Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date September 30, 2019

Original Release Date May 28, 2019

Superseding Document

Status Final

Series/Number NIST Interagency or Internal Report (NISTIR) 8183A Volume 2

Title Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 2 – Process-based Manufacturing System Use Case

Publication Date September 2019

DOI https://doi.org/10.6028/NIST.IR.8183A-2

CSRC URL https://csrc.nist.gov/publications/detail/nistir/8183a/vol-2/final

Additional Information

National Institute of Standards and Technology
U.S. Department of Commerce

DRAFT NISTIR 8183A
Volume 2

Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide:
Volume 2 – Process-based Manufacturing System Use Case

Keith Stouffer
Timothy Zimmerman
CheeYee Tang
Jeffrey Cichonski
Neeraj Shah
Wesley Downard

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183A-2-draft

National Institute of Standards and Technology
U.S. Department of Commerce

DRAFT NISTIR 8183A Volume 2

Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide:

Volume 2 – Process-based Manufacturing System Use Case

Keith Stouffer
Timothy Zimmerman
CheeYee Tang
Intelligent Systems Division
Engineering Laboratory

Neeraj Shah
Strativia, LLC
Largo, Maryland

Jeffrey Cichonski
Applied Cybersecurity Division
Information Technology Laboratory

Wesley Downard
G2, Inc.
Annapolis Junction, Maryland

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183A-2-draft

May 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Internal Report 8183A, Volume 2
401 pages (May 2019)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183A-2-draft

Public comment period: *May 28, 2019* through *July 8, 2019*

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: CSF_Manufacturing_Profile_Implementation@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This guide provides example proof-of-concept solutions demonstrating how open-source and commercial off-the-shelf (COTS) products that are currently available today can be implemented in process-based manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile [4] Low Security Level. The example proof-of-concept solutions include measured network, device, and operational performance impacts observed during the implementation. Depending on factors like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they may voluntarily implement. The CSF Manufacturing Profile can be used as a roadmap for managing cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry best practices. The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to compliment but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

Keywords

Computer security; Cybersecurity Framework (CSF); distributed control systems (DCS); industrial control systems (ICS); information security; manufacturing; network security; programmable logic controllers (PLC); risk management; security controls; supervisory control and data acquisition (SCADA) systems.

Supplemental Content

Additional volumes of this publication include:

Draft NISTIR 8183A Volume 1, *Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide: Volume 1 – General Implementation Guidance.* https://doi.org/10.6028/NIST.IR.8183A-1-draft

Draft NISTIR 8183A Volume 3, *Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide: Volume 3 – Discrete-based Manufacturing System Use Case.* https://doi.org/10.6028/NIST.IR.8183A-3-draft

Acknowledgments

The authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication. A special acknowledgement to the members of the ISA99, Industrial Automation and Control Systems Security Committee and the Department of Homeland Security Industrial Control System Joint Working Group (ICSJWG) for their exceptional contributions to this publication.

Note to Reviewers

This guide does not describe the solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to CSF_Manufacturing_Profile_Implementation@nist.gov.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

i) under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

ii) without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: CSF_Manufacturing_Profile_Implementation@nist.gov

Table of Contents

210

Executive Summary

This guide provides example proof-of-concept solutions demonstrating how open-source and commercial off-the-shelf (COTS) products that are currently available today can be implemented in process-based manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile [4] Low Security Level. The example proof-of-concept solutions include measured network, device, and operational performance impacts observed during the implementation. Depending on factors like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they may voluntarily implement.

The CSF Manufacturing Profile can be used as a roadmap for managing cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry best practices. The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to compliment but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

The CSF Manufacturing Profile focuses on desired cybersecurity outcomes and can be used as a roadmap to identify opportunities for improving the current cybersecurity posture of the manufacturing system. The Manufacturing Profile provides a prioritization of security activities to meet specific business/mission goals. Relevant and actionable security practices that can be implemented to support key business/mission goals are then identified.

While the proof-of-concept solutions in this guide used a suite of commercial products, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Each organization's information security experts should identify the products that will best integrate with their existing tools and manufacturing system infrastructure. Organizations may voluntarily adopt these solutions or one that adheres to these guidelines in whole, or can use this guide as a starting point for tailoring and implementing parts of a solution. This guide does not describe regulations or mandatory practices, nor does it carry any statutory authority.

1. Introduction

The Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," [1] directed the development of the voluntary Cybersecurity Framework that provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risk [1] for those processes, information, and systems directly involved in the delivery of critical infrastructure services.

The Cybersecurity Framework is a voluntary risk-based assemblage of industry standards and best practices designed to help organizations manage cybersecurity risks [2]. The Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without imposing additional regulatory requirements.

To address the needs of manufacturers, a Manufacturing Profile [4] of the Cybersecurity Framework was developed, through collaboration between government and the private sector, to be an actionable approach for implementing cybersecurity controls into a manufacturing system and its environment. The Profile defines specific cybersecurity activities and outcomes for the protection of the manufacturing system, its components, facility, and environment. Through use of the Profile, the manufacturer can align cybersecurity activities with business requirements, risk tolerances, and resources. The Profile provides a manufacturing sector-specific approach to cybersecurity from standards, guidelines, and industry best practices.

1.1 Purpose and Scope

Many small and medium sized manufacturers have expressed that they are challenged in implementing a standards-based cybersecurity program. This guide provides example proof-of-concept solutions demonstrating how open-source and commercial off-the-shelf (COTS) products that are available today can be implemented in manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile Low Security Level. Example proof-of-concept solutions with measured network, device, and operational performance impacts for a process-based manufacturing environment (Volume 2) and a discrete-based manufacturing environment (Volume 3) are included in the guide. Depending on factors like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they may voluntarily implement. The CSF Manufacturing Profile can be used as a roadmap for managing cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry best practices. The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to enhance but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

While the proof-of-concept solutions in this guide used a suite of commercial products, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Each organization's information security experts should identify the products that will best integrate with their existing tools and manufacturing system

infrastructure. Organizations may voluntarily adopt these solutions or one that adheres to these guidelines in whole, or can use this guide as a starting point for tailoring and implementing parts of a solution. This guide does not describe regulations or mandatory practices, nor does it carry any statutory authority.

This project is guided by the following assumptions: The solutions were developed in a lab environment. The environment is based on a typical small manufacturer. The environment does not reflect the complexity of a production environment. An organization can access the skills and resources required to implement a manufacturing cybersecurity solution.

1.2 Audience

This document covers details specific to manufacturing systems. Readers of this document should be acquainted with operational technology, general computer security concepts, and communication protocols such as those used in networking. The intended audience is varied and includes the following:

- Control engineers, integrators, and architects who design or implement secure manufacturing systems.
- System administrators, engineers, and other information technology (IT) professionals who administer, patch, or secure manufacturing systems.
- Managers who are responsible for manufacturing systems.
- Senior management who are trying to understand implications and consequences as they justify and implement a manufacturing systems cybersecurity program to help mitigate impacts to business functionality.
- Researchers, academic institutions and analysts who are trying to understand the unique security needs of manufacturing systems.

1.3 Document Structure

Volume 2 is divided into the following major sections:

- Section 2 provides an overview of the process-based manufacturing system use case.
- Section 3 provides the detailed policy and procedure documents developed for the process-based manufacturing system use case.
- Section 4 provides the detailed technical capability implementations and associated performance measurements for the process-based manufacturing system use case.
- Appendix A provides a list of acronyms and abbreviations used in this document.
- Appendix B provides a glossary of terms used in this document.
- Appendix C provides a list of references used in the development of this document.

2. Process-based Manufacturing System Low Security Level Use Case

2.1 Introduction

This use case is a proof-of-concept solution demonstrating how open-source and commercial off-the-shelf (COTS) products that are currently available today can be implemented in a manufacturing environment to satisfy the requirements in the CSF Manufacturing Profile Low Security Level. Depending on factors like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their own determinations about the breadth of proof-of-concept solution they may voluntarily implement.

2.2 Process-based Low Security Level Use Case

The fictional company, Westman Chemical (i.e. Westman), is a chemical manufacturer producing commercial grade chemical products for use in the transportation, building and construction, and other industrial products. It is headquartered in Westland, a city with population of about 100,000 people.

Westman operates its manufacturing facility 24 hours per day, 7 days per week (24/7), with the exception of a schedule maintenance shutdown for about 2 weeks every year, typically scheduled at the end of December.

To increase industrial competitiveness, Westman has introduced process automation equipment to improve the production efficiency and to lower production costs. Industrial automation equipment like programmable logic controllers (PLC), human-machine-interfaces (HMI), and data historians are deployed in the factory to monitor and control the production operation.

2.2.1 Mission

To supply high quality chemical products for industrial application.

2.2.2 Facility

Westman facility is a single building about 50,000 square foot, with about 35,000 square foot of manufacturing space which includes the production space, a distribution facility, and several above ground chemical storage tanks. The remainder of the facility contains the administrative and engineering office space.

The perimeter of the facility is fenced, and the main entrance has gate that is open during business hours and is locked after hours. There are two entrances to the main building. One is for employee's access and is protected by a badge access system. Employees must swipe their assigned badge to enter the building. The other entrance is located at the front lobby, staffed by a receptionist during normal business hours. Guests and visitors are required to sign in and receive proper identification before entering the building or facility. The Westman facility does not have any contracted security guards at the gate or entrances.

2.2.3 Employees

Westman Chemical has 200 full-time employees, with most of the employees working on the manufacturing floor. A small team of full-time manufacturing/control engineers responsible for the manufacturing, control and automation equipment controlling manufacturing process. Their mission is to ensure the safe and efficient operation of the production system.

Westman also has a small team of full-time IT personnel responsible for the enterprise IT systems.

Westman Management position and responsibility:

Westman Management	Major Responsibility
CEO/General Manager	Oversight of the company
Director of Operations	Oversight of manufacturing operations. Management of the manufacturing staff and control engineers. Reports to the CEO/General Manager.
Director of Product Development	Oversight of product development. Management of the on-site chemists. Reports to the CEO/General Manager.
Director of Marketing	Oversight of marketing and sales. Reports to the CEO/General Manager.
Controller/Finances	Manager of finance staff. Reports to the CEO/General Manager.
General Counsel	Handles all legal matters. Reports to the CEO/General Manager.
IT Manager	Manager of IT staff. Reports to the CEO/General Manager.
HR Manager	Manager of human resources staff. Reports to the CEO/General Manager.

2.2.4 Supply Chain

Raw materials are utilized continuously to support the continuous operation of the manufacturing process. Raw materials are typically supplied through a long-term contract established with suppliers and are transported to the facility on a regular basis.

The end products are typically sold to customers in large quantity. Delivery is sub-contracted to several logistics companies which will handle the transportation from the Westman facility to the end customers. Westman's products are typically used as raw materials or additives in chemical processes performed by other industrial manufacturers.

2.2.5 Supporting Services

The supporting services required by Westman are electricity, natural gas, water, and Internet. The broadband Internet connection is a business class service provided by a large national provider with business class service level agreement.

2.2.6 Legal and Regulatory Requirements

As a chemical manufacturer, Westman and its employees are required to comply with all federal and state legal and regulatory requirements for chemical and hazardous materials. Westman is also required to comply with all legal, regulatory and safety requirements.

2.2.7 Critical Infrastructure

The chemical sector is considered as a critical infrastructure under the Presidential Policy Directive 21 (PPD-21).

2.2.8 Manufacturing Process

The manufacturing system consists of five major chemical processing components: a reactor, a product condenser, a vapor-liquid separator, a recycle compressor, and a product stripper to separate the end products. The manufacturing system has 12 valves for controlling the flow of chemicals through the system, and 41 sensor measurements for monitoring the chemical process. All valves and sensors are connected to the automation equipment (PLCs) through a DeviceNet communications bus. Valves are equipped with manual overrides, enabling workers to override the automation equipment during an emergency.

Raw materials are fed to the reactor where the materials are mixed and the main reaction takes place. Output from the reactor flows downstream to the product condenser and the vapor-liquid separator. Any output from the reactor still in the gaseous form is recycled through a compressor and fed back into the main reactor. All condensed components continuously flow to the product stripper separate the components into the final products. Quality assurance samples are taken at various stage of the process to validate the product quality and process efficiency.

2.2.9 Systems

The administrative office is supported by a small team of IT personnel mainly using general enterprise IT applications (e.g., email, web applications, and enterprise planning applications).

The IT personnel maintains a central file storage that is used to store source code, chemical formulas, drawings, procedures, and diagrams, and is backed up regularly. The product development staff and the manufacturing engineers are authorized to access this storage.

The IT personnel also installed and configured a Historian database on the manufacturing floor to record manufacturing process data. IT personnel is responsible for regular data backup of the Historian, and the manufacturing engineers are responsible for the configuration and operation of the Historian.

2.2.10 Data

Data transferred over, or stored within the company network include:

- PLC program code
- Chemical formulas and calculations
- Workflow and operating manuals and documentation
- Electrical diagrams
- Network diagrams
- Quality Assurance procedures
- Historical production data

NOTE: All data listed above are considered to be proprietary, trade secrets, and/or confidential.

2.2.11 Network

The IT systems within the administrative offices are connected to the corporate network, which is managed by the IT team. The manufacturing floor has a separate network for automation equipment and is managed by the manufacturing engineers.

The manufacturing network consists of a typical Ethernet based TCP/IP network and other industrial protocols, e.g., DeviceNet.

Some of the production equipment vendors required Westman to provide remote access to the equipment. The remote access allows the authorized vendors to connect to the manufacturing equipment to provide maintenance and support.

2.2.12 Mission Objectives

Maintain Personnel Safety

Westman commits to safe operation of the manufacturing system and to always put personnel safety as its highest priority. All manufacturing process, protocols, automation process and equipment, operating procedures and guidelines are designed to ensure personnel safety.

Maintain Environmental Safety

Westman complies to all applicable regulations regarding environment safety. Westman is committed to ensuring environmentally-friendly operation of its manufacturing process and working to reduce its environment footprint. Environmental impact caused by the manufacturing process is measured and reviewed on a quarterly basis.

Maintain Quality of Product

Westman has a world-class manufacturing facility and process. It has employed state of the art automation, equipment, and techniques to ensure the high quality of its product. It has developed a quality assurance program using automation equipment, including PLCs, Historian, and high precision sensors operating on a high-speed control network to monitor product quality.

Maintain Production Goals

Meeting the monthly production goals is an important objective for Westman, and ensures the supply of products to its customers in a timely fashion. It also maintains financial stability for Westman.

Constant 24/7 production enables Westman to plan its manufacturing operation to meet its production goals and customer demand. The investment in automation equipment and skilled professional assists Westman to maintain the monthly production goals.

Protect Trade Secrets

Westman is committed to protecting its trade secrets, including product development, manufacturing processes, product quality, and supply chain management.

3. Policy and Procedure Implementations

This section includes example policy and procedure documents and statements that were developed for the fictional company Westman. Each organization's information security experts should identify the policy and procedure documents and statements that will best integrate with their existing cybersecurity program and manufacturing system infrastructure.

3.1 Security Program Document Example

Security Program

for

Westman

Document Owner:	Director of Operations, Westman

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	CEO		4-22-2018
	Legal Counsel		4-23-2018

3.1.1 Purpose

The Information Security Program establishes guidelines and principles for initiating, implementing, maintaining, and improving cybersecurity management for Westman.

This program is designed to:

- Ensure the security and confidentiality of employees and business information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to Westman, its partners, customers, or any member.

In addition, the Director of Operations oversees the development, implementation, and maintenance of the information security program.

3.1.2 Who Should use this Document?

This document is intended to be used by the CEO/General Manager, IT Manager, Director of Operations and any other members as deemed appropriate by the management. It supports an agencies responsibility for implementing a cybersecurity program.

3.1.3 Commitment from Management

Westman's leadership team is committed to the development of this Information Security Program. It fully supports and owns the ultimate responsibility of this program. This commitment involves allocating necessary funding to information security work and responding without delay to new situations. The leadership team will participate in any information security related event as organized.

3.1.4 Organization Overview

Role in the Industrial sector

Westman is a chemical manufacturer producing commercial grade chemical products for use in the transportation, building and construction, and other industrial products.

Westman operates its manufacturing facility 24 hours per day and 365 days per year. To increase competitiveness, Westman has introduced process automation equipment to improve the production efficiency and to lower cost. Industrial automation equipment like Programmable Logic Controller (PLC), Human-Machine-Interface (HMI), and Data Historian are deployed in the factory to control and monitor the production operation.

The chemical sector is considered as a **Critical infrastructure** under the Presidential Policy Directive 21 (PPD-21).

Mission Objectives

1. **Maintain Personnel Safety**
   Westman commits to safe operation of the manufacturing system and to always put personnel safety as its highest priority. All manufacturing process, protocols, automation process and equipment, operating procedures and guidelines are designed to ensure personnel safety.

2. **Maintain Environmental Safety**
   Westman complies to all applicable regulations regarding environment safety. Westman is committed to ensuring environmentally-friendly operation of its manufacturing process and working to reduce its environment footprint. Environmental impact caused by the manufacturing process is measured and reviewed on a quarterly basis.

3. **Maintain Quality of Product**
   Westman has a world-class manufacturing facility and process. It has employed state of the art automation, equipment, and techniques to ensure the high quality of its product. It has developed a quality assurance program using automation equipment, including PLCs, Historian, and high precision sensors operating on a high-speed control network to monitor product quality.

4. **Maintain Production Goals**
   Meeting the monthly production goals is an important objective for Westman, and ensures the supply of products to its customers in a timely fashion. It also maintains financial stability for Westman. Constant 24/7 production enables Westman to plan its manufacturing operation to meet its production goals and customer demand. The investment in automation equipment and skilled professional assists Westman to maintain the monthly production goals.

5. **Protect Trade Secrets**
   Westman is committed to protecting its trade secrets, including product development, manufacturing processes, product quality, and supply chain management.

Role in the Supply chain

Raw materials are supplied through a long-term contract established with suppliers and are transported to the facility on a regular basis.

The end products are typically sold to customers on a large quantity. Delivery is sub-contracted to several logistics companies which will handle the transportation from the Westman facility to the end customers. Westman's products are typically being used as raw materials or addictive for other industrial manufacturers

Communication to Organization

All critical and operational aspects of the Manufacturing system, key resources should be documented in network diagrams, manuals or other artifacts. The documentation will be reviewed on a yearly basis by the Director of Operations with assistance from the IT Manager. This information will be shared with all employees, contractors depending on their role in the Company.

Critical Manufacturing System Components:

The following are a list of critical Manufacturing system components:

- Engineering workstation
- Supervisory PLC
- HMI Server
- OPC and Controller Server
- Historian Database Server
- Network devices

Supporting Services:

The supporting services required by Westman are broadband Internet connection, electricity, natural gas, and water supply. The broadband Internet connection is a business class service provided by a large national provider with business class service level agreement

3.1.5 Information Security Policy

The purpose of this Information Security Policy is to provide an overview of the policies, standards, procedures and Technical controls that make up Westman's Information Security Program. This policy is developed and executed by the Director of Operations, and has expectations set for protecting Westman's IT and OT assets.

3.1.6 Applicable Laws and Regulations

As a chemical manufacturer, Westman is required to comply with all federal and state legal or regulatory requirements for chemical and hazardous materials. Westman is also required to comply with all legal, regulatory and safety requirements being an employer.

3.1.7 Security Organization and Governance

Information security is an inherent part of governance and consists of the leadership, organizational structures and processes that safeguard Westman's information, its operations, its market position, and its reputation.

Organizational Role	Security Responsibilities
CEO/General Manager	• Reviewing and approving the information security program and supporting policies, at least annually. • Assigning the Director of Operations responsibility for organization's policies and procedures for use of any IT/OT assets, implementation, documentation and for meeting its compliance obligations. • Serve as Point of Escalation for any incidents. • Responsible for data breaches. • Comply with Westman security policy
Controller / Finances	• Comply with Westman security policy • Report any security incident and/or concerns to the Director of Operations
Control Engineers	• Report any security incident and/or concerns to the Director of Operations. • Help with the security requirements for their specific area. • Comply with Westman security policy • Assist in remediating vulnerabilities if asked by the Director.
Director of Marketing	• Comply with Westman security policy • Report any security incident and/or concerns to the Director of Operations
Director of Product Development	• Comply with Westman security policy • Report any security incident and/or concerns to the Director of Operations
Director of Operations	• Responsible for overall security of all IT/OT assets. • Responsible for remediating vulnerabilities and/or mitigating any risks. • Develop, implement and maintain the Security Program and Security Policy documents. • Act as a liaison between operators, vendors, and management on matters relating to information security. Acting as a liaison between plant operators, vendors and management on matters relating to information security. • Reports to the CEO about the status of the Security Program and security related risks or incidents.

IT Manager and IT Team	• Remediate vulnerabilities as directed by the Director of Operations. • Report any security incident and/or concerns to the Director of Operations. • Help with the security requirements for their specific business unit and area of expertise. • Comply with the Security Policy.
Legal Counsel	• Handling of any legal questions/issues relating to security incidents. • Handling of any external communications related to security incidents. • Report any security incident and/or concerns to the Director of Operations
HR Manager	• Handling of any personnel and disciplinary issues relating to security incidents. • Report any security incident and/or concerns to the Director of Operations

All employees, contractors and vendors are responsible for ensuring the security, confidentiality, and integrity of information by complying with all corporate policies and procedures

3.1.8 Privacy of Personal Information

Employees should not assume any degree of privacy to information they create or store on Westman's systems. Westman is a private organization and any information stored on its information systems may be subject to disclosure under state law. Westman will disclose information about individuals only to comply with applicable laws, regulations or valid legal requests.

3.1.9 Operational Security

Risk Management:

The Organization's Risk Management Strategy can be found in section 3.4 Risk Management Document. The Director of Operations shall conduct yearly risk assessments to identify potential internal and external risks to the security, confidentiality and integrity of Westman.

Risk assessment involves evaluating risks and their likelihood along with selecting and implementing controls to reduce risks to an acceptable level. Each risk assessment documents major findings and risk mitigation recommendations.

All employees are encouraged to report any potential or existing risks to the Director of Operations. Once the Director of Operations has identified or acknowledged the risks, the next course of action will be determined (e.g., accept the risk, seek assistance from the IT Team, contact a vendor to remediate the risk). Similarly, a vendor or contractor can also notify the

Director of Operations if they identify any threats or risks to their equipment. A detailed description of risk notification process can be found in Section 3.4 Risk Management Document.

Physical Security:

The perimeter of the facility is fenced, and the main entrance has a gate that is open during business hours and locked after hours. There are two entrances to the main building. One is for Employees only which is normally locked, employees need to swipe their personal badges to enter the building. The other entrance located at the front lobby staffed by a receptionist during normal business hours. Guests and visitors are required to sign in with proper identification. Additional details about Physical security requirements are mentioned in the Physical Security Section of the Security Policy document.

Personnel security is addressed through pre-employment screenings, adequate position descriptions, terms of employment, and security education and training.

Access Control:

User access to IT and OT systems is based on the principle of least privilege depending on the user's role in the organization. Proper authorization and approval by the Director of Operations is required prior to granting access or operating any manufacturing system equipment. Sets of controls are in place to restrict access through authentication methods and other technical means. Passwords are managed through a formal process and secure log-on procedures. Sensitive systems are explicitly identified and audited regularly.

Appropriate authentication controls are used for external connections and remote users. Physical and logical access to critical infrastructure is controlled. Duties are separated to protect systems and data. Access rights are audited at regular intervals

3.1.10 Security Awareness Training

Security awareness information is provided to new employees at the time of hire. Online resources are provided to educate employees on best practices and the importance of reporting security incidents. Additionally, the Director of Operations will ensure the employee understands their role and responsibilities in Westman's information security program.

Any information about potential or existing cyber threats to Westman's systems may be exchanged routinely between the Director of Operations and external vendors. Likewise, any news about email scams, phishing attempts and other malicious actions are posted to inform users of possible threats.

Training for Users and Managers

Employees must perform online computer-based training or classroom-based training per management approval. Below is a list of training options. Trade organization subscriptions to newsletters and magazines will offer more industry specific training classes.

Computer Based Training

- ICS-CERT VLP (Virtual Learning Portal)
  https://ics-cert-training.inl.gov
- DHS Recommended Training
  https://www.dhs.gov/chemical-sector-training
- SCADAhacker
  https://scadahacker.com/training.html
- In Person Training
  Sans Industrial Control Systems Training
  https://ics.sans.org/training/courses

Training for Privileged Users

Privileged Users in the Organizational Use case:

- **Director of Operations**
  - This user has complete control of the manufacturing process within Westman.
- **IT Manager**
  - This user has complete control of the manufacturing process within Westman.

Responsibilities:

- Any privileged user within manufacturing environment will have two accounts. A primary account used for normal activities, and a privileged "administrator" account for performing privileged functions.
  - Primary accounts are used for normal daily operations.
  - Primary accounts will have same rights as a standard Westman user account (e.g., email access, Internet access).
  - Privileged accounts will have administrative privileges, and must only be used when performing administrative functions within manufacturing system (e.g., system updates of firmware or software, system reconfigurations, device restarts).

Privileged users will adhere to securely using Administrative account when performing duties within manufacturing system. If a privilege account becomes compromised this could have a damaging impact on the manufacturing process.

Training**:**

- Training for privileged users will include training for regular users. Advance training will be provided from industry trade group specializing in automation process, or other specialty training organization focusing on manufacturing security for ICS environments.

Examples:
- International Society of Automation (ISA) https://www.isa.org
- SANS (Information Security Training) https://www.sans.org

Training for Third Party contractors

- There are many different training options available. Training can be completed in person at a training facility, or online in a virtual classroom environment. In person training at a facility will have a cost associated and it not always appropriate depending on the level of training required. Online training can also have a cost depending on the level required, but there are also options that are free and provide a good understanding of the difference between a traditional Information Technology (IT) environment and Operations Technology (OT) environment.
- Payed Training Options.
  - https://www.sans.org/course/ics-scada-cyber-security-essentials (Offers hands on training with experienced instructors).
- Free Online Training Options.
  - https://ics-cert-training.inl.gov/learn (Offers virtual classroom environment at no cost).

3.1.11 Third Party Responsibilities and Requirements

- Third party contactors and vendors are required to be aware of the sensitive information within Westman facility and the steps to ensure propriety information is kept secret.
- Third party contactors and vendors will be re-evaluated yearly from the date of completion of first security compliance check. During this re-certification all objectives listed in the Security Awareness Training section above will be reviewed again to ensure security compliance with original plan.
- Remote connections from third party providers will be conducted using a VPN Connection. All third-party remote connections will be monitored and audited.
- All software and hardware tools used within Westman network will be approved first before service provider can proceed.
- No data shall leave Westman's network without written approval from President.
- Network accounts will be limited to only enabled when needed. Accounts used by service for remote access will require approval before being allowed to connect during normal business hours. Refer to Remote Maintenance Approval process in the Security Policy document for additional details.

3.1.12 Fire and Safety Regulations

- Fire Protection Systems will compile with Local, State, and Federal laws. This is to include Fire Protection Systems specially designed for manufacturing process. Fire Protection System will place emphasis on human safety first and for most, before concern for

manufacturing system. Fire Protection Systems will be checked minimum once per year unless shorter intervals are required from superseding regulations.

- Only Industry approved Environmental Controls will be used within manufacturing systems, to included compliance with all Local, State, Federal laws. Environmental Control will be implemented to place human/community safety first before manufacturing systems.
- Fire protection for a manufacturing environment should be designed to safeguard electrical equipment. Fire Protection should be designed and implemented to protect human life first and equipment second. Installed fire protection systems will be certified compliant with existing/new environment by a licensed and accredited vendor. Check industry standards for any required baselines.

3.1.13 Emergency Power

A short-term uninterruptible power supply (UPS) to facilitate both an orderly shutdown and transition of the organization to a long-term alternate power in the event of a major power loss.

3.1.14 Incident Management

Westman's Incident Response and Recovery Plan describe the detection, analysis, containment, eradication, recovery and review of security incidents. The process for responding to security incident is designated in Incident Response Plan, while the procedures for incident recovery and resilience requirements are defined in the Incident Recovery Plan. Security incidents are managed by the Director of Operations who ensures that security incidents are promptly reported, investigated, documented and resolved in a manner that restores operation quickly and, if required, maintains evidence for further disciplinary, legal, or law enforcement actions. The Incident Response Plan and Recovery Plans are reviewed annually and updated as needed.

Lessons learned from cybersecurity events will be used to revise and improve device detection ability while increasing protection for the organization and manufacturing system.

3.1.15 Information Sharing Plan

Information sharing with outside entities like trade organizations and local, state, and federal agencies can help strengthen cybersecurity. Information sharing, especially when receiving information from other outside entities, will improve Westman's situational awareness, and result in a more secure manufacturing system.

Trade Organizations:

Relationships will be established with trade organizations. These relationships will be used to share information regarding cybersecurity incidents detected within the manufacturing facility. Information shared with trade organizations regarding cybersecurity incidents must have all proprietary information and trade secrets removed. This information will be listed as unclassified. Information regarding a cybersecurity incident containing information relating to

proprietary, customer, or trade secret process will require a Non-Disclosure Agreement before data is transmitted; this would be considered classified information requiring approval from executive management before being sent.

Local Government:

Relationships with any local government organization whose purpose is to share cybersecurity incident data should be established.

State Government:

Relationships with any state government organization whose purpose is to share cybersecurity incident data should be established. Trade organizations should be able to provide contact information for state government incident sharing organizations, if they exist.

Federal Government:

Relationships with federal government agencies whose purpose is to share cybersecurity incident data should be established. Some federal government agencies are listed below.

DHS (CISA) Agency for reporting incidents of Phishing, Malware, Vulnerabilities.
https://www.us-cert.gov/report
DHS (NCCIC) Agency for reporting cybersecurity incidents relating to Industrial Control Systems.
https://ics-cert.us-cert.gov/Report-Incident

3.1.16 Periodic Reevaluation of the Program

The Security Program document will be continuously updated to reflect changes made to manufacturing system and to improve cybersecurity. Lessons learned will be incorporated to help improve this document in the event a cybersecurity incident occurs.

The Director of Operations shall reevaluate and modify the Program from time to time as deemed appropriate. The Director of Operations shall base such reevaluation and modification on the following:

- The results of the risk assessment and monitoring efforts
- Any material changes to the Westman's operations, business or infrastructure components
- Any cybersecurity incident
- Any other circumstances that the Director of Operations knows or is informed of by the CEO

3.1.17 References

1. Implementing Effective Information Security Program by SANS Resources https://www.sans.org/reading-room/whitepapers/hsoffice/designing-implementing-effective-information-security-program-protecting-data-assets-of-1398

2. InfoSec Program Plan by University of Tennessee Knoxville https://oit.utk.edu/wp-content/uploads/2015-11-11-utk-sec-prog-plan.pdf

3. GCADA Sample Information Security Procedure http://www.gcada.org/pdf/Sample%20Information%20Security%20Procedure%20(safeguard%20policy).pdf

4. IT Security Program by Old Dominion University https://www.odu.edu/content/dam/odu/offices/occs/docs/odu-it-security-program.pdf

3.2 Security Policy Document Example

Security Policy

for

Westman Chemicals

Document Owner:	Director of Operations, Westman

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	CEO/General Manager		4-22-2018

3.2.1 Purpose

This Security Policy document defines the security requirements for the proper and secure use of IT and OT services in the organization. The goal of the policies defined within is to protect the organization and its users to the maximum extent possible against cybersecurity threats that could jeopardize their integrity, privacy, reputation, and business outcomes.

3.2.2 Scope

Any employee, contractor, or individual with access to the organization's systems or data.

3.2.3 Policy Maintenance

The Security Policy must be approved by the Director of Operations in consultation with the IT Manager and CEO/General Manager before it can be disseminated to employees. Any updates to this document will must also be approved by the Director of Operations.

This policy document will be reviewed by the Director of Operations on an annual basis and will notify all employees of any updates made to the policy.

3.2.4 Role-based Security Responsibilities

Security responsibilities vary depending on an individual's role in the company. Each is defined below.

Employees

Organizational Role	Security Responsibilities
CEO/General Manager	• Serve as Point of Escalation for any incidents. • Responsible for data breaches. • Comply with Westman security policy
Controller / Finances	• Comply with Westman security policy • Report any security incident and/or concerns to the Director of Operations
Control Engineers	• Often assume responsibility for intrusion detection in Manufacturing system. • Report any security incident and/or concerns to the Director of Operations. • Help with the security requirements for their specific area. • Comply with Westman security policy • Assist in remediating vulnerabilities if asked by the Director.
Director of Marketing	• Comply with Westman security policy • Report any security incident and/or concerns to the Director of Operations
Director of Product Development	• Comply with Westman security policy • Report any security incident and/or concerns to the Director of Operations
Director of Operations	• Responsible for overall security of all IT/OT assets. • Responsible for remediating any detected events and vulnerabilities • Implement and maintain Security Policy documents.

	• Serve as a SPOC for any security related incident and keeping upper management in the loop.
IT Manager and IT Team	• Assist in remediating vulnerabilities if asked by the Director of Operations. • Report any security incidents, anomalies detected and/or concerns to the Director of Operations. • Help with the security requirements for their specific area. • Comply with Westman security policy
Legal Counsel	• Handling of any legal questions/issues relating to security incidents. • Handling of any external communications related to security incidents. • Report any security incident and/or concerns to the Director of Operations
HR Manager	• Handling of any personnel and disciplinary issues relating to security incidents. • Inform Law Enforcement if security incident involves data breach of sensitive information. • Report any security incident and/or concerns to the Director of Operations

External Personnel

Role	Security Responsibilities
Equipment Vendor	• Assist in remediating vulnerabilities, upgrading software or hardware as required. • Comply with Westman security policy if called in.
Visitor	• Comply with Westman security policy if called in.

3.2.5 Employee requirements

1. Employees must complete security awareness training and agree to uphold the acceptable use policy.
2. Employees must immediately notify the Director of Operations if an un-escorted or unauthorized individual is found in the facility.
3. Employees must always use a secure password on all systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.

4. Terminated employees must return all company records, in any format.
5. Employees must verify with the Director of Operations that authorizations have been granted before allowing external personnel to connect to the IT or OT network.
6. Employees must report any physical security incidents to the Supervisor.
7. Employees must understand and diligently follow the physical security requirements stated in the next section.

3.2.6 Physical Security

1. Employees must always use and display physical identification (ID) provided by the company.
2. IDs must be designed to enable the immediate visual distinction between employees, external personnel, and visitors.
3. Sharing of IDs for any reason is strictly prohibited.
4. A sign-in sheet will be maintained by the receptionist to record all Visitor visits. These log records will be reviewed periodically by the Director of Operations.
5. Any visitors, contractors and/or maintenance personnel must always be escorted by an employee.
6. Unauthorized removal of any documentation, equipment, or media from any device is restricted, unless authorized. Authorization can be obtained from the Director of Operations.
7. All activities of visitors, contractors, and maintenance personnel will be subject to monitoring while onsite. An employee from the IT team will be assigned to monitor all computer activities if the visitor, contractor, or maintenance personnel is connected to any company network.
8. A supervisor will conduct monthly security status monitoring of the company to check for any physical security incidents.

3.2.7 Information Technology (IT) Assets

1. IT assets must only be used for the business activities they are assigned and authorized to perform.
2. Every employee is responsible for the preservation and proper use of the IT assets they have been assigned.
3. IT assets must not be left unduly exposed.
4. Desktops and laptops must be locked if left unattended. This policy should be automatically enforced whenever possible.
5. IT assets must not be accessed by non-authorized individuals. Authorization can be obtained from Director of Operations.
6. Configuration changes are to be conducted through the change control process, identifying risks and noteworthy implementation changes to security management.
7. All assets must be protected by authentication technologies (e.g., passwords).
8. Passwords must follow the password policy.

9. The Director of Operations must be notified immediately after an asset is discovered to be lost or stolen.
10. Use of personal devices to access IT resources is prohibited.
11. Storage of sensitive information on portable media is prohibited, unless authorized by the Director of Operations.
12. Any sensitive information stored on IT assets, or being transported on a portable device, must be protected in such a way to deny unauthorized access, and must be encrypted in line with industry best practices and any applicable laws or regulations.

Description	Quantity
SuperMicro Servers	6
Allen Bradley 5700 Switches	2
Allen Bradley 8300 Router	1
HP Tower Workstation	1

IT Assets Inventory

3.2.8 Operational Technology (OT) Assets

1. OT assets must not be used for operations they are not assigned or authorized to perform.
2. The Director of Operations and Operators are responsible for the preservation and correct use of the ICS assets they have been assigned.
3. Physical access to OT assets is forbidden for non-authorized personnel. Granting access to the assets involved in the provisioning of a service must be authorized by Director of Operations.
4. All personnel interacting directly with OT assets must have proper training.
5. The Director of Operations is responsible for all OT devices. A Control Engineer is solely responsible for maintenance/configuration of the device they are assigned. No other personnel are authorized to modify OT asset configurations, including any modification to interfacing hardware or software.
6. Usage of security tools on the OT network must be approved by the Director of Operations, and all affected Control Engineers must be notified.
7. Concept of least privilege must be followed when authorizing access to OT assets.
8. OT assets, such as PLCs, safety systems, etc., should have their keys in the “Run” position at all times unless being actively programmed.
9. Accessing IT devices or internet use from the OT network, or OT assets, unless authorized, is prohibited.

10. Accessing IT devices or internet use from the OT network, or OT asset, is prohibited.
11. Use of personal devices to access OT resources is prohibited.

Description	Quantity
Allen Bradley ControlLogix PLC	1

OT Assets Inventory

3.2.9 Lifecycle Accountability of assets

1. Any IT or OT asset that needs to be decommissioned must be sanitized of all data, as per the manufacturer guidelines. This task will be usually performed by the IT Support staff.
2. In case of an employee termination, an IT asset such as desktop PC or laptop must be reimaged prior to assigning it to a different employee.

3.2.10 System Maintenance

1. Any maintenance tasks involving external resources such as Vendors, Contractors or other non-employees must be pre- approved by the Director of Operations. This can be coordinated by filling out the Maintenance Order approval form.
2. It is the responsibility of Vendors, Contractors and/or Maintenance personnel with access to Westman's resources that due care is ensured to properly secure their own resources.
3. It is responsibility of the IT staff that due care is ensured when using vendor devices on networks.
4. All systems and/or technical controls must be verified upon the completion of maintenance for any cybersecurity related impact.
5. All systems and/or technical controls must be verified upon the completion of maintenance for any cybersecurity related impact.
6. All maintenance work details will be logged in a Maintenance Tracker Excel sheet. The Supervisor will update all details of the work performed in the sheet.

3.2.11 Data

1. Access to sensitive data must be authorized by Director of Operations.
2. Data should not be shared informally. When access to sensitive information is required, personnel can request it from their supervisors and should take all necessary steps to prevent unauthorized access.
3. You must immediately notify the Director of Operations in the event a device containing sensitive data is lost (e.g. mobiles, laptops, USB devices).
4. It is recommended personnel use encrypted portable media or secure protocols while transferring data across systems. Director of Operations can provide you with systems or devices that fit this purpose. You must not use other mechanisms to handle sensitive data.

5. If you have been permitted to work remotely you, extra precautions must be taken to ensure sensitive data is appropriately protected.
6. Physical copies of data should be stored in a secure location where unauthorized personnel cannot access it.
7. Personnel should ensure physical copies of sensitive data are not left unattended on a printer.
8. Physical copies of sensitive data should be shredded or disposed in a secure manner.

Description	Digital Files	Physical Copies	Databases
PLC program code	✓		
Chemical formulas	✓	✓	
Quality Assurance Procedures	✓	✓	
Operating manuals and documentation	✓	✓	
Electrical diagrams	✓	✓	
Network diagrams	✓	✓	
Historical production data	✓		✓

Data types considered sensitive, proprietary, or containing trade secrets.

3.2.12 Credentials Management

The purpose of this policy is to establish a standard for the creation of strong passwords, protection of those passwords, frequency of change and employee expectations.

All staff, vendors, contractors or other stakeholders who use Westman's IT and OT systems should be given authenticated access to those systems by assigning individual credentials [username and password]. All access and restrictions to those access will be controlled by these credentials.

The creation and removal of IT system accounts is managed via Microsoft Active Directory. In addition, The IT manager will determine and authorize user access to IT or OT systems.

Westman reserves the right to suspend without notice access to any system or service.

3.2.13 Password Policy for Active Directory Accounts

1. All employee and system passwords must be at least 10 characters long and contain a combination of upper-case and lower-case letters, numbers, and special characters.
2. Passwords must be changed every 90 days and cannot match a password used within the past 12 months.
3. Passwords must not be a dictionary name or proper name.
4. Passwords must not be inserted into email messages or other forms of electronic communication.
5. Employees must choose unique passwords for all company accounts and may not use a password that they are already using for a personal account.
6. Whenever possible, use of multi-factor authentication is recommended.
7. Default passwords, such as those preconfigured in newly-procured assets, must be removed before the asset is installed or connected to any organizational network.
8. Sharing of passwords is forbidden.
9. Passwords must not be revealed or exposed to public sight.
10. Personnel must refrain from writing passwords down.
11. Personnel must not use the "remember password" feature prevalent on many applications.

3.2.14 Privileged Accounts

Privileged Users

- **Director of Operations**
  - This user has complete control of the manufacturing process within Westman.
- **IT Manager**
  - This user has complete control of the manufacturing process within Westman.

Responsibilities

- Any privileged user within manufacturing environment will have two accounts. A primary account used for normal activities, and a privileged "administrator" account for performing privileged functions.
  - Primary accounts are used for normal daily operations.
  - Primary accounts will have same rights as a standard Westman user account (e.g., email access, Internet access).
  - Privileged accounts will have administrative privileges, and must only be used when performing administrative functions within manufacturing system (e.g., system updates of firmware or software, system reconfigurations, device restarts).
- Privileged users will adhere to securely using Administrative account when performing duties within manufacturing system. If a privilege account becomes compromised this could have a damaging impact on the manufacturing process.

3.2.15 Antivirus

1. Antivirus software must be installed on all workstations and servers.
2. Virus signatures must be updated daily.
3. Antivirus software must provide the capability to push signatures on an ad-hoc basis.

3.2.16 Internet

1. Internet access is provided for business purposes.
2. Limited personal navigation is permitted from IT networks if no perceptible consumption of organizational system resources is observed, and the productivity of the work is not affected.
3. Only authorized Internet access from the OT network is permitted. Authorized access can be obtained from Director of Operations.
4. Inbound and outbound traffic must be regulated using firewalls in the perimeter.
5. All Internal/External communications must be monitored and logged by in-house network security tools. Logs must be reviewed regularly by the IT staffs and any anomalies detected should be reported to the Director of Operations or IT Manager.
6. When accessing the Internet, users must behave in a way compatible with the prestige of the organization.

3.2.17 Continuous Monitoring

1. Westman will implement a Security Continuous Monitoring program. This will include performing comprehensive network monitoring using Commercial or Open source tools to detect attacks, attack indicators and unauthorized network connections.
2. The Manufacturing system will be monitored for any cybersecurity attack indicators or IOC's.
3. All External boundary network communications will be monitored.
4. All cybersecurity incidents must be logged in the Incident Response Management tool for documentation purposes.
5. All Local, State, and Federal detection activities applying to organization or manufacturing system will be followed in accordance within the law. Detection activities are to include any industry regulations, standards, policies, and other applicable requirements.
6. Monitoring activity levels will be increased during periods of increased risk and/or any other factors as necessitated by Westman's Management.

7. All cybersecurity events detected will be communicated to the below list of defined personnel identified by the Director of Operations.

Event Severity	List of Personnel
Low (All Events)	Control Engineers
Medium	IT Staff, Control Engineers
High (Requiring Urgent Attention)	IT Manager, Director of Operations

8. Details of cybersecurity events will be shared with ICS-CERT (https://ics-cert.us-cert.gov/) to help secure the organization, including helping secure the industry. Cyber + Infrastructure (CISA) is an agency of Department of Homeland Security which provides reporting capabilities for manufactures related to cybersecurity events

3.2.18 External Service Provider Communications:

1. All communications from External Service Providers to Westman's systems will be monitored to ensure work provided by service provider is done correctly, including following all cybersecurity best practices and complying with Westman's security policies. Monitoring will include designated employee to oversee all activities performed.

2. Any Indicator of Compromise (IOC's) detected while monitoring external service provider communications will be reported and escalated via appropriate communication channels. The Director of Operations will reach out to the External service provider upon verifying the threat to discuss and seek an immediate remediation path accordingly.

3.2.19 User Access Agreement

Each employee provided with access to any Westman's resources, including Email and HR system, is required to review and accept the terms of the User Access Agreement.

As an employee of Westman:

1. You may use Westman's IT, OT systems and networks to which you have been granted access for work related purposes only. Accounts and access are granted based on each individual's roles and responsibilities.
2. You should not expect any privacy on Westman's premises or when using Westman's property or networks either when onsite or accessing remotely
3. You will act responsibly to maintain the security and integrity of the information systems that you use, so as to minimize the chance of any problems or security breaches for Westman.

4. You agree to co-operate with any audit by us or our Contractors of your access to the System.
5. You understand your responsibility for respecting other employee's privacy and protecting the confidentiality of information to which you have access, and will comply with all privacy laws, codes and guidelines including,
6. Internet access must not be used for activities that are not authorized under existing laws, regulations, or organization policies.
7. Any company laptops assigned to you should only be used for the purpose of conducting Westman's business. You are expected to take due care while using laptops.
8. All laptops must be returned at the end of employment.
9. You understand that Transmission or intentional receipt of any inappropriate material or material in violation of law or district policy is prohibited. This includes but is not limited to: copyrighted material; threatening or obscene material: material protected by trade secrets; the design or detailed information pertaining to explosive devices: criminal activities or terrorist acts; gambling; illegal solicitation; racism; inappropriate language.
10. You shall be subject to disciplinary action up to and including termination for violating this agreement or misusing the internet.

3.2.20 Remote Access

This policy applies to the users and devices that need access the organization's internal resources from remote locations.

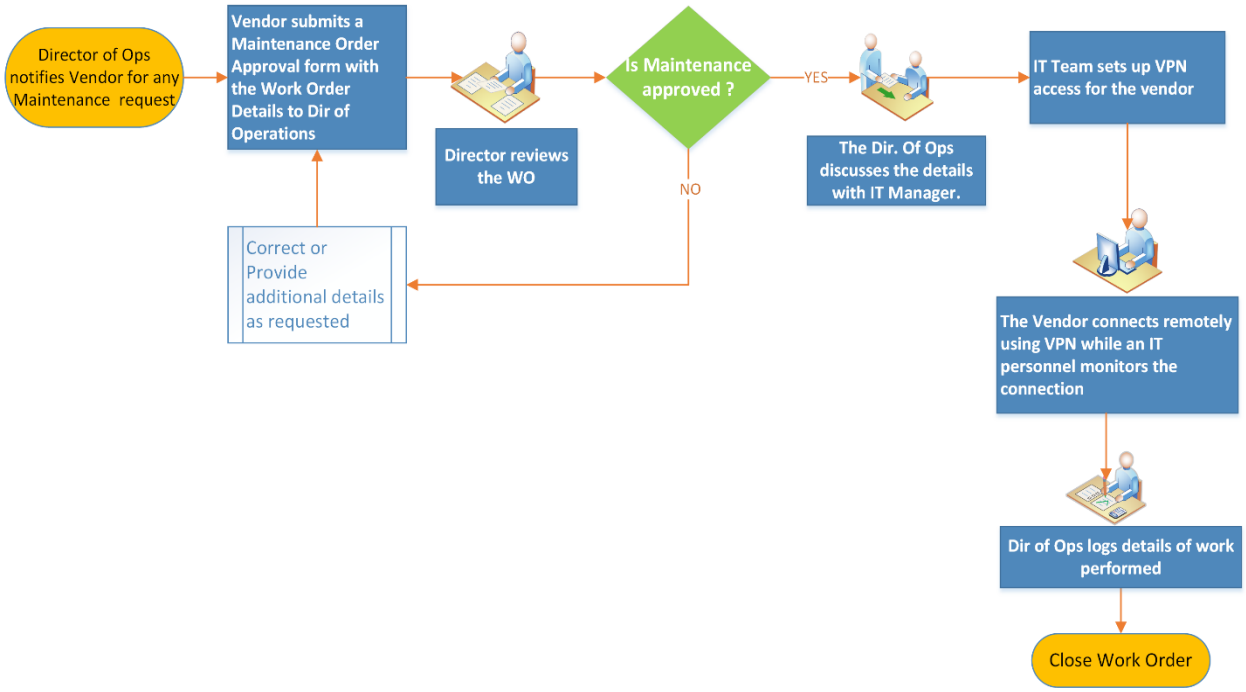
1. Remote access for personnel requires pre-approval by Director of Operations. The IT manager must also be informed. Vendors requesting remote access must be registered with the company and are required to submit all work order details using the Maintenance Order Approval Form.
2. The Director will determine list of authorized users for remote access.
3. Remote access to sensitive or confidential information is not permitted on an unencrypted connection. Exception to this rule may only be authorized in cases where it's strictly required.
4. A VPN account will be setup by the IT Team and credentials shared with the vendor. The Once connected via a VPN, the vendor will be permitted Remote Desktop Access to select systems such as the Engineering Workstation or HMI Server depending on the nature of the task. The access will be disabled upon completion of the work.
5. All activities will be subject to monitoring by IT staff. Monitoring will start and continue until remote session is no longer required, or work has been completed. Appointed individual will indicate when remote session is active and ensure manufacturing system environment has been returned to same state before remote connection was established
6. Installation of any software such as desktop sharing software etc. on authorized devices will be performed by the IT staff.
7. Use of remote access technologies on personal devices is prohibited.

8. All devices connected via remote access technologies must use the most up-to-date anti-virus software and virus signatures.
9. During an onsite visit, all activities will be subject to monitoring. Dedicated IT personnel will be assigned to monitor the vendor over the shoulder while he/she is working off a computer.
10. Split tunneling will be disabled. All internet bound traffic will be directed through Corporate network during a VPN session.

3.2.21 Usage Restrictions

- To avoid confusing official company business with personal communications, employees, contractors, and temporary staff with remote access privileges must never use non-company e-mail accounts (e.g. Hotmail, Yahoo, etc.) to conduct business.
- No employee is to use Internet access through company networks via remote connection for illegal transactions, harassment, competitor interests, or obscene behavior, in accordance with other existing employee policies.
- Where supported by features of the system, session timeouts are implemented after a period of no longer than 30 minutes of inactivity. Where not supported by features of the system, mitigating controls are implemented.

3.2.22 Remote Maintenance Approval Process



3.2.23 Maintenance Approval Form

Maintenance Order Approval Form	
Vendor Name	
Vendor Address	
Vendor Phone number	
Does the Vendor provide support to Westman currently?	☐ YES ☐ NO
Does the Vendor system intended to be used have an Anti-virus installed?	☐ YES ☐ NO
What items will be supported and/or worked upon during this session?	☐ PC / Laptops ☐ Servers ☐ Control System Devices ☐ Any other IT/OT Device ☐ Software Details:
Will any software or program need to be installed on Westman's systems?	☐ YES ☐ NO Details (if YES):
Does this software require licensing to be purchased?	☐ YES ☐ NO
Details of the task to be performed	
Is this a recurring activity	☐ YES ☐ NO
Vendor Signature	
Work Approved *(To be filled by Director of Operations)*	☐ YES ☐ NO
Director of Operations Signature	

3.2.24 Communicate Information to Organization

All critical and operational aspects of the Manufacturing system, key resources should be documented in network diagrams, manuals or other artifacts. The documentation will be reviewed on a yearly basis by the Supervisor.

This information will be shared with all employees, contractors depending on their role in the Company.

3.2.25 Definitions and Acronyms

Asset	A device owned by the organization
AV	Anti-virus
AV scanning	The act of scanning a device for viruses
Change control process	A systematic approach to managing all changes made to a product or system. The purpose is to ensure that no unnecessary changes are made, that all changes are documented, that services are not unnecessarily disrupted and that resources are used efficiently.
Device	Electronic hardware (e.g., machine, computer, laptop, phone, networking equipment)
Employee	An individual directly employed by the organization
External personnel	An individual who is not an employee (e.g., contractor, visitor)
Human machine interface (HMI)	Asset used by personnel to interface and interact with OT (e.g., machines)
ID	Physical identification (e.g., badge)
Industrial control system (ICS)	Typically, the hardware and software used to control processes, or operate machines and manufacturing processes
Information technology (IT)	Hardware devices such as computers, laptops, network switches, firewalls etc.
Least privilege	A user is only authorized to perform the functions necessary to perform their job
Operating system	Software that operates a device (e.g., Windows, Linux); typically, the interface used by the user
Operational technology (OT)	ICS and other devices (typically internetworked) used by the manufacturing process
Personal device	A device owned by an individual; not owned or controlled by the organization

Personnel	All employees and external personnel, excluding visitors
Portable media	USB flash drive, compact disc (CD), external hard drive, laptop
Remote access technologies	Software used to connect a device to the IT or OT network via the Internet, usually performed by personnel located off-site
Sensitive data	Data containing proprietary information or trade secrets pertaining to the operations of the organization; data that could cause damage to the organization if obtained by an attacker
Split tunneling	Split tunneling allows a mobile user access public network (e.g. Internet) and local LAN/WAN Corporate network at the same using same or different network connections
User	Individual using a device
Virus signature	Data used by antivirus software to identify viruses
VPN	Virtual private networking; see 'remote access technologies'.
Vulnerability scanning	Software used to detect common or known vulnerabilities on a device

3.2.26 References

1. Security Policies by SANS Resources https://www.sans.org/security-resources/policies
2. Template for Security Policy by Project Management Docs http://www.projectmanagementdocs.com/template/Security-Policy.doc
3. Data Security Policy by Sophos labs https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en

3.3 Standard Operating Procedures Document Example

Standard Operating Procedures

for

Westman

Document Owner:	Director of Operations, Westman

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	CEO/General Manager		4-22-2018

3.3.1 Introduction

This document defines the procedural steps management and employees will follow ensuring consistence daily actives along with response to events occurring within the manufacturing system for Westman. Within this document contains content which should be referred to often ensuring all employees/individuals performing work within manufacturing system are not inadvertently compromising cybersecurity posture by not following Standard Operation Procedures (SOPs).

3.3.2 Purpose

To provide a consistent repeatable process that can be followed to perform tasks within manufacturing system.

3.3.3 Scope

Management, employees, contractors, or individuals requiring access to manufacturing system for changes should be familiar with the contents included within this document.

IDENTIFY

3.3.4 Asset Inventory

Identifying assets within manufacturing system for Westman is a vital first step in protecting organization from malicious activates that could result in disruption to production. Westman uses multiple tools for asset inventory, some manual and some automated. Knowing the environment and what devices are installed allows the ability to detect non-approved devices on the network which could be an indication of malicious activity. Keeping devices updated with the latest patches ensure to mitigate potential weakness within manufacturing system. All patches will be carefully examined to determine if there could be any performance impact effecting production within manufacturing system.

Manual

Devices not able to be automatically scanned will be added to the Excel spreadsheet and updated quarterly. Devices included in manual process would be PLC and machine stations, including any additional devices that are unable to be scanned automatically with a tool. All inventory will be conducted during manufacturing system planned down time and inventory will include hardware and software.

Automated

Devices with the ability to be scanned will be added to Westman's asset inventory tool and scanned quarterly. Scanning quarterly will ensure manufacturing process is not affected. All scanning should be performed when manufacturing system has been placed into a non-production mode (system down time). Westman has chosen an asset inventory tool that has multiple version from open source to enterprise edition. Westman has selected Enterprise edition since this version provides the ability to schedule scans, baseline systems for monitoring changes. For additional information and references see.

Westman inventory management tools will be configured for group access to ensure only individuals requiring access are allowed. This ensure that people within the organization only requiring read accesses are not granted a higher level, which could lead to inadvertent changes to tools configuration. See reference for how groups are created.

Scans of manufacturing system will be conducted quarterly ensuring not to effect manufacturing process. Scans will audit software including license information, version, and configuration. Devices within the manufacturing systems will have software inventory audited and reviewed quarterly. Changes occurring to devices' software before the next update will trigger a required

inventory to remain compliant. See reference for additional details for performing scanning within manufacturing system.

Westman will apply updates to asset inventory software as they become available. Updates are required to keep system free from known vulnerabilities while including new features. See reference for additional information

3.3.5 Network Baseline

Network baseline is important as it provides the ability to detect malicious active occurring on manufacturing system network. Westman will periodically perform baseline scans to identify any unusual traffic, which could be indication of malicious activity. All traffic observed during scanning should be reconciled to help create a more secure network. See reference for network baseline performed.

3.3.6 External Connections

Using company provided network diagram tools all network connection for external communication will be mapped. Mapping will include all relevant information for connection service provided. Example of information required would be assigned IP address for device providing service, support phone number, customer number, person of contact, and support level agreement and hours. External providers will include cloud services. Network diagram will be updated quarterly.

3.3.7 Baseline Configurations

Baseline configurations was captured using two methods since some ICS devices don't allow automated tool scanning; for these devices' spreadsheet tracking is the preferred method. Devices lacking SSH, SNMP, WMI ability will require manual entry in spreadsheet.

Steps used to perform automated scanning for Westman.

Baseline configurations Westman implemented within Manufacturing systems helps to ensure inadvertent changes are detected before systems' integrity has been compromised.

Open-AudIT [1] has been chosen for Westman due to scalable configuration depending on required needs. Instruction are listed for performing scanning. Once scanning has been performed changes with ICS devices are detectable by running reports identifying new software changes.

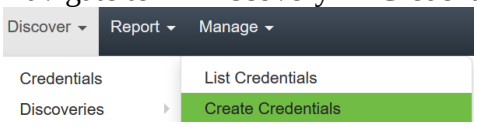
Manufacturing systems was scanned to get initial baseline. Scanning steps used are listed below. Completed scans result scan be exported to CSV file for storage. See end of instructions for exported configuration.

[1] Open-Audit: https://www.open-audit.org

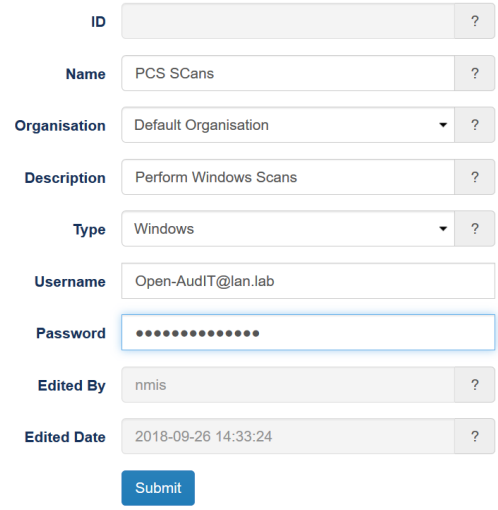
Open-Audit Configuration steps within Process Control System once system has been installed

Initial Configuration:

- Login to Open-AudIT via web portal
- Navigate to → Discovery → Credentials → Create Credentials

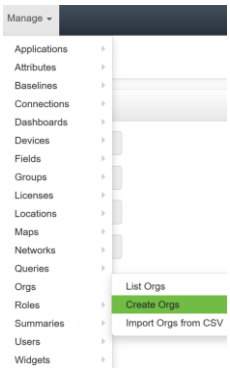


- Credentials can be assigned to any organization that has already been created. If you want credentials to only apply to specific organizational group, then select that from the appropriate drop-down during credential creation and select the desired group these credentials will apply to.
- Our environment consists of mainly Windows machine, so Windows will be used for connection type.
- Now create a credential and select **Windows** for the type. Once completed click **Submit**.



Organization Groups Creation:

- Click on Manage → Orgs → Create Orgs

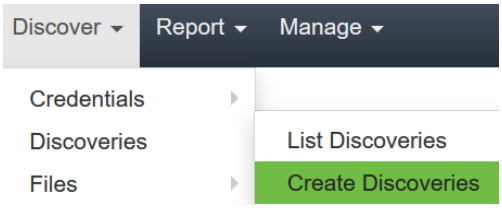


- Now enter **Name**: **Description**: and click submit at the bottom of the page to save.

- If you have multiple machines / equipment in different locations you can make Organizational groups based on business units, or related task.

Configure Discovery Scan:

- Now click on Discover → Discoveries → Create Discoveries



- Enter a meaningful name for discover being created

- Next, enter the subnet that'll be used for performing this scan. This scan is using 172.16.0.0/22 

Search online for additional subnetting information / calculators if you'd like to learn more.

- **Network address:** should already be defaulted to Open-AudIT installed location, if this is not true, click the drop-down arrow and select your installed location.

- Now, click on the advanced button to see more options. 

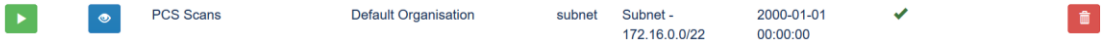
- Once **Advanced** has been expanded you'll have additional options to select if desired. These options are **Org, Type, Devices Assigned to Org,** and **Devices Assigned to Location**. These options aren't required but allow you to organize found devices into groups.

- Once all are selected click on **Submit** button to continue.

Discoveries:

- Once the above steps have been completed clicking on **Submit** button you'll be taken to a new webpage that will allow you to run discovery process created in the previous step.

- To start discovering devices click on **green** arrow button. If you need to verify details for this scan click on the button that looks like an **eye**: finally, if you need to delete this scan click on the **trash** can icon to the right. See screen shot for details.



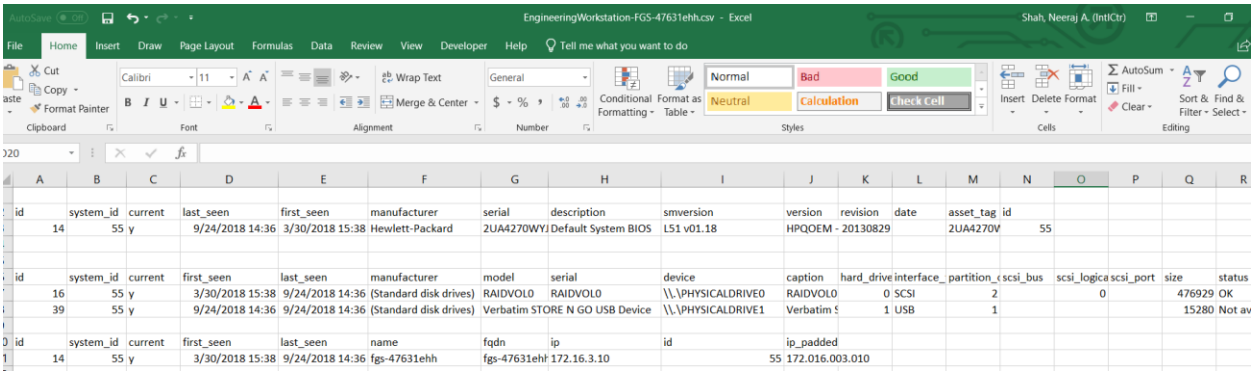
- Once discovery has started you'll be taken to a new page allowing you to view status or cancel.

Newly found devices are added to **My Devices** which is found on the home screen.

Process Control System 

Detailed baseline reports generated out of Open-AudIT can be obtained from [PCS Baseline Data]

Shown below is an export of the baseline data from one of the devices using Open-AudIT in the Process Control System.



d	system_id	current	first_seen	last_seen	mac	net_index	ip	netmask	cidr	version	network	set_by	interface	id	ip_padded
74	55	n	3/30/2018 9:26	3/30/2018 15:36			172.16.3.10	255.255.255.0	24	4	172.16.3.0/24			55	172.016.003.
75	55	y	3/30/2018 15:38	##############	40:a8:f0:3d:48:ae	7	172.16.3.10	255.255.255.224	27	4	172.16.3.0/27			55	172.016.003.
76	55	y	3/30/2018 15:38	9/24/2018 14:36	40:a8:f0:3d:48:ae	7	fe80::5cca:8dfd:2281:992e		64	6				55	

d	system_id	current	first_seen	last_seen	name	file_name	file_size	max_file_size	overwrite	id
148	55	y	3/30/2018 15:38	9/24/2018 14:36	Application	C:\Windows\	3140	20480	As Needed	55
149	55	y	3/30/2018 15:38	9/24/2018 14:36	FTDiag	C:\Windows\	3140	25600	As Needed	55
150	55	y	3/30/2018 15:38	9/24/2018 14:36	HardwareEvents	C:\Windows\	68	20480	As Needed	55
151	55	y	3/30/2018 15:38	9/24/2018 14:36	Internet Explorer	C:\Windows\	68	1028	As Needed	55
152	55	y	3/30/2018 15:38	9/24/2018 14:36	Key Management Serv	C:\Windows\	68	20480	As Needed	55
153	55	y	3/30/2018 15:38	9/24/2018 14:36	Media Center	C:\Windows\	68	8192	As Needed	55
154	55	y	3/30/2018 15:38	9/24/2018 14:36	Security	C:\Windows\	204804	204800	As Needed	55
155	55	y	3/30/2018 15:38	9/24/2018 14:36	Symantec Endpoint Pr	C:\Windows\	6212	8192	As Needed	55
156	55	y	3/30/2018 15:38	9/24/2018 14:36	System	C:\Windows\	20484	20480	As Needed	55
157	55	y	3/30/2018 15:38	9/24/2018 14:36	Veeam Agent	C:\Windows\	1028	1028	As Needed	55
158	55	y	3/30/2018 15:38	9/24/2018 14:36	Windows PowerShell	C:\Windows\	68	15360	As Needed	55

d	system_id	current	first_seen	last_seen	serial	bank	type	form_factor	detail	size	speed	tag	id
10	55	y	3/30/2018 15:38	9/24/2018 14:36	16142323	DIMM4	Synchronous	DIMM	Unknown	4096	1333	Physical Memory	55
11	55	y	3/30/2018 15:38	9/24/2018 14:36	16142314	DIMM3	Synchronous	DIMM	Unknown	4096	1333	Physical Memory	55
12	55	y	3/30/2018 15:38	9/24/2018 14:36	16142322	DIMM2	Synchronous	DIMM	Unknown	4096	1333	Physical Memory	55
13	55	y	3/30/2018 15:38	9/24/2018 14:36	16142352	DIMM1	Synchronous	DIMM	Unknown	4096	1333	Physical Memory	55

d	system_id	current	first_seen	last_seen	manufacturer	model	serial	description	device	manufactu	size	aspect_ratio	edid_versi	cost_code	id
6	55	y	3/30/2018 15:38	9/24/2018 14:36	Dell	DELL P2414H	27HW349M0EDL	1920 x 1080	A09A	14-Oct	24	16:09			55
11	55	y	9/24/2018 14:36	9/24/2018 14:36	Sharp	SHARP HDMI	0	1920 x 1080	1.00E+06	13-Jan	80	16:09			55

List of programs installed:

10661	55	y	3/30/2018 15:38	9/24/2018 14:36	Internet Explorer	9.10.9200.17609			########	1/1/2000 0:00	Microsoft Cor	
10662	55	y	3/30/2018 15:38	9/24/2018 14:36	Notepad++ (64-bit x64)	7.5.6			C:\Program Files\Notepad++\un	0000-00-00 00:0(	Notepad++ Te	
10663	55	y	3/30/2018 15:38	9/24/2018 14:36	Intel(R) Network Connections Drivers	19	C:\Windows\system32		Prounstl.exe	0000-00-00 00:0(	Intel	
10664	55	y	3/30/2018 15:38	9/24/2018 14:36	OSIsoft MS Runtime Redistributables x64	3.1.1			MsiExec.e	20150306	0000-00-00 00:0(	Rockwell A D:\
10665	55	y	3/30/2018 15:38	9/24/2018 14:36	Microsoft Visual C++ 2010 x64 Redistributa	10.0.40219			MsiExec.e	20150306	0000-00-00 00:0(	Microsoft c:\
10666	55	y	3/30/2018 15:38	9/24/2018 14:36	Java 8 Update 60 (64-bit)	8.0.600.27	C:\Program Files\Java\jr		MsiExec.e	20150928	0000-00-00 00:0(	Oracle Cor C:\
10667	55	y	3/30/2018 15:38	9/24/2018 14:36	Veeam Agent for Microsoft Windows	2.0.0.700	C:\Program Files\Veeam		MsiExec.e	20170731	0000-00-00 00:0(	Veeam Sof C:\
10668	55	y	3/30/2018 15:38	9/24/2018 14:36	Microsoft SQL Server 2012 Management O	11.1.3000.0			MsiExec.e	20170731	0000-00-00 00:0(	Microsoft C:\
10669	55	y	3/30/2018 15:38	9/24/2018 14:36	PI Software Development Kit (PI SDK) x64	1.4.2.445	C:\Program Files\Rockw		MsiExec.e	20150306	0000-00-00 00:0(	Rockwell A C:\
10670	55	y	3/30/2018 15:38	9/24/2018 14:36	Microsoft Visual C++ 2008 Redistributable	9.0.30729.6161			MsiExec.e	20150306	0000-00-00 00:0(	Microsoft c:\
10671	55	y	3/30/2018 15:38	9/24/2018 14:36	Microsoft .NET Framework 4.6.2	4.6.01590	C:\Windows\Microsoft.I		MsiExec.e	20180301	0000-00-00 00:0(	Microsoft C:\
10672	55	y	3/30/2018 15:38	9/24/2018 14:36	PI AF Client (x64) 2012	2.5.1.5159	C:\Program Files (x86)\R		MsiExec.e	20150306	0000-00-00 00:0(	Rockwell A D:\
10673	55	y	3/30/2018 15:38	9/24/2018 14:36	Microsoft SQL Server Compact 4.0 x64 EN(	4.0.8482.1	C:\Program Files\Micros		MsiExec.e	20150306	0000-00-00 00:0(	Microsoft D:\
10674	55	y	3/30/2018 15:38	9/24/2018 14:36	Microsoft System CLR Types for SQL Serve	11.1.3000.0			MsiExec.e	20170731	0000-00-00 00:0(	Microsoft C:\
10675	55	y	3/30/2018 15:38	9/24/2018 14:36	SST DeviceNet Products 3.10	3.10.000	C:\Program Files (x86)\S		MsiExec.e	20171026	0000-00-00 00:0(	Molex Inc(C:\
10676	55	y	3/30/2018 15:38	9/24/2018 14:36	Microsoft SQL Server 2012 Express LocalDI	11.3.6020.0			MsiExec.e	20170731	0000-00-00 00:0(	Microsoft C:\
10677	55	y	3/30/2018 15:38	9/24/2018 14:36	Microsoft Message Analyzer	4.0.7948.0			MsiExec.e	20160519	0000-00-00 00:0(	Microsoft E:\
10678	55	n	3/30/2018 15:41	9/24/2018 14:36	Symantec Endpoint Protection	14.0.3876.1100	C:\Program Files (x86)\S		MsiExec.e	20180206	0000-00-00 00:0(	Symantec E:\
10679	55	y	3/30/2018 15:38	9/24/2018 14:36	FactoryTalk Historian Site Edition 4.00 Live	4.00.00.0104					0000-00-00 00:0(	Rockwell Auto
10680	55	y	3/30/2018 15:38	9/24/2018 14:36	FileZilla Client 3.28.0	3.28.0	C:\Program Files\FileZilla FTP Client				0000-00-00 00:0(	Tim Kosse
10681	55	y	3/30/2018 15:38	9/24/2018 14:36	Redundancy Module Config Tool	8.4.1.0	C:\Program Files (x86)\Rockwell Sof			20170926	0000-00-00 00:0(	Rockwell A C:\
10682	55	y	3/30/2018 15:38	9/24/2018 14:36	AX88772B Windows Drivers	1.0.0.0	C:\Program Files (x86)\ASIX Electro			20150914	0000-00-00 00:0(	ASIX Electr D:\
10683	55	y	3/30/2018 15:38	9/24/2018 14:36	Matrikon OPC Server for Simulation						0000-00-00 00:00:00	
10684	55	y	3/30/2018 15:38	9/24/2018 14:36	MatrikonOPC Sniffer						0000-00-00 00:00:00	
10685	55	n	3/30/2018 15:38	3/30/2018 15:41	Mozilla Firefox 41.0.2 (x86 en-US)	41.0.2	C:\Program Files (x86)\Mozilla Firefox				0000-00-00 00:0(	Mozilla
10686	55	n	3/30/2018 15:38	3/30/2018 15:41	Mozilla Maintenance Service	41.0.2.5765					0000-00-00 00:0(	Mozilla
10687	55	y	3/30/2018 15:38	9/24/2018 14:36	OSSEC HIDS 2.9.2	2.9.2					0000-00-00 00:00:00	
10688	55	y	3/30/2018 15:38	9/24/2018 14:36	PI Software Development Kit (PI SDK) x86 2	1.4.2.445	C:\Program Files (x86)\Rockwell Software\FactoryTalk Hi				0000-00-00 00:0(	Rockwell Auto
10689	55	y	3/30/2018 15:38	9/24/2018 14:36	PI Software Development Kit (PI SDK) x64 2	1.4.2.445	C:\Program Files\Rockwell Software\FactoryTalk Historia				0000-00-00 00:0(	Rockwell Auto

List of patches installed:

10880	55	y	3/30/2018 15:38	9/24/2018 14:36	Rockwell Automation Generic Safety Modu	9.05.3364.0				20150306		0000-00-00 00
10881	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2764913					1/19/2015	fgs-47631(	0000-00-00 00
10882	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2764916					1/19/2015	fgs-47631(	0000-00-00 00
10883	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2718695					1/19/2015	fgs-47631(	0000-00-00 00
10884	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2670838					1/19/2015	fgs-47631(	0000-00-00 00
10885	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2830477					3/6/2018	fgs-47631(	0000-00-00 00
10886	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2592687					3/6/2018	fgs-47631(	0000-00-00 00
10887	55	y	3/30/2018 15:38	9/24/2018 14:36	KB971033					1/19/2015	fgs-47631(	0000-00-00 00
10888	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2479943					1/19/2015	fgs-47631(	0000-00-00 00
10889	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2491683					1/19/2015	fgs-47631(	0000-00-00 00
10890	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2506014					1/19/2015	fgs-47631(	0000-00-00 00
10891	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2506212					1/19/2015	fgs-47631(	0000-00-00 00
10892	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2506928					1/19/2015	fgs-47631(	0000-00-00 00
10893	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2509553					1/19/2015	fgs-47631(	0000-00-00 00
10894	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2511455					1/19/2015	fgs-47631(	0000-00-00 00
10895	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2515325					1/20/2015	fgs-47631(	0000-00-00 00
10896	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2532531					1/19/2015	fgs-47631(	0000-00-00 00
10897	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2533552					1/19/2015	nt authorit	0000-00-00 00
10898	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2533623					1/19/2015	fgs-47631(	0000-00-00 00
10899	55	y	3/30/2018 15:38	9/24/2018 14:36	KB2534111					1/19/2015		0000-00-00 00

3.3.8 Update Baseline after Modifications

Manufacturing baseline will be reviewed quarterly and updated with any changes that have occurred since last review. During period between baseline updates any new equipment added, or configuration changes implemented will initiate a new baseline scan to be performed. GRASSMARLIN[2] and Wireshark[3] are the tools used for updating baseline after modification have occurred. Examples of changes within the manufacturing system would be updating software, license, system patches, firmware updates, new devices like PLCs' or HMIs' and other ICS components required for operations.

3.3.9 Network Operations Baseline

Network baseline will be created within manufacturing system to identify all crucial components required for production to operate. Tools used for this process are as listed, GRASSMARLIN and Wireshark. Each tool listed provides slightly different capabilities and detail. GRASSMARLIN generates a diagram for easy visualization, compare to Wireshark which provides data without diagrams. These tools provide the required network operations baseline required for manufacturing process.

3.3.10 Priorities for Manufacturing Missions

The priorities for manufacturing missions have been identified in the "Organization Overview" Section of the Security Program document.

3.3.11 Critical Manufacturing system components and functions

The critical manufacturing system components and functions have been identified in the Organization Overview Section of the Security Program document.

PROTECT

3.3.12 Security

Security within the organization including the manufacturing system will be followed at all time to reduce risk of cybersecurity incidents. Sections below contain multiple references to procedures used at Westman for securing the manufacturing system.

[2] GRASSMARLIN: https://github.com/nsacyber/GRASSMARLIN

[3] WireShark: https://github.com/nsacyber/GRASSMARLIN

3.3.13 Training

Training is a vital role for keeping the company safe for Cybersecurity threats. All employees, contractors and vendors should have completed required training before being allowed to work within manufacturing system. Awareness and Training for Third Party Contractors and Vendors should be reviewed and signed before being allowed to access manufacturing systems.

3.3.14 Port Security

Port security allows the ability to configure network ports to be associated with individual device's Media Access Control (MAC) addresses. Enabling port security ensures only designated devices are allowed access, any device not already in the approved list will be denied access. Port Security provides additional protection, when used with defense in depth strategies. See reference for steps required for setup within Westman.

3.3.15 Network Segmentation

Westman network for manufacturing systems has been segmented to improve speed and security within the environment. Network segmentation provides ability to control traffic from each network, ensuring only allowed communication can pass between each network. See reference for steps used for Westman.

Task: Implement network segmentation.

- The Work Cell consists of the following network hardware.

Type	Description
Allen Bradley Stratix 8300	Boundary protection Firewall, Router
Allen Bradley Stratix 5700	Layer-2 Switch for the Control Network
Allen Bradley Stratix 5700	Layer-2 Switch for the Supervisory Network

- Network segmentation was implemented using the Allen Bradley Boundary router. The router has the following sub-networks defined.

Interface	IP address of Interface	Network / Subnet	Description
Fa 1/1	172.16.1.1	172.16.1.0/24	Supervisory Vlan1
Fa 1/2	172.16.2.1	172.16.2.0/24	Control Vlan1
Fa 1/3	172.16.3.1	172.16.3.0/24	Engineering LAN
Fa 1/4	10.100.0.40		Uplink to Cybersecurity LAN

- One of the Stratix 5700 switches was connected to the Fa 1/1 interface of the 8300 Router and used for the Supervisory (Vlan1) sub-network. Devices connected to this switch were assigned an IP address from the 172.16.1.0/24 subnet

- The other Stratix 5700 switch was connected to the Fa 1/2 interface of the Router and used for the Plant (Vlan2) sub- network. Devices connected to this switch were assigned an IP address from the 172.16.2.0/24 subnet.

Task: Identify and control connections.

	From	To	Direction	Controlled using
Connection	Cybersecurity LAN	Supervisory LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Cybersecurity LAN	Plant LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Supervisory LAN	Plant LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Engineering LAN	Supervisory LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Engineering LAN	Plant LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Supervisory, Plant and Engineering LAN	Internet	One way	Boundary Firewall (Cisco ASA) in the Cybersecurity LAN

3.3.16 Monitor Boundary Connections

Network traffic will be monitored for external and internal communications using a firewall, or other type of device that allows for the ability to control connection traffic. Required network traffic leaving the manufacturing system will be allowed, all other traffic will be explicitly dropped. Traffic to manufacturing system will be limited to only those machines required for monitor from corporate network to manufacturing system and machines won't be allowed internet access. Device monitoring external/ internal connection/communications will forward all logging to internal Syslog server for archival purposes.

- External Boundary communications are monitored using Cisco ASA Firewall in the Cybersecurity LAN network.

- Internal Boundary communications are monitored using Stratix 8300 series Firewall in the Work Cell.

Tool: Boundary Protection Device

The table below lists the boundary protection devices implemented

Type	Description
Allen Bradley Stratix 8300	Firewall/Router for Work Cell
Cisco ASA Firewall	Firewall/Router in the Cybersecurity LAN

Document: Boundary protection device configuration.

Refer to section 4.19 Network Boundary Protection

3.3.17 Actions that can be performed with/without Authentication

Authentication Required to Physically/Logically Interact with Device?								
	Engineering Workstation	**Supervisory PLC**	**HMI**	**Controller**	**Local Historian**	**OPC Server**	**VLAN switches**	**Boundary router**
Physical Interaction (All Users*)	Y	N	N	Y	Y	Y	Y	Y
Logical/Network Interaction (All Users*)	Y	Y	Y	Y	Y	Y	Y	Y

HMI User Actions Requiring Authentication			
	View Process Status	**Modify Process Setpoints**	**Silence/Clear Alarms**
All Users*	N	Y	Y

Engineering Workstation User Actions Requiring Authentication				
	Login to Workstation	**View/Modify PLC Logic**	**Access Engineering Files**	**All Other Actions**
All Users*	Y	Y	Y	Y

1385

1386

Historian User Actions Requiring Authentication				
	View Historical Data	**Modify Historical Data**	**Modify Configuration**	**Login to Server Desktop/CLI**
All Users*	Y	Y	Y	Y

1387

OPC Server User Actions Requiring Authentication		
	Modify Configuration	**Login to Desktop/CLI**
All Users*	Y	Y

1388

Controller User Actions Requiring Authentication			
	Modify Configuration	**Login to Desktop/CLI**	**Modify Control Logic**
All Users*	Y	Y	Y

1389

1390

VLAN switches User Actions Requiring Authentication		
	Modify Configuration	**View switch status**
All Users*	Y	Y

1391

	PLC Actions Requiring Authentication				
	Power On/Off	**Reboot**	**Process Interaction (Run/Stop/Reset)**	**Modify Logic**	**Change Mode (Run/Config)**
All Users*	N	N	N	Y	Y

1392 * Authentication for *all users* does not imply authorization has been granted to any specific

1393

1394 ### 3.3.18 Network Connections

1395 All network connection with manufacturing system will be documented to include port numbers
1396 and cables will be labeled indicating their designated purpose.

1397 All connection will be reviewed and authorized before being placed into production.

1398 ### 3.3.19 Remote Maintenance

1399 Remote maintenance activities will be coordinated and approved before vendor access is
1400 allowed. All remote maintenance activities provided by a vendor will be controlled and
1401 monitored to ensure no harmful or malicious activities occur. Any vendors or contractors
1402 connecting to Westman for remote maintenance will require approval before connecting.
1403 Requests will be documented to ensure proper audit trail for activity conducted within
1404 manufacturing system. See reference for detailed plan.

1405 ### 3.3.20 System Maintenance

1406 Reference System Maintenance within Security Policy

1407 ### 3.3.21 Change Control

1408 Changes to manufacturing system will be submitted to a change control process ensuring that all
1409 applicable parties are aware and agree on actions being performed. Management will have final
1410 approval since production could be affected by down time.

Changes within the manufacturing systems will be scheduled during non-production hours as not to affect processing within manufacturing system. Changes will be reviewed and authorized before being implemented. Potential system performance issues from the potential change must be determined before the change is made. Once changes have been completed a review will be conducted ensuring same security level continues to be maintained after changes have been implemented.

Responsible parties will evaluate security impact on change controls being performed within the manufacturing system environment. Change control reviewers will have final say for changes being implemented along with changes having an impact on security.

Below is a list of items that need to be change controlled

Device Name	Item Type	Details
Engineering Workstation	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), Plant apps (Factory Talk, RSLinx etc.)
	Hardware	Storage and Memory upgrade
OPC Server	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), Plant apps (PI, FactoryTalk Services Platform, RSLINX, Matrikon OPC)
	Hardware	Storage and Memory upgrade
Historian VM	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), SQL Server patches,
	Hardware	Storage and Memory upgrade
Plant Simulator	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.)
	Hardware	Storage and Memory upgrade
Controller Host	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), Plant apps (MATLAB, Matrikon OPC)
	Hardware	Storage and Memory upgrade
HMI Host	Software	OS Patches (Windows), BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), Plant apps (FactoryTalk View Site, FT Services Platform, FT View Studio)
	Hardware	Storage and Memory upgrade

PLC	Software	Firmware upgrade and any type of configuration change
Allen Bradley Boundary Router	Software	Firmware upgrade, Firewall rules and any type of configuration change
Allen Bradley Layer-2 Switches	Software	Firmware upgrade and any type of configuration change
Cisco ASA Firewall	Software	Firmware upgrade, Firewall rules and any type of configuration change
Switches	Software	Firmware upgrade and any type of configuration change
Active Directory	Software	Group Policy deployment, User account creation/modification
Symantec Antivirus	Software	Antivirus version upgrades, Any Endpoint policy deployment via Symantec Manager
Nessus	Software	Running vulnerability scan(s)

1423

1424 ### 3.3.22 Media Sanitization for Devices

Assets / Device type	Method used	Details
Hard Drives on servers, workstations	**CLEAR**	Tool: DBAN [4], Category: Software, Type: Open-Source Instructions: (1) Download and create a bootable media of DBAN (2) Boot the server using the bootable media (3) Follow the on-screen instructions to run the multiple passes of data wipe. (4) Once complete, verify if wipe was successful by booting the server without the DBAN media

[4] https://dban.org/

Allen Bradley 8300 Boundary Router	**CLEAR**	The below instructions are found in the Allen Bradley manual for Stratix Managed Switches[5] Clear: (1) Login to Web Admin console (2) Navigate to **Device Management | Restart/Reset** in the menu (3) Select **Reset Switch to Factory Defaults** and click on Submit
Allen Bradley 5700 L2 switch	**CLEAR**	The below instructions are found in the Allen Bradley manual for Stratix Managed Switches [6] Clear: (1) Login to Web Admin console (2) Navigate to **Device Management | Restart/Reset** in the menu (3) Select **Reset Switch to Factory Defaults** and click on Submit
HMI	**CLEAR**	The HMI program is installed on a Windows 7 system. To uninstall this program (1) Login to the Windows system via an admin account. Go to **Control Panel** >> **Programs and Features** (2) Select and Uninstall all "**FactoryTalk**®" components. Reboot the machine if required.
Historian	**CLEAR**	This consists of 2 parts – Historian Suite and SQL Server database. Both are installed on a Windows system. They can be treated as any other program/software on a Windows system. To uninstall Historian program: (1) Login to the Windows system via an admin account. Go to **Control Panel** >> **Programs and Features** (2) Select and uninstall all "**FactoryTalk**®" components. Reboot the machine if required. OR (1) Click on Start Menu >> Programs >> Rockwell Software >> Factory Talk Site Edition >> Uninstall Factory Talk.

http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

		To uninstall the SQL Database (1) From **Program and Features** select "SQL Server Compact Edition" and uninstall it.
Allen Bradley PLC	**CLEAR**	The Allen Bradley PLC is a modular chassis consisting of different modules such as DeviceNet Scanner, ControlLogix Module, EthernetIP Module and HIPROM time. To reset the HIPROM Time Module: (1) Follow the instructions as per Allen Bradley HIPROM [7] manual and set the Rotary Switch to 888. To reset the DeviceNet Scanner Module (2) Follow the instructions as per Allen Bradley DeviceNet [8] manual and set the Rotary Switch to 888. To clear the ControlLogix 5571 Module, Refer to the below instructions. These are defined in Allen Bradley ControlLogix 5000 Manual[9] . Clear the Program from On-board NVS Memory If your application allows it, follow these steps to clear the program from the 1756-L7x controller's on-board NVS memory. 1. Remove the ESM from the controller. 2. Remove power from the controller. You can remove power in either of the following two ways: • Turn power off to the chassis while the controller is installed in the chassis. • Remove the controller from a powered chassis. 3. Reinstall the ESM into the controller. 4. Restore power to the controller in one of two ways.

1425

1426

http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um538_-en-p.pdf

http://literature.rockwellautomation.com/idc/groups/literature/documents/in/1756-in566_-en-p.pdf

http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um001_-en-p.pdf

3.3.23 Backup Procedures

Servers, Workstations:

Refer Section 9.4.5 Veeam Backup and Replication

Network Devices:

1. Launch the TFTP server on Engineering Workstation
2. SSH to the switch / router and run the below commands

```
Router# enable
Router# copy running-config tftp
Address or name of remote host []? <IP-address of Workstation>
Destination filename [router-confg]? <Enter a file-name>
```

3. Ensure to manually save the configuration backup at a central secure location

ICS Devices:

Follow the Manufacturer's product manual to perform a backup

Ensure to manually save the configuration backup at a central secure location

3.3.24 Priority Analysis

Manufacturing system will be evaluated quarterly to identify devices importance. Devices importance will be used to provide a criticality report containing the minimum pieces of equipment required to continue productions.

3.3.25 Vendor Requirements

Service Level Agreements (SLA) will be outlined and discussed, along with the need for required notification when an employee transfers departments', leaves the company, or is terminated that had direct network connectivity into Westman's network

Service Level Agreement:

Service Level Agreement (SLA)

for *Vendor*

by

Westman

Effective Date: 02-22-2019

Document Owner:	Westman President

Version

Version	Date	Description	Author
1.0	02-22-2019	Service Level Agreement	Westman President

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this Agreement.)

Approvers	Role	Signed	Approval Date
Westman	Customer		2-22-2019
Vendor	Service Provider		2-22-2019

Agreement Overview

This Agreement represents a Service Level Agreement ("SLA" or "Agreement") between Westman and Vendor (Service Provider) for the provisioning of IT/OT services required to support and sustain the Product or service.

This Agreement remains valid until superseded by a revised agreement mutually endorsed by the stakeholders.

This Agreement outlines the parameters of all IT/OT services covered as they are mutually understood by the primary stakeholders. This Agreement does not supersede current processes and procedures unless explicitly stated herein.

Goals and Objectives

The **purpose** of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent IT/OT service support and delivery to Westman by the Service Provider(s).

The **goal** of this Agreement is to obtain mutual understanding for IT/OT services provision between the Service Provider and Westman.

The **objectives** of this Agreement are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present a clear, concise and measurable description of service provision to the customer.
- Match perceptions of expected service provision with actual service support and delivery.

Stakeholders

The following Service Provider and Westman will be used as the basis of the Agreement and represent the **primary stakeholders** associated with this SLA:

IT Service Provider: Service Provider
IT/OT Customer: Westman

Periodic Review

This Agreement is valid from the **Effective Date** outlined herein and is valid until further notice. This Agreement should be reviewed at a minimum once per fiscal year; however, in lieu of a review during any period specified, the current Agreement will remain in effect.

The **Business Relationship Manager** ("Document Owner") is responsible for facilitating regular reviews of this document. Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all affected parties. The Document Owner will incorporate all subsequent revisions and obtain mutual agreements / approvals as required.

Business Relationship Manager: Westman (President)
Review Period: Yearly (12 months)
Previous Review Date: 02-22-2019
Next Review Date: 02-22-2020

Service Agreement

The following detailed service parameters are the responsibility of the Service Provider in the ongoing support of this Agreement.

Service Scope

The following Services are covered by this Agreement:

- Apply system updates to manufacturing environment per vendor's recommendation
- Apply system updates to IT equipment when patches are released per vendor.
- Backup configure information for all IT/OT equipment within Westman
- Ensure cybersecurity tools are operating correctly within the environment
- Provide liaison service between OT vendor and Westman
- Product recommendation for new equipment being purchased and installed with Westman's manufacturing environment
- Manned telephone support
- Monitored email support

- Remote assistance using Remote Desktop and a Virtual Private Network where available
- Planned or Emergency Onsite assistance (extra costs apply)
- Monthly system health check

Customer Requirements

Westman's responsibilities and/or requirements in support of this Agreement include:

- Payment for all support costs at the agreed interval.
- Reasonable availability of customer representative(s) when resolving a service related incident or request.

Service Provider Requirements

Service Provider responsibilities and/or requirements in support of this Agreement include:

- Meeting response times associated with service related incidents.
- Appropriate notification to Customer for all scheduled maintenance.

Service Assumptions

Assumptions related to in-scope services and/or components include:

Changes to services will be communicated and documented to all stakeholders.

Service Management

Effective support of in-scope services is a result of maintaining consistent service levels. The following sections provide relevant details on service availability, monitoring of in-scope services and related components.

Service Availability

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

- Telephone support: 8:00 A.M. to 5:00 P.M. Monday – Friday
    - Calls received out of office hours will be forwarded to a mobile phone and best efforts will be made to answer / action the call, however there will be a backup answer phone service
- Email support: Monitored 8:00 A.M. to 5:00 P.M. Monday – Friday
    - Emails received outside of office hours will be collected, however no action can be guaranteed until the next working day
- Onsite assistance guaranteed within 72 hours during the business week

Service Requests

In support of services outlined in this Agreement, the Service Provider will respond to service related incidents and/or requests submitted by Westman within the following time frames:

- 0-8 hours (during business hours) for issues classified as **High** priority.
- Within 48 hours for issues classified as **Medium** priority.
- Within 5 working days for issues classified as **Low** priority.

Remote assistance will be provided in-line with the above timescales dependent on the priority of the support request.

Personal Changes:

When an individual user with remote access leaves service provider, is transferred, or is terminated the service provider will notify Westman. If user had access to Westman's network, that access will be disabled, or deleted as soon as possible. System account passwords the service provider had will need to be changed to ensure user access into the network has been completely removed.

DETECT

3.3.26 Event Logging

Devices within manufacturing system shall be configured to send log data to central repository (Syslog Server) when supported. Logs sent from devices allow additional forensics analysis, which will be useful after a cybersecurity event. Westman logs all devices events alerts to central log server for review and archive purpose. Recorded events help identify any malicious activity within the manufacturing systems. Logs will be checked periodically looking for abnormal alerts generated from manufacturing system. See reference for additional information.

3.3.27 Event Impacts

Logged events will be examined to determine the impact if any against the manufacturing system. Events impacting manufacturing system will be reviewed to determine correlation with risk assessment outcomes. Once correlation has been completed action will be taken if required to increase cybersecurity posture to lessen future threats.

3.3.28 Monitor

All personnel within the manufacturing system will be required to sign-in upon entering ICS environment with date and time of entry, including when leaving work space. Any person found in violation of mandatory sign-in/sign-out sheet will be escorted out of the manufacturing environment. Individuals will be challenged to ensure they are employees or are being escorted around the environment.

All network switches have been configured for port security, so unauthorized devices won't be allowed access to the manufacturing network without prior approval.

Weekly wireless scans will be completed using a laptop within manufacturing system. Rouge or unknown wireless devices will be brought to management's attention for additional review.

Periodic software scans with be performed on devices within manufacturing system to detect any unauthorized software.

Switch logs within manufacturing system will be checked regularly to ensure no rogue devices have attempted to connect. Output from switch logs will be compared against hardware inventory performed in.

3.3.29 Forensics

Syslog server will be used for collection of system logs. Logs can analysis to understand the attack target along with determining the method that was used during the attack against devices within manufacturing system. In addition, tools such as Security Onion and Wireshark may be used to analyze events and packet captures respectively.

3.3.30 Detect non-essential capabilities

System scanning/auditing tool will be used to identify non-essential software applications installed on devices within manufacturing system. Software not required for operations will be removed and baseline configuration updated to reflect new configuration state.

3.3.31 Ensure resources are Maintained

Systems performance and resources can have a drastic effect on manufacturing process. Individual in charge of manufacturing system will be responsible for performing daily checks on all systems within the manufacturing system environment (OT). Checks will include, but not limited to physical observation of all operational components ensuring any warning lights or other area of concern are investigated further. System logs of all manufacturing devices will be checked at the beginning and end of every shift looking for any deviation from the normal baseline performance.

RESPOND

3.3.32 Fire Protection Systems

Fire protection for a manufacturing environment should be designed to safeguard electrical equipment. Manufacturing systems requiring protection can be PLCs', HMIs', Robots, Machining equipment, computers and other required devices. Fire Protection should be designed and implemented to protect human life first and equipment second. Installed fire protection

systems will be certified compliant with existing/new environment by a licensed and accredited vendor. Check industry standards for any required baselines.

3.3.33 Emergency and Safety Systems

Emergency and Safety Systems will compile with Local, State, and Federal laws. This is to include safety regulations for workers' safety from Occupational Safety and Health Administration (OSHA). Industry regulation for safety will be followed per guidance from regulating industry.

Fire Protection Systems will compile with Local, State, and Federal laws. This is to include Fire Protection Systems specially designed for manufacturing process. Fire Protection System will place emphasis on human safety first and for most, before concern for manufacturing system. Fire Protection Systems will be checked minimum once per year unless shorter intervals are required from superseding regulations.

Only Industry approved Environmental Controls will be used within manufacturing systems, to included compliance with all Local, State, Federal laws. Environmental Control will be implemented to place human/community safety first before manufacturing systems.

3.3.34 Detected Events

Detected cybersecurity event notification will be investigated to determine root cause and appropriate remediation steps will be taken to clear events returning the organization / manufacturing system to known good operating state.

This can be done by reviewing the logs or events in Graylog and/or Security Onion

3.3.35 Vulnerability Management Process

Vulnerability management is an essential component of any information security program and the process of vulnerability assessment is vital to effective vulnerability management.

Vulnerability Scanning and Management Tools

Tenable- Nessus will be used to perform vulnerability scans. The Results report generated by Nessus at the completion of the scan, is then fed into NamicSoft which is a vulnerability management, parsing and reporting tool.

NamicSoft can create customized reports and logically group results for a consistent workflow within the organization. The reports are reviewed by the foreman and then shared with the machine operators.

Vulnerability Scan Targets

All devices connected to both Plant and Supervisory network segments are scanned. The IT Staff will configure a scan for all network segments of Westman.

A new scan can be established, or an existing one changed, by submitting a request to the Director of Operations.

Vulnerability Scan Frequency/Schedule

Scans are performed by the IT Staff on an on-demand, per-request basis as needed. The IT manager shall make provisions for an assessment once per month.

- All IT/OT device scans should be scheduled in the 2 weeks of maintenance window in December of each year.
- All device scans should be performed during hours appropriate to the business needs of the organization and to minimize disruption to normal operations
- Any new device discovered needs to be classified under its appropriate group.

General Rules

- The Engineers or IT staff will not make any temporary changes to information systems, for the sole purpose of "passing" an assessment. Vulnerabilities on information systems shall be mitigated and eliminated through proper analyses and repair methodologies.
- No devices connected to the network shall be specifically configured to block vulnerability scans from authorized scanning engines.
- Use caution when running vulnerability scans against OT Networks such as the Supervisory LAN and Field LAN Network. Scans should be scheduled off hours and during periods of maintenance.
- It is recommended to run authenticated scans from the vulnerability scanner.

Vulnerability Reporting

Upon completion of a vulnerability scan, the data is fed into NamicSoft out of which report is generated. A report will always be generated as proof that an assessment occurred.

All IT/OT devices are organized into appropriate groups in NamicSoft as per the system they reside in. A device may belong to one or more systems. Reporting is done system wise so that the devices and vulnerabilities can more easily be distributed to the IT Staff, Manager and Director of Operations. Below is a table of type of reports that will be sent out.

Status Reports	Frequency	Purpose
Host table with affected vulnerabilities	Monthly	Information is presented for each host.
Vulnerability Assessment Report	Monthly	Information is presented for both scanned networks.

Host specific report	Ad-hoc	Information is presented for requested host.
Mitigated vulnerabilities report	Post remediation	Upon re-scanning a host to check if vulnerabilities have been mitigated or not

Remediation Management and Priorities

All vulnerabilities discovered must be analyzed by the Director, Control Engineers with assistance from IT Team and OT Contractor (if needed) to decide on the next course of action.

All vulnerabilities discovered should be remediated.

The below chart should be used for remediation timelines

Severity	Description	Remediation time
Critical	Nessus uses Common Vulnerability Scoring System (CVSS) for rating vulnerabilities. A Critical vulnerability has a CVSS base score of 9.0 or 10.	15 days of discovery
High	High-severity vulnerabilities have a CVSS score between 7.0 and 8.9.	30 days of discovery
Medium	Medium-severity vulnerabilities have a CVSS score of 4.0 to 6.9 and can be mitigated within an extended time frame.	45 days of discovery
Low	Low-severity vulnerabilities are defined with a CVSS score of 1.0 to 3.9. Not all low vulnerabilities can be mitigated easily due to applications and normal operating system operations. These should be documented	180 days of discovery
Info	Info level do not present security risk and are listed for informational purposes only. It is optional to remediate them.	Not required to remediate

Exceptions Management

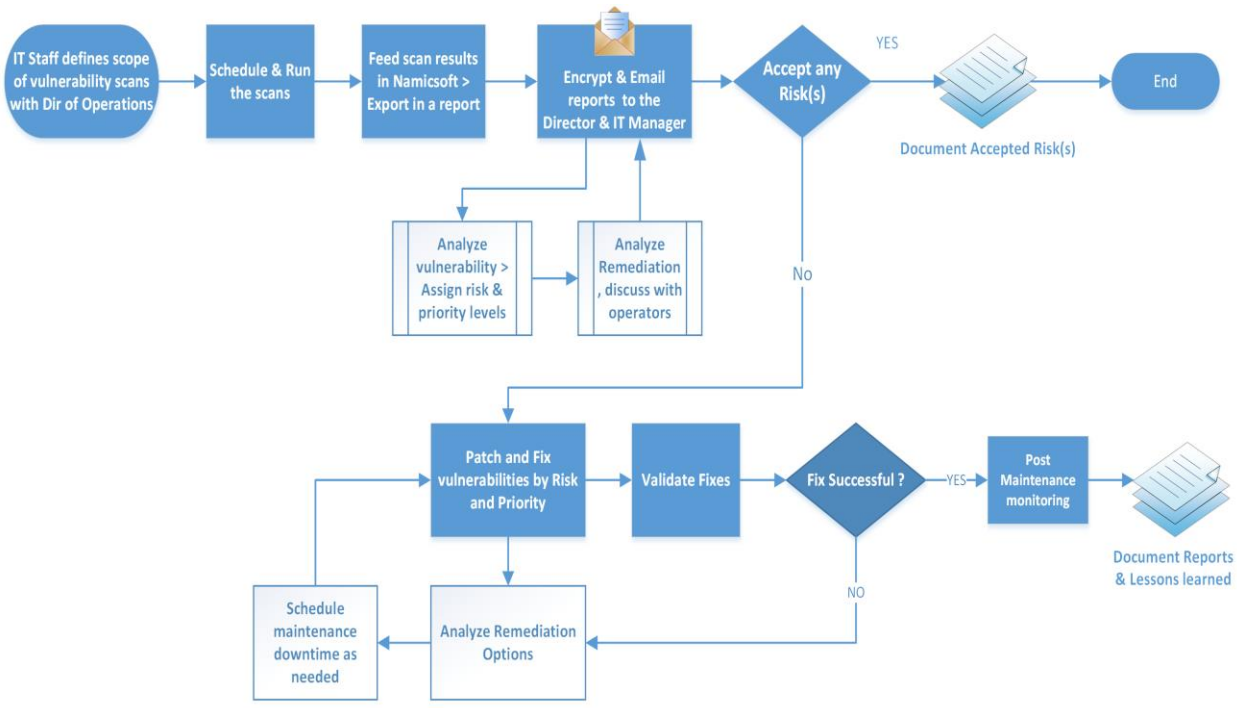
Any exceptions to this policy, such as exemption from the vulnerability assessment process must be internally discussed and approved by the Foreman.

Vulnerabilities may exist in operating systems, applications, web applications or OT devices. While every effort must be made to correct issues, some vulnerabilities cannot be remediated. Vendors may have appliances that are not patched, services may be exposed for proper application operations, and systems may still be commissioned that are considered end-of-life by the developer and manufacturer. In these cases, additional protections may be required to mitigate the vulnerability. Exceptions may also be made so that the vulnerabilities are not identified as items of risk to the system and organization.

False Positives identification may be documented through emails or the NamicSoft tool with the security staff. Acceptable Risk exceptions must be requested through the IT Team with an explanation containing:

- Mitigating controls – what changes, tools, or procedures have been implemented to minimize the risk.
- Risk acceptance explanation – details as to why this risk is not relevant to the company and systems.
- Risk analysis – if the vulnerability is indeed compromised, what risk and systems will be affected.

Process Overview



Westman Chemicals Vulnerability Management Process

RECOVER

3.3.36 Recovery Plan

Purpose and Objective:
Westman developed this incident recovery plan (IRP) to be used in the event of a significant disruption to the features listed in the table below. The goal of this plan is to outline the key recovery steps to be performed during and after a disruption working to return to normal operations as quickly as possible.

Scope:
The scope of this IRP document addresses technical recovery only in the event of a significant disruption. The intent of the IRP is to be used in conjunction with the business continuity plan (BCP) Westman developed. A IRP is a subset of the overall recovery process contained in the BCP. Plans for the recovery of people, infrastructure, and internal and external dependencies not directly relevant to the technical recovery outlined herein are included in the Business Continuity Plan and/or the Corporate Incident Response and Incident Management plans Westman has in place.

The specific objectives of this incident recovery plan are to:

- Establish a core group of leaders to assess the technical ramifications of a situation;
- Set technical priorities for the recovery team during the recovery period;
- Minimize the impact of the disruption to the impacted features and business groups;
- Stage restoration of operations to back full processing capabilities;
- Enable rollback operations once disruption has been resolved and determined appropriate by recovery team.

Within the recovery procedures there are significant dependencies between and supporting technical groups within and outside Westman. This plan is designed to identify the steps that are expected to take to coordinate with other groups / vendors to enable their own recovery. This plan is not intended to outline all the steps or recovery procedures that other departments need to take in the event of a disruption, or in the recovery from a disruption.

Incident Recovery Strategies:

The overall IR strategy of Westman is summarized in Section 3.6 Incident Recovery Plan.

3.4 Risk Management Document Example

Risk Management Strategy

for

Westman

Document Owner:	Director of Operations, Westman

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	CEO/General Manager		4-22-2018

This Risk Management Plan defines how risks associated with the Westman will be identified, analyzed, and managed. This document can be used by the Director of Operations and Executives to foresee risks, estimate impacts, and define responses to issues.

3.4.1 Scope

Any employee, contractor, or individual with access to the organization's systems or data.

3.4.2 Risk Management Process

Process

The overall process involves Identifying, Analysis, Categorizing, Reporting and Remediating. Risks will be identified as early as possible in the project to minimize their impact. The steps for accomplishing this are outlined in the following sections.

Risk Identification

Risk identification will involve the Company's Director of Operations, Control Engineers, IT Manager, evaluation of environmental factors, organizational culture and the project management plan including the project scope. There are many different types of threats that can affect IT and OT infrastructure. These can include:

- Technical threats — disruption caused by technological advances or failures
- Structural threats — anything related to the building that houses your IT infrastructure that could cause it to be harmed
- Financial threats — If the business loses funding or experiences another significant financial change
- Human threats — human error or loss of important individual
- Natural threats — weather and natural disasters such as earthquakes, tornadoes, and floods

A Risk Management Log will be generated and updated as needed, a sample of which is shown in the latter half of this document

Software tools such as CSET[10] will be used to perform RISK Assessments. The reports generated will be discussed with the CEO.

Additionally, the Control Engineers and Director of Operations will subscribe to NVD, USCERT, ICS-CERT and ISACS alert feeds to keep up with the latest vulnerabilities.

This is an iterative process. As the program progresses, more information will be gained about the program and the risk statement will be adjusted to reflect the current understanding. New risks will be identified as the project progresses through the life cycle.

Risk Analysis

All risks identified either manually or via CSET will be assessed to identify impact on operations. Qualification will be used to determine which risks are the top risks and which ones can be ignored.

Qualitative Risk Analysis

The probability and impact of occurrence for each identified risk will be assessed by the Director of Operations with input from the control engineers using the following approach:

Probability

- High – Greater than <70%> probability of occurrence in a year

[10] CSET: https://ics-cert.us-cert.gov/Assessments

- Medium – Between <30%> and <70%> probability of occurrence in a year
- Low – Below <30%> probability of occurrence in a year

Impact

- High – Risk that has the potential to greatly impact project cost, project schedule or performance
- Medium – Risk that has the potential to slightly impact project cost, project schedule or performance
- Low – Risk that has relatively minor impact on cost, schedule or performance

Quantitative Risk Analysis

This involves assigning a numeric value to the risk calculated as the product of probability of occurrence and impact score. Analysis of risk events that have been prioritized using the qualitative risk analysis process and their effect on project activities will be estimated, a numerical rating applied to each risk based on this analysis, and then documented in the risk management log.

3.4.3 Risk Monitor and Control

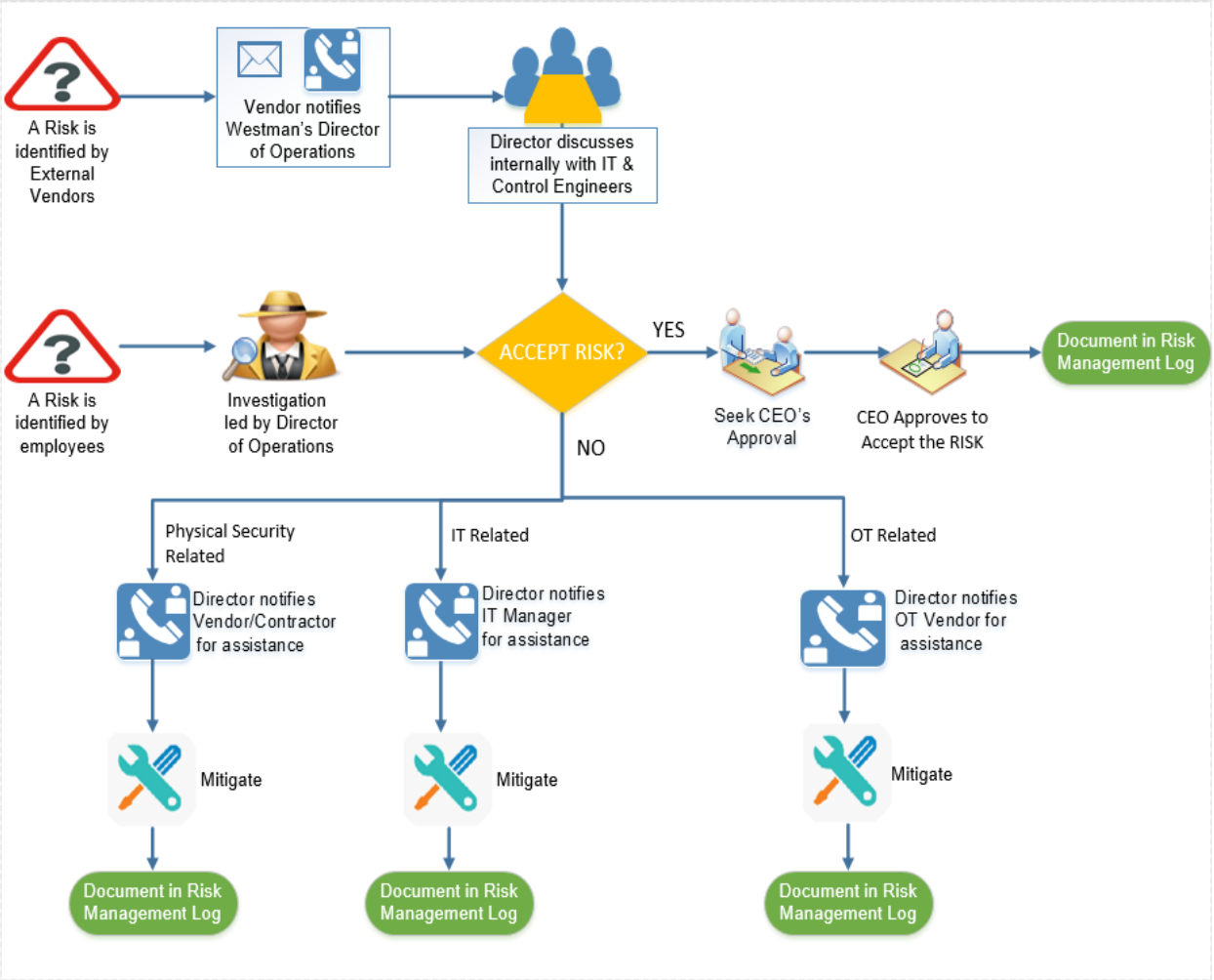
The Director of Operations and IT Team will conduct yearly risk assessments which includes CSET assessments, vulnerability scans of the manufacturing system that take into account vulnerabilities and potential impact to the manufacturing operations. An identified risk can be bought to Director's attention either by Westman's employees or by external contractors.

The IT Team will scan the IT and OT assets when called upon; with Nessus to monitor for any software-based risks. The Nessus results will be fed into NamicSoft. Reports will be generated out of this tool and shared with the process owners. Any other type of risks like hardware based, physical, environmental will be identified and documented manually.

All software-based vulnerabilities discovered using Nessus should be mitigated as per the Vulnerability Management Plan.

If a software vulnerability has been remediated; a Nessus scan be re-run to see whether the situation has changed in a way that affects the manufacturing operations. For any corrective action has been taken, the risk management log will be updated.

3.4.4 Risk Notification Process



3.4.5 Risk Response / Remediation Strategy

For each major risk, one of the following approaches will be selected to address it:

- **Avoid** – eliminate the threat by eliminating the cause
- **Mitigate** – Identify ways to reduce the probability or the impact of the risk
- **Accept** – Nothing will be done
- **Transfer** – Make another party responsible for the risk (buy insurance, outsourcing, etc.)

For each risk that will be mitigated, the team will identify ways to prevent the risk from re-occurring or reduce its impact or probability of occurring. This may include

- Prototyping.
- Adding tasks to the project schedule
- Determining and allocating resources.

For each risk that needs to be "Accepted", a document containing the list of accepted risks will be maintained by the Director of Operations.

The Director will reach out to an IT/OT Vendor for any risks and request remediation assistance.

3.4.6 Risk Appetite

Risk appetite - is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. [4]

Risk Appetite scale [5]:

- High - the manufacturing system accepts disciplined risk taking because the organization has determined the potential benefits outweigh the potential risk.
- Moderate - the manufacturing system accepts some risk taking, assuming the organization has reviewed the potential benefits and potential risks.
- Low - the manufacturing system accepts minimal risk taking.
- None - the manufacturing system accepts no risk taking because the risk is intolerable.

3.4.7 Risk Tolerance

Risk tolerance - is the acceptable level of variance in performance relative to the achievement of objectives. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite. [4]

Risk tolerance scale [6]:

- Low - the level of risk will not considerably impact the ability of the manufacturing system to meet its mission objectives.
- Moderate - the level of risk may impact the ability of the manufacturing system to meet its mission objectives.
- High - the level of risk will significantly impact the ability of the manufacturing system to meet its mission objectives.

3.4.8 Risk Categories

Risk Categories are used to classify a risk. This table represents a sample of potential categories that may be applied to each risk.

- Safety - the risk that human and/or environmental safety are compromised by an incident in the manufacturing system.
- Production - the risk that product quality and/or production goals are compromised by an incident in the manufacturing system.
- Trade Secrets - the risk that intellectual property and sensitive business data are compromised by an incident in the manufacturing system.

1904

Risk Category	Risk Tolerance	Risk Appetite	Mission Objectives
Safety	Moderate	Moderate	Maintain human safety
			Maintain environmental safety
Production	Moderate	High	Maintain quality of product
			Maintain production goals
Trade Secrets	Moderate	Moderate	Maintain trade secrets

1905

1906 ### 3.4.9 Risk Reporting

1907 This table describes the frequency and format of how the Director or IT Manager will document,
1908 analyze, communicate, and escalate outcomes of the risk management processes.
1909

Reporting Method	Description	Frequency
Risk Management log	A document to report the results of risk identification, analysis, and response planning	Twice a year
CSET Report	A document describing Risk assessment results	Twice a year
NamicSoft report	A document containing results of Nessus vulnerability scans.	Manual/Post vulnerability assessment

1910

1911 The Director will share the results of risk assessments (either the Risk Management Log or
1912 CSET Report) with the CEO.

1913

3.4.10 Sample Risk Management Log

A Risk Log will be maintained by the Director of Operations and IT manager. These will be reviewed in the project team meetings. This log captures the results of a qualitative and quantitative risk analysis and the results of planning for response.

Risk	**Category (Technical, Management, Contractual, External)**	**Probability (High /** Likely to occur =3, Medium / May or May not occur =2, Low / Unlikely =1)	**Impact (**High = 3, Medium = 2, Low =1)	**Score (Product of Probability x Impact 1-3 Green 4-6 Yellow 7-9 - Red)**	**Risk Mitigation Strategy** (e.g. Avoid, Transfer, Mitigate or Accept the risk)	**Actions required**	**Status (Open, closed, In Progress)**	**Due Date**

3.4.11 Periodic Review

This document will be reviewed and updated annually by the Director in consultation with the IT Manager.

Annual reviews will be conducted determining component value within the manufacturing process being performed. Values will be used to determine required devices for continued manufacturing process and the effects if a cyber incident occurs against a device.

3.4.12 Asset Criticality Matrix

After a list of Westman assets or systems of value requiring protection have been identified by the Hardware Inventory process, they will be assigned a value. Asset Value is the degree of impact that would be caused by the unavailability, malfunctioning or destruction of the asset.

Westman will use the following scale to calculate Asset value.

ASSET VALUE	
Critical	10
High	7-9
Medium	3-6
Low	1-2

Critical – Loss or damage of this asset would have grave / serious impact to the Operations of the Manufacturing system directly impacting production. This can result in total loss of primary services, core processes or functions. These assets are single point of failure.

High - Loss or damage of this asset would have serious impact to the Operations of the Manufacturing system directly impacting production. This can result in major loss of primary services, core processes or functions. These assets can also be single point of failure.

Medium - Loss or damage of this asset would have moderate impact to the Operations of the Manufacturing system or Production. This can result in some loss of primary services, core processes or functions.

Low - Loss or damage of this asset would have minor to no impact on the Operations of the Manufacturing system or Production. This can result in little or no loss of primary services, core processes or functions.

A list of assets belonging to Westman with assigned value is presented in the below table.

Asset	Value	Numeric Value
IT / Communication Systems	High	8
OT / Field Devices – PLC, HMI	Critical	10
OT / Machining Stations	High	8
OT / Robots	High	9
Electrical Systems	Critical	10
Utility Systems	Medium	6
Site	Medium	6

3.4.13 Definition and Acronyms

IT	Information Technology which includes devices such as servers, laptops, workstations, switches and routers.
OT	Operational Technology which includes Industrial control system devices that are used by the manufacturing process.
Vulnerability	A weakness or a flaw in the system which an attacker can exploit to gain access.

3.4.14 References

1. Risk Management plan – Maryland Department of Information Technology doit.maryland.gov/SDLC/Documents/Project%20Risk%20Managment%20Plan.doc

2. Sample Risk Management plan – State of North Dakota https://www.nd.gov/itd/sites/itd/files/legacy/services/pm/risk-management-plan-sample.pdf

3. Office of Management and Budget, “Management’s Responsibility for Enterprise Risk Management and Internal Control”, *Office of Management and Budget,* OMB Circular No. A-123, 2016. [Online]. Available:

https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf.

4. United States Agency for International Development, "U.S. Agency for International Development Risk Appetite Statement", *United States Agency for International Development*, 2018. [Online]. Available: https://www.usaid.gov/sites/default/files/documents/1868/USAID_Risk-Appetite-Statement_Jun2018.pdf.

5. Office of the Comptroller of the Currency, "Enterprise Risk Appetite Statement", *Office of the Comptroller of the Currency*, 2016. [Online]. Available: https://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/risk-appetite-statement.pdf.

3.5 Incident Response Plan Document Example

Incident Response Plan

for

Westman

Document Owner:	Director of Operations, Westman

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major revision	Director of Operations

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	CEO/General Manager		4-22-2018

3.5.1 Statement of Management commitment

Westman's leadership team is committed to information security and appropriate incident response to accidental or deliberate incident within the company. Westman has established the Incident Response Program to establish an actionable information security incident handling capability that includes preparation, detection, analysis, containment, recovery, and reporting for information security incidents. Westman's CEO oversees the Incident Response Program as a whole, supports and funds maintenance of the program and ensures that resources are appropriately maintained for preparedness.

3.5.2 Purpose

An incident can be defined as any event that, if unaddressed, may lead to a business interruption or loss. This document describes the plan for responding to information security incidents at Westman. It defines the roles and responsibilities of participants, characterization of incidents,

relationships to other policies and procedures, and reporting requirements. The purpose of this plan is to detect and react to security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

This Plan is to be executed during or after a cybersecurity incident.

3.5.3 Scope

This plan applies to all the employees of Westman.

3.5.4 Roles and Responsibilities

The Westman Incident Response Team is comprised of:

ROLE	RESPONSIBILITIES	CONTACT DETAILS
Director of Operations	• Supervise other employees and working of the organization. • Serves as a primary point of contact for any type of incident • Making sure that all employees understand how to identify and report a suspected or actual security incident • Leading the investigation for any type of incident, initiating the Security Incident Response Plan, filling out the Incident Report Form and reporting status to the CEO as needed. • Documenting details of all incidents.	Name: Phone: Email:
Control Engineer(s)	• Reporting a suspected or actual security incident to the Director. • Reporting any other operational issues or concerns to the Director • Complying with the security policies and procedures of Westman.	Names: Phone: Email:

IT Manager	• Manages access to systems and applications for internal staff. • Complying with the security policies and procedures of Westman. • Assist in investigation, troubleshooting and resolving any IT/OT related incident summoned for. • Advising the Director for any recommendations to procedures, policies and best practices.	Name: Phone: Email:
General Counsel	• Handling of any legal questions/issues relating to security incidents. • Handling of any external communications related to security incidents.	Name: Phone: Email:
HR Manager	• Handling of any personnel and disciplinary issues relating to security incidents. • Inform Law Enforcement if security incident involves data breach of sensitive information.	Name: Phone: Email:

3.5.5 Categories of Incident

Westman defines the following categories/types of incident for internal classification. These have been mentioned in the Incident Reporting Form as well.

- Intrusion
- Denial of Service
- Loss of Power
- Virus / Malware
- Social Engineering (Phishing, Phone, Email etc.)
- Data Breach
- Hardware Stolen
- User account compromise
- System Misuse
- Technical Vulnerability

3.5.6 Severity Classification

The Severity of an incident is determined based on the impact to the company and the urgency of restoration.

SEVERITY	DEFINITION
High	• All users of the company are affected • Work stoppage situation • The incident involves sensitive data breach. • The incident threatens Westman's operational goals • There is no viable workaround
Medium	• There is a viable workaround • Moderate to Low impact to the Operations. • Service interruption potentially affects specific users and does not involve sensitive or personal data breach.
Low	• No impact to operations. • Service interruption potentially affects only one person and does not involve sensitive or personal data breach.

3.5.7 Restoration Priorities

RESTORATION PRIORITIES	DEFINITION
High	• Service Restoration must be completed immediately, or significant loss of revenue, reputation, or productivity will occur.
Medium	• Service Restoration must be completed within two business days or there is a potential for significant loss of revenue, reputation or productivity.
Low	• Service Restoration can be delayed up to three or more business days without loss of revenue, reputation or productivity.

3.5.8 Incident Response Policy

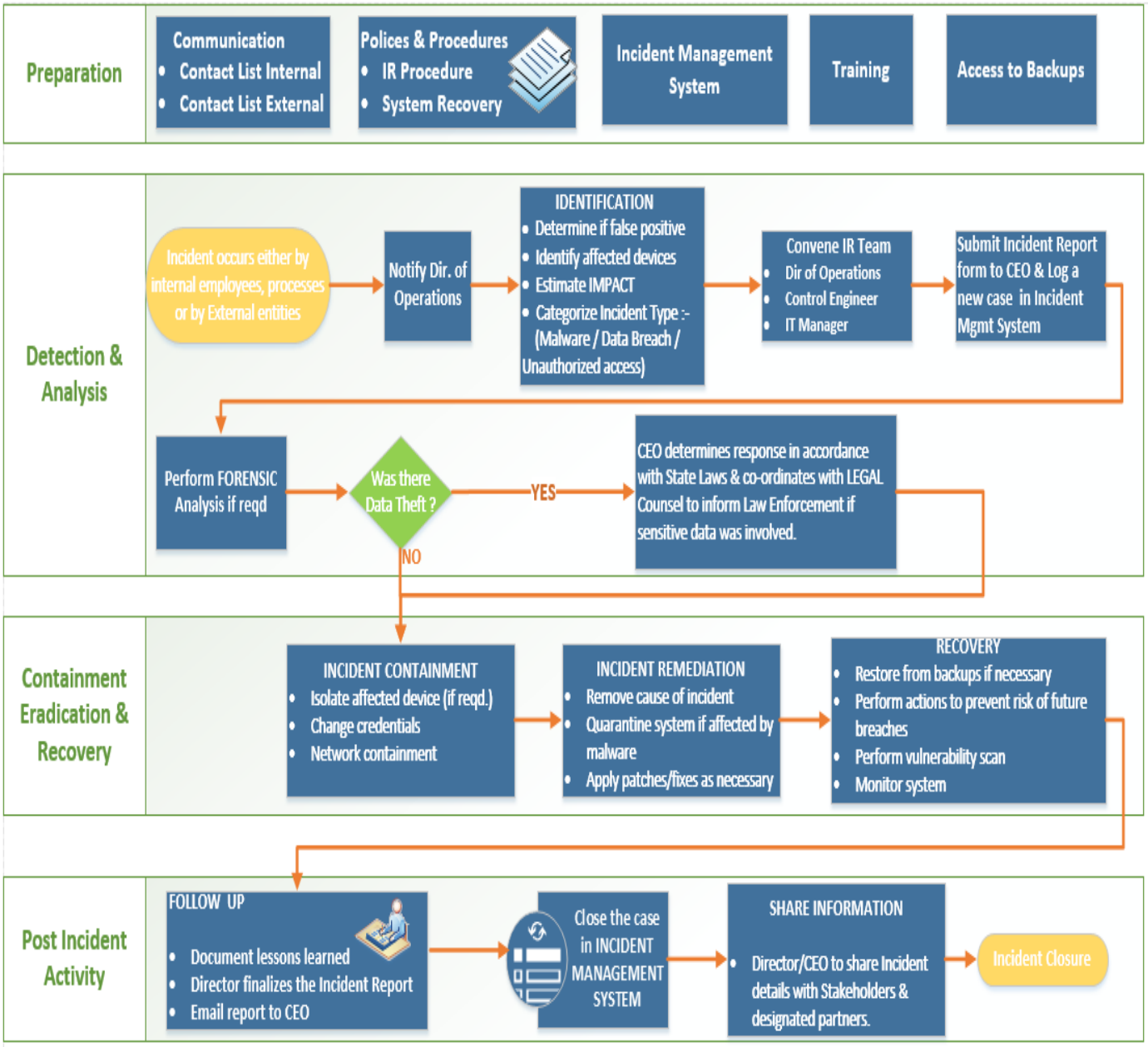
1. An incident upon detection or being reported needs to be thoroughly investigated as per the process defined under "Detection and Analysis" step of the IR process in the next section. The investigation may be performed by the Director or by convening an IR Team.
2. The incident needs to be classified as per the categories defined previously.
3. Upon Investigation, the impact to the Manufacturing system must be determined. The IR Team may co-relate detected event information with Risk assessment outcomes to achieve perspective on the incident impact across the Organization. The incident will accordingly be assigned a Severity level and reported to the CEO. The Incident Report Template form should be used for this purpose.
4. During the "Detection and Analysis" step, detailed troubleshooting or forensic analysis should be performed to determine the root cause. This may be done using in place log management tools or commercial products such as Wireshark.
5. Upon investigation, the incident must be mitigated as per the "Containment, Eradication and Recovery" step of the IR Process.
6. The Director of Operations or IT Manager will co-ordinate incident response plan with Westman stakeholders.
7. The Director of Operations or CEO will share information about any cybersecurity incidents and its mitigation with its designated sharing partners.
8. The overall Incident Response process and plan will be revised or improved after every incident. Procedures must be updated regularly to address evolving threats such as APTs, Organizational changes, Manufacturing changes and/or after any problems discovered during implementation, execution or testing
9. User awareness Training and Testing procedures will be updates after every incident.
10. The Director will communicate any changes or updates made to this policy.

3.5.9 Incident Plan Response Process / Workflow

The NIST Computer Security Incident Handling [1] Guide divides the incident response lifecycle into the following four steps:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication and Recovery
4. Post-incident Activity

Westman' IR process contains the following activities corresponding to each of the above steps:



3.5.10 Guidelines for Information Sharing

Interactions with Law Enforcement

- All communications with external law enforcement authorities should be made after consulting with the CEO/General Manager.
- The Director of Operations will co-ordinate with the CEO and IT Manager to determine and share the minimum necessary information as required for incident response.

Communications Plan

- The CEO will share information about any cybersecurity incidents and its mitigation with its designated sharing partners. Refer to the Next section for additional details
- All public communications about an incident or incident response to external parties outside of Westman are made in consultation with the CEO.
- The minimum information necessary to share for a particular incident is determined by the CEO in consultation with Director and other staff.

3.5.11 Guidelines for Reporting to Stakeholders

Overview:

- The Director of Operations will compile all the details of incident(s) occurred in consultation with the IT manager.
- The Director will share the details in the IR Report Template form with CEO/General Manager and General Counsel. This will be used to determine level of severity, allowing the company to plan according.
- The Company's leadership team consisting of CEO/General Manager, Director of Operations, General Counsel, and IT Manager will make sure all facts have been gathered relating to the security incident before addressing any concerned with outside parties.
- The Company's response needs to be consistent ensuring message being delivered will not need to be retracted or changed due to lack of clarity.

Who will be responding:

- Depending on the severity of the security incident this role can be filled by CEO/General Manager, Directory of Operations or the General Counsel.
- If the severity of a security incident requires additional resources, they should be contacted and brought in to help gather forensic information along with responding to inquiries.
    - Examples:
        - Public Relation
        - Forensic Investigator
        - IT consultant (Work in conjunction with IT Manager)
        - Security Consultant (Work in conjunction with IT Manager and Director of Operations)
        - Law Enforcement (Depends on severity)

Notification:

- General Counsel will oversee notification planning since the potential for legal actions against Westman arising from security incident in question.
- If required, an outside Public Relations firm may be required depending on the severity level of the incident to help with crafting a response.

- General Counsel approval is required for work with any outside agency.
- CEO and General Counsel will both approve all communication being sent out regarding a security incident.

Communications:

- CEO/General Manager will contact primary partners/vendors via phone call to inform them of the security incident. This should be done once all information has been gathered and a corporate response has been prepared.
- No voicemails will be left concerning the security incident in question. If recipient is unavailable schedule a follow up call.
- Director of Operations, Director of Marketing, Controller/Finance, General Counsel and IT Manager are the **only** Westman employees authorized to call partners/vendors not already contacted by CEO/General Manager.
- Responses to partners/vendors should be scripted to ensure the delivered message is consistent, while ensuring only information regarding security incident are discussed.
- Email communication will be completed as a follow-up to a phone.
- Any email communications being sent will have additional proof reading completed by either Director of Operations, Controller/Finance, General Counsel, IT Manager.
- Depending on the impact of security incident a Public Relation firm may be required to help with a response when providing communications via electronic or verbal.
- Media communication can **ONLY** be approved by CEO/General Manager and General Counsel.

Restoring Trust:

- Westman's CEO or Director of Operations with the advice consultants and Forensic experts will notify partners/vendors and customers with the steps being taken to restore and strength system security.
- Westman IT Manager, Director of Operations will discuss with employees what caused security incident and what is being done to avoid a similar issue in the future.
- Once the security incident has been resolved and all fact are known Westman leadership team will provide a full report which will be made publicly available containing facts relating to the security incident, along with the steps being taking to safe guard IT infrastructure ensuring this and future events don't happen again.

3.5.12 Incident Report Form Template

Incident Reporting Template Form			
Contact information			
Date Reported :		**Time Reported:**	
Name:	**Title:**	**Dept:**	
Office Phone:			
Details			
Date of Incident :		**Time of Incident:**	
Type of Incident - Check all that apply			
☐ Intrusion	☐ Social Engineering (Phishing, Phone,Email etc)	☐ Technical Vulnerability	
☐ Denial of Service	☐ Data breach	☐ System misuse	
☐ Loss of power	☐ Hardware stolen	☐ Others, pls specify	
☐ Virus / Malware	☐ User account compromise		
Incident Description			
Provide a brief description:			
Impact / Potential impact - Check all of the following that apply to this incident.			
☐ Loss / Compromise of Data	☐ Financial Loss		
☐ Damage to systems	☐ Other Organizations affected		
☐ Damage to public	☐ Damage to Integrity or Delivery of Goods, Services		
☐ System downtime	☐ Unknown at this time		
Provide a brief description:			
Affected System(s) information			
Host	**IP**	**Application (if any)**	**O.S**
Sensitivity of Data compromised (incase of Data loss)			
☐ Public (Information is already approved for release & unauthorized disclosure will not cause problems for the Company).			
☐ Internal Use (Information is intended for internal use within the Company or with other affiliated orgnaziations, business partners. Unauthorized disclosure may be against laws, regulations and may harm the Company or its business partners or its customers. For example: Email contacts, emails etc).			
☐ Confidential (Related to Privacy Violation. Information is private & sensitive in nature. It must be restricted to those with legitimate business need for access. Unauthorized disclosure is against laws, regulations and will harm the Company or its business partners or its Customers. For example: Trade secrets, Software code, Citizen's data etc).			
Details of the Data loss			
Provide a description of what was compromised:			
Follow up action taken so far			
☐ Law enforcement notified	☐ System disconnected from Network.		
☐ Restored backups	☐ Log files examined		
☐ AV Virus definition updated	☐ Any other action taken, pls specify		
☐ System reimaged or quarantined	☐ No action taken		
Supervisor's Name:	**Supervisor's Signature:**	**Date:**	

3.5.13 Definitions and Acronyms

CEO	Head of the organization. Serves as an escalation point.
HR Manager	An employee who deals with recruitment efforts and overall administration.
Incident	An event that is not part of normal operations that disrupts operational processes.
Director of Operations	An employee who supervises other employees and working of the organization.
Vulnerability	A weakness or flaw in the system which an attacker can exploit to gain access to.
Vulnerability Scan	The act of scanning a device or network for vulnerabilities
Control Engineer	An employee who operates the manufacturing equipment and reports to Director of Operations
Legal Counsel	Handles all legal matters. Reports to the CEO.
Stakeholders	Business Owners, System Owners, Integrators, Vendors, Human Resources Offices, Physical and Personnel Security Offices, Legal Departments, Operations Personnel.

3.5.14 References

1. NIST Publication for handing Computer Security Incident
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

3.6 Incident Recovery Plan Document Example

Incident Recovery Plan

for

Westman

Document Owner:	Director of Operations, Westman

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	CEO/General Manager		4-22-2018

3.6.1 Scope

The scope and purpose of this document is to inventory all of infrastructure and capture information relevant to the Westman's ability to recover its IT/OT environment from a cybersecurity incident. It, in turn also aims to provide an effective and efficient recovery effort.

3.6.2 Objectives

This plan has been developed to accomplish the following objectives:

1. Limit the magnitude of any loss by minimizing the duration of a critical application service interruption.
2. Assess damage, repair the damage, and activate the repaired computer center.
3. Manage the recovery operation in an organized and effective manner.

4. Prepare technology personnel to respond effectively in an incident recovery situation.

This IR Plan is to be executed during or after a cybersecurity incident.
The person discovering the incident must notify the Director of Operations or IT Manager, who collectively assume responsibility for deciding which - if any - aspects of the IR plan should be implemented, and for establishing communication with employees, management, partners and customers.

3.6.3 RPO and RTO Targets

Westman defines the following SLA's or Restoration times for operations recovