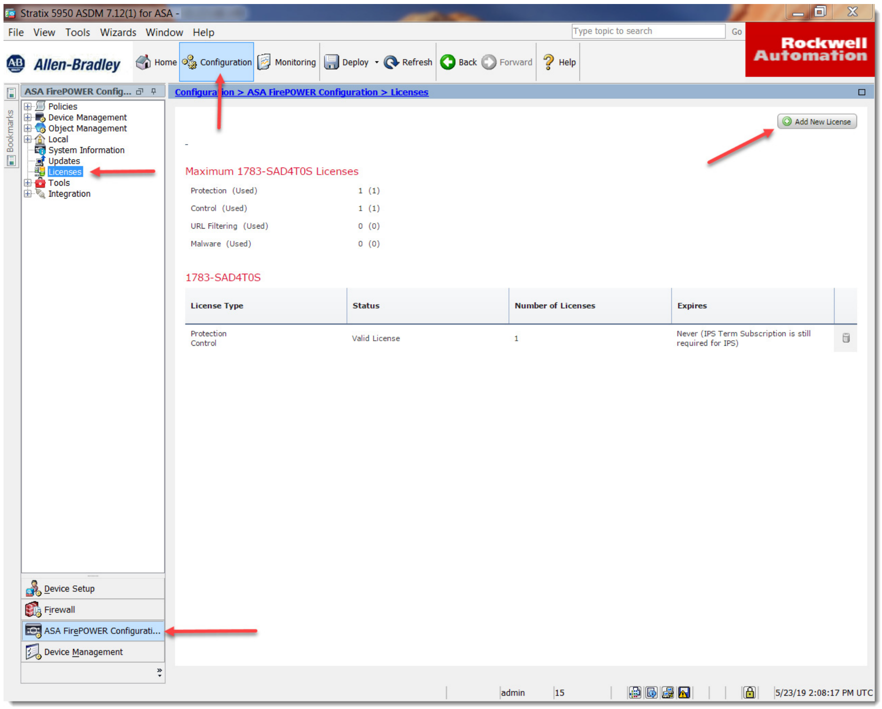
    The device prompts you to change the password and to enter the networking information recorded in Step 1. The settings are applied and the SFR is initially configured, which takes about 5 minutes. When complete, the carat prompt (>) for the SFR is displayed.

19. To return to ASA, press CTRL+SHIFT+6 and then X.

Restore the Controls License

To restore the controls license, follow these steps.

1. Log in to ASDM to reinstall the controls license and backed-up SFR policies from Back Up Controls License.
2. On the ASDM Home dialog, click Configuration > ASA FirePower Configuration > Licenses.



Maximum 1783-SAD4T0S Licenses

Protection (Used)	1 (1)
Control (Used)	1 (1)
URL Filtering (Used)	0 (0)
Malware (Used)	0 (0)

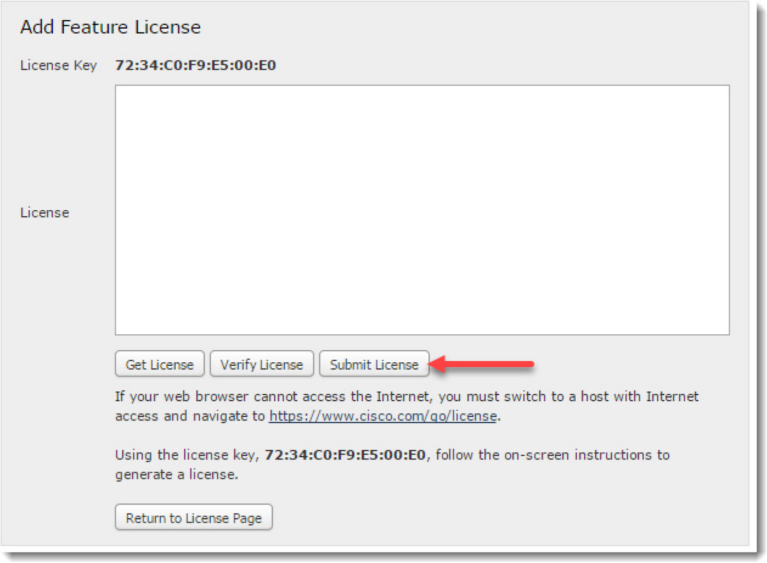
1783-SAD4T0S

License Type	Status	Number of Licenses	Expires
Protection Control	Valid License	1	Never (IPS Term Subscription is still required for IPS)

3. Click Add New License.
4. Paste the license that you copied in Back Up Controls License.

IMPORTANT If you did not back up the controls license, contact Rockwell Automation technical support for a replacement license. It could take multiple days to receive a replacement license.

5. Click Submit License.



Add Feature License

License Key 72:34:C0:F9:E5:00:E0

License

If your web browser cannot access the Internet, you must switch to a host with Internet access and navigate to https://www.cisco.com/go/license.

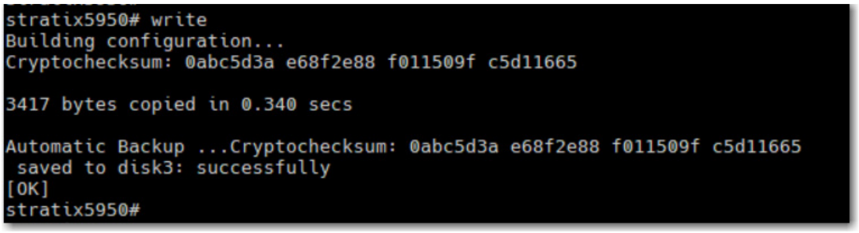
Using the license key, 72:34:C0:F9:E5:00:E0, follow the on-screen instructions to generate a license.

The device loads the license and indicates "Success: Successfully Saved License". If necessary, contact the Rockwell Automation Support Site for assistance.

Upgrade the Bootloader

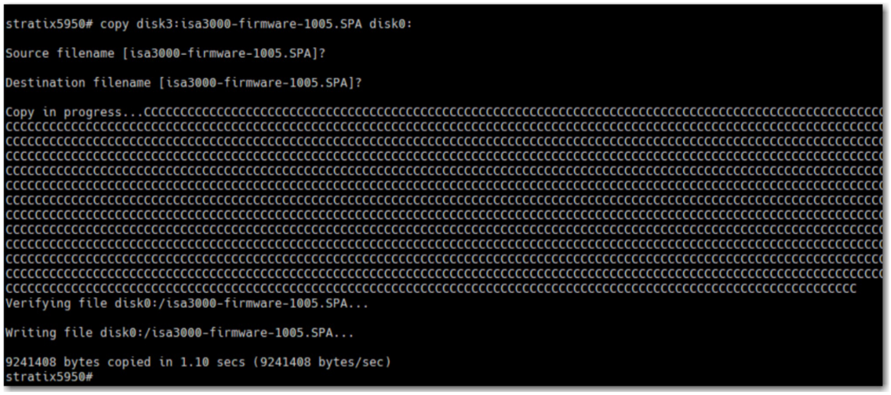
To install Bootloader 1.0.5, follow these steps via the CLI:

1. Log in to the CLI console for the ASA.
2. Save your configuration by issuing a write command.



```
stratix5950# write
Building configuration...
Cryptochecksum: 0abc5d3a e68f2e88 f011509f c5d11665

3417 bytes copied in 0.340 secs

Automatic Backup ...Cryptochecksum: 0abc5d3a e68f2e88 f011509f c5d11665
 saved to disk3: successfully
[OK]
stratix5950#
```

3. Copy the bootloader image to disk0 via FTP, HTTP, TFTP, or SD card.



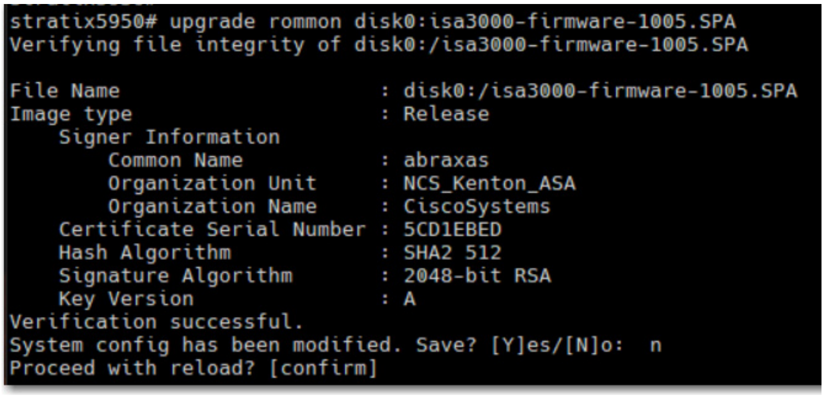
```
stratix5950# copy disk3:isa3000-firmware-1005.SPA disk0:

Source filename [isa3000-firmware-1005.SPA]?

Destination filename [isa3000-firmware-1005.SPA]?

Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying file disk0:/isa3000-firmware-1005.SPA...

Writing file disk0:/isa3000-firmware-1005.SPA...

9241408 bytes copied in 1.10 secs (9241408 bytes/sec)
stratix5950#
```

4. Once the file is coped to disk0, execute the following command to begin the upgrade procedure:

   upgrade rommon disk0:isa3000-firmware-1005.SPA

5. When prompted, do not save the configuration.

6. When prompted to proceed with the reload, press Enter.

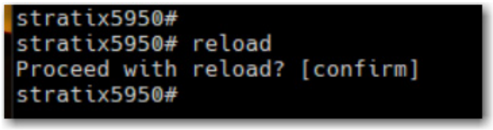
   ```
   stratix5950# upgrade rommon disk0:isa3000-firmware-1005.SPA
   Verifying file integrity of disk0:/isa3000-firmware-1005.SPA

   File Name                      : disk0:/isa3000-firmware-1005.SPA
   Image type                     : Release
       Signer Information
           Common Name            : abraxas
           Organization Unit      : NCS_Kenton_ASA
           Organization Name      : CiscoSystems
       Certificate Serial Number : 5CD1EBED
       Hash Algorithm             : SHA2 512
       Signature Algorithm        : 2048-bit RSA
       Key Version                : A
   Verification successful.
   System config has been modified. Save? [Y]es/[N]o:  n
   Proceed with reload? [confirm]
   ```

   The device restarts and begins the upgrade process for the rommon bootloader.

   IMPORTANT Do not restart the device during the upgrade process.

7. Once the upgrade is complete and the device returns to the ASA login prompt, log in and restart the device by issuing a reload command.

8. To confirm the reload, press Enter.

   ```
   stratix5950#
   stratix5950# reload
   Proceed with reload? [confirm]
   stratix5950#
   ```

Notes:

Troubleshoot

Obtain the Current Running Software Versions

Before troubleshooting, make sure you know the latest information about the software versions your system is running. You must provide this information when you contact customer support.

1. To use the ASDM method, follow these steps.

   a. Log in to ASDM.
   b. Go to ASDM > Home > Device Dashboard >Device Information.
   c. Record the ASA version.
   d. Record the ASDM version.
   e. Go to ASDM > Home > ASA FirePOWER Status > Module Information.
   f. Record the Software Version.

2. If the ASDM method does not work, use the following ASA console method.

   a. Log in to ASA console.
   b. Enter **stratix5950>enable**.
   c. Enter **stratix5950# show version**.
   d. Record the version for Cisco® ASA software.
   e. Record the version for Device Manager.
   f. Enter **stratix5950# show module sfr**.
   g. Record the SSM application version.

Reset the Device to Factory Defaults

WARNING: Only complete this procedure when required and requested by Rockwell Automation Technical Support. This procedure can take at least 10 hours of interactive time to perform.

This procedure is based on the following assumptions and performed with the following versions of Cisco software.

The procedures are based on instructions from the Cisco website:

https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configure-firepower-00.html

This procedure does not perform a true factory reset, but it installs the same software that was included out-of-box.

Software

- ASA: asa962-lfbff-k8.SPA
- ASDM: asdm-76267.bin
- FirePOWER: Cisco_Network_Sensor_Patch-5.4.1.7-18.sh

Prerequisites

The following are prerequisites that are required to get the same results:

- Personal computer supported by ASDM.

  For example, Windows 7.

- An FTP server installed.

  For example, FileZilla (https://filezilla-project.org/download.php?type=server)

- SFR files to restore with:
  a. asasfr-sys-5.4.1-213.pkg
  b. asasfr-5500x-boot-5.4.1-213.img
  c. Cisco_Network_Sensor_Patch-5.4.1.2-23.sh
  d. Cisco_Network_Sensor_Patch-5.4.1.4-15.sh
  e. Cisco_Network_Sensor_Patch-5.4.1.6-37.sh
- Start FTP server, with asasfr-sys-5.4.1-213.pkg and asasfr-5500x-boot-5.4.1-213.img in the root directory
- Serial cable, DB9-to-RJ45
- 2x IP addresses on same network as FTP server:
  - ASA IP address
  - SFR IP address

Hardware Setup

The following list is the hardware preparation that was designed for this example.

1. Set NIC on the computer to DHCP.
2. Connect the management interface cable on the Stratix® 5950 security appliance to NIC on computer.
3. Connect serial cable from console port on Stratix 5950 appliance to serial port on the computer.
4. Plug in the Stratix 5950 appliance and apply power.
5. Hold in Express Setup button for 5 seconds.

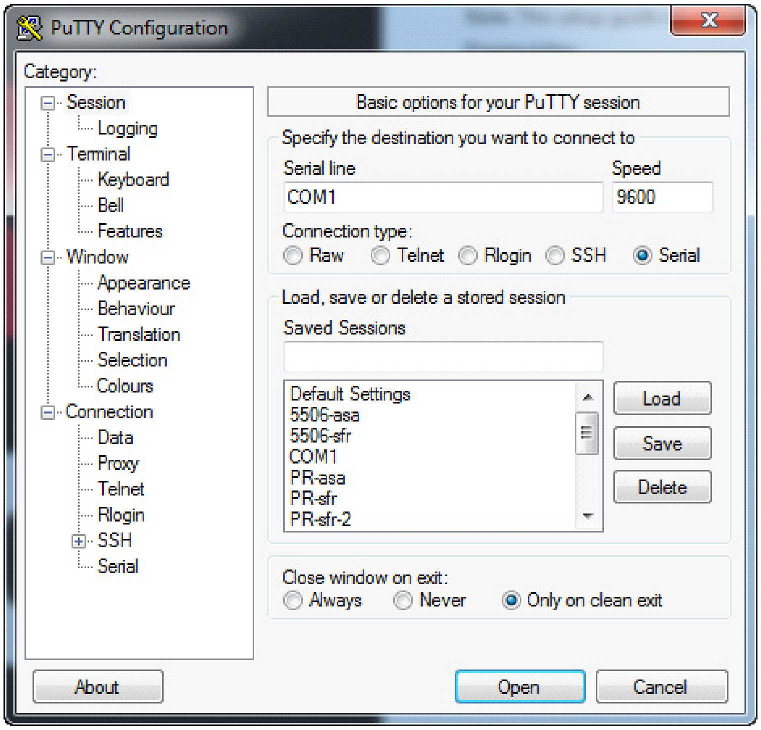
   This action reloads the ASA configuration and reboots the device.

6. Wait 5 minutes for the device to restart.

Uninstall an Old SFR Module

Follow these steps to uninstall an old SFR module.

1. Use PuTTY to connect to the serial port of the device.



Specify the destination you want to connect to

Serial line: COM1

Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

Saved Sessions

Default Settings
5506-asa
5506-sfr
COM1
PR-asa
PR-sfr
PR-sfr-2

Close window on exit: ○ Always ○ Never ● Only on clean exit

2. Enter **stratix5950> enable**.
3. Press Enter when prompted for “Password.”
4. Enter **stratix5950(config)# configure terminal**.

5. At the prompt, Would you like to enable anonymous error reporting to help improve the product?, enter **N**.
6. Enter the following commands:

```
stratix5950(config)# enable password
<YOUR_ENABLE_PASSWORD>

stratix5950(config)# interface Management1/1

stratix5950(config-if)# ip address
<ASA_IP_ADDRESS> <ASA_NETMASK>

stratix5950(config)# http <ASA_IP_ADDRESS>
<ASA_NETMASK> management

stratix5950(config)# wr

copy ftp://
FTP_USERNAME:FTP_PASSWORD@FTP_IP_ADDRESS/
asasfr-5500x-boot-5.4.1-213.img disk0:

stratix5950(config-if)# dir
```

7. Confirm that asasfr-5500x-boot-5.4.1-213.img is listed.
8. Enter **stratix5950(config-if)# sw-module module sfr shutdown**.
9. Wait until SFR module status shows “Down” by running “`how module sfr`”
10. Enter **stratix5950(config-if)# sw-module module sfr uninstall**
11. Enter **stratix5950(config-if)# reload**
12. Wait 5 minutes until the system restarts.

Reinstall an SFR Module

Follow these steps to reinstall an SFR module from the command line.

1. Enter **stratix5950> enable.**
2. Set the current time:

   stratix5950# clock set 14:28:00 16 March 2016
3. Enter **stratix5950# sw-module module sfr recover configure image disk0:asasfr-5500x-boot-5.4.1-213.img**.
4. Enter **sw-module module sfr recover boot**.
5. When the console is ready, enter **show module sfr details**.
6. Wait until the "Console session:" shows "Ready"
7. Enter **stratix5950# session sfr console**.
8. Log in with: username=admin, password=Admin123
9. Enter **asasfr-boot>setup**.

10. Complete the steps with the networking information for the SFR IP address.

11. Enter **system install noconfirm ftp://FTP_IP_ADDRESS/asasfr-sys-5.4.1-213.pkg**

    Enter the username/password, and the system begins to download the package. It shows 'Download...'

    After the package is downloaded, it takes about 60 minutes to complete the following steps.

    a. Extracting
    b. Upgrading
    c. Starting upgrade process
    d. Populating new system image
    e. The system is going down for reboot

    After the system reboots, wait another 60 minutes until 'show module sfr' shows that the status is 'Up'.

12. Enter **stratix5950(config)# session sfr console.**

13. Log in with username = admin, password = Sourcefire.

14. Accept the EULA when prompted.

15. Change the admin password when prompted.

16. Change the networking settings to the SFR IP address.

17. Wait until this step completes: 'Applying 'Default Allow All Traffic' access control policy.'

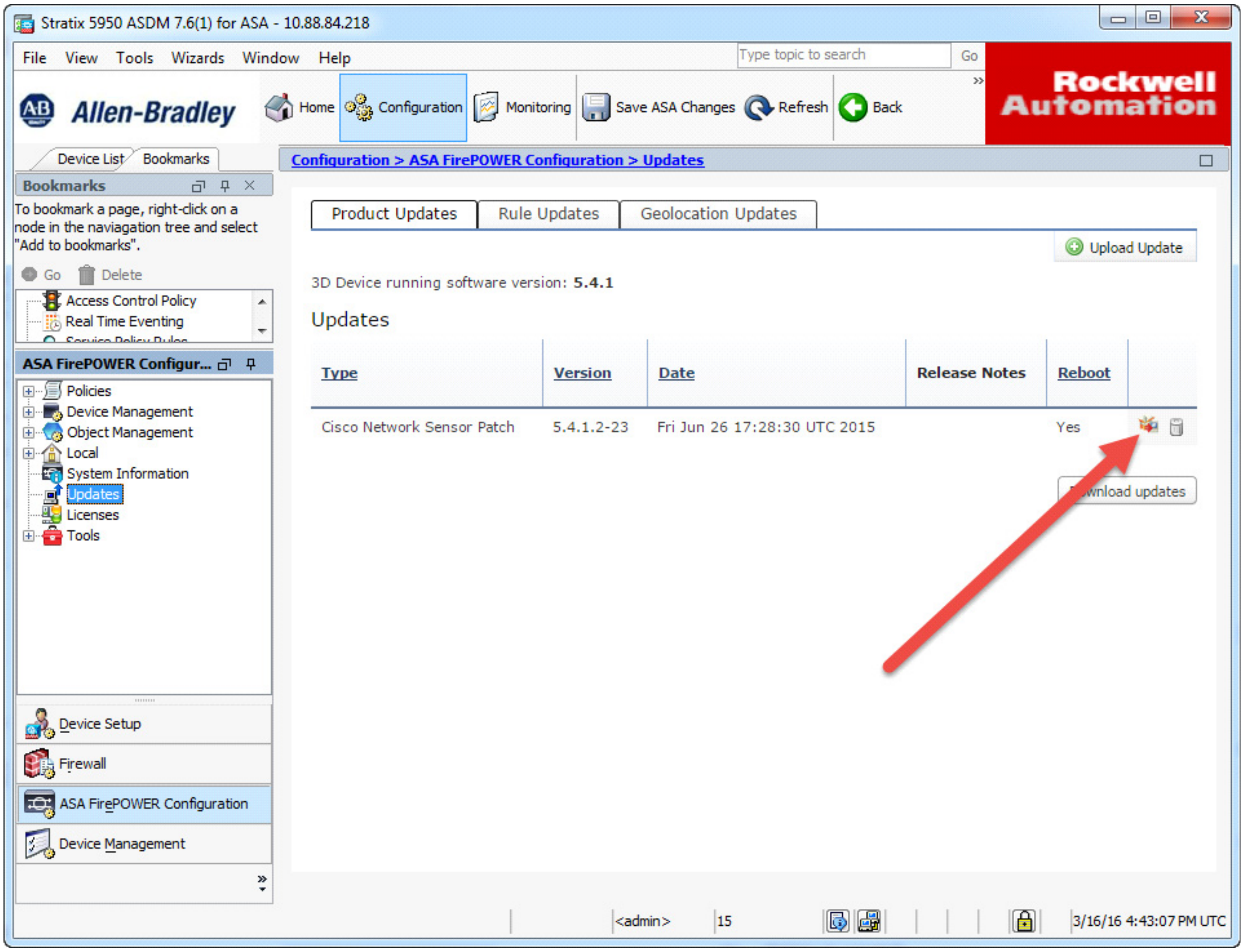
Install the SFR 5.4.1.2 Update

Follow these steps to install the SFR 5.4.1.2 update. Only do perform this update if you are running the 5.4 branch and you do not want to run 6.4. However, we recommended you update to 6.4.

1. Log in to ASDM, by going to:

   https://ASA_IP_ADDRESS/admin/public/index.html

2. Select Run ASDM.
3. Log in with the ASA enable password that you set earlier.
4. ASDM > Configuration > ASA FirePOWER Configuration > Updates -> Upload Update.
5. Select Cisco_Network_Sensor_Patch-5.4.1.2-23.sh.
6. After the file uploads, install the update.



Bookmarks

To bookmark a page, right-click on a node in the naviagation tree and select "Add to bookmarks".

Configuration > ASA FirePOWER Configuration > Updates

3D Device running software version: **5.4.1**

Updates

Type	Version	Date	Release Notes	Reboot
Cisco Network Sensor Patch	5.4.1.2-23	Fri Jun 26 17:28:30 UTC 2015		Yes

7. Wait 2 hours.
8. Exit ASDM.

Install the SFR 5.4.1.4 Update

Follow these steps to install the SFR 5.4.1.4 update. Only perform this step if you are running the 5.4 branch and you do not want to run version 6.4. However, we recommend that you install version 6.4.

1. Log in to ASDM.
2. Go to ASDM > Monitoring >ASA FirePOWER Monitoring > Task Status. Confirm that the previous patch that was being installed is now "Completed".
3. Go to ASDM > Configuration > ASA FirePOWER Configuration > Updates > Upload Update.
4. Select Cisco_Network_Sensor_Patch-5.4.1.4-15.sh.
5. After the file uploads, install the update.
6. Wait 2 hours.
7. Exit ASDM.

Install SFR 5.4.1.6 Update

Follow these steps to install the SFR 5.4.1.6 update. Only perform this step if you are running the 5.4 branch and you do not want to run version 6.4. However, we recommend that you install version 6.4.

1. Log in to ASDM.
2. Go to ASDM > Monitoring > ASA FirePOWER Monitoring > Task Status.
3. Confirm that the previous patch that was being installed is now "Completed".
4. Go to ASDM > Configuration > ASA FirePOWER Configuration > Updates > Upload Update.
5. Select Cisco_Network_Sensor_Patch-5.4.1.6-37.sh.
6. After the file uploads, install the update.
7. Wait 2 hours.
8. Exit ASDM.

Final Reset

Follow these steps to perform a final reset on the system.

1. Log in to ASA CLI.
2. Enter the following commands:

   ```
   stratix5950> enable
   stratix5950# configure terminal
   stratix5950(config)# configure factory-default
   stratix5950(config)# wr
   ```
3. Unplug power to device.

Glossary

The following terms and abbreviations are used throughout this manual. For definitions of terms not listed here, refer to the Allen-Bradley Industrial Automation Glossary, publication AG-7.1.

ASA Adaptive security appliance

ASDM Cisco device management software for ASA platform

Bypass Relay Bypass relay is used when there is a loss of power or under software control. Two cases trigger a bypass, a power failure of the system or you enable the bypass through a CLI command.

CIP Common Industrial Protocol

CLI Command-line interface

Clientless SSL Helps ensure secure access to pre-configured network resources on a corporate network using an SSL-enabled web browser.

CPwE architecture Converged Plantwide Ethernet (CPwE) is a collection of tested and validated architectures that are developed by subject matter authorities at Cisco and Rockwell Automation® which follows the Cisco Validated Design (CVD) program.

CSM: Cisco Security Management System The Cisco Security Manager (CSM) provides scalable, centralized management for the firewall component of the IFW.

CSM Version 4.11 The Stratix 5950 security appliance is a joint technology collaboration with Cisco. You can leverage the CSM and FireSIGHT Management Center Cisco software bundles with this device.

DHCP Dynamic Host Configuration Protocol

DIN Rail A metal rail of a standard type that is widely used for mounting circuit breakers and industrial control equipment inside equipment racks.

EIP ModStatus The System status indicator shows the power status of the appliance.

FireSIGHT Management Center Version 5.4.1.6 The Cisco FireSIGHT Management Center manages the FirePOWER module of the IFW.

Firewall Firewalls are used to separate networks with differing security requirements, such as the Enterprise zone and the Industrial Zone.

Internet Protocol (IP) Internet Protocol Common protocol used in conjunction with Ethernet, commonly used with the Internet. It is the protocol used for forwarding packets on a network.

IP/Sec IPSec is a standard set of protocols that provide data security at the IP packet level.

Intrusion Prevention System (IPS) IPS is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

K9 License A web-based filtering technology that provides automatic updates when you need a robust, real-time solution.

Management Information Base (MIB) is a database used for managing the entities in a communication network. Most often associated with the Simple Network Management Protocol (SNMP), the term is also used more generically in contexts such as in OSI/ISO Network management model.

Secure Digital (SD) Secure Digital memory card format developed by the SD Card Association (SDA) for use in portable devices.

Simple Network Management Protocol (SNMP) SNMP is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

SSL VPN Allows for the creation of a secure, encrypted connection without requiring specialized software on an end user’s computer.

System On Chip (SoC) A system on a chip or system on chip (SoC or SOC) is an integrated circuit (IC) that integrates all components of a computer or other electronic system into a single chip.

TA License Helps provide increased control and protection during system updates.

Virtual Private Network (VPN) VPN is a virtual version of a secure, physical network.

Rockwell Automation Support

Use the following resources to access support information.

Technical Support Center	Knowledgebase Articles, How-to Videos, FAQs, Chat, User Forums, and Product Notification Updates.	https://rockwellautomation.custhelp.com/
Local Technical Support Phone Numbers	Locate the phone number for your country.	http://www.rockwellautomation.com/global/support/get-support-now.page
Direct Dial Codes	Find the Direct Dial Code for your product. Use the code to route your call directly to a technical support engineer.	http://www.rockwellautomation.com/global/support/direct-dial.page
Literature Library	Installation Instructions, Manuals, Brochures, and Technical Data.	http://www.rockwellautomation.com/global/literature-library/overview.page
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	http://www.rockwellautomation.com/global/support/pcdc.page

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the How Are We Doing? form at http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf.

Rockwell Automation maintains current product environmental information on its website at http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1783-UM010D-EN-P - October 2019
Supersedes Publication 1783-UM010C-EN-P - June 2019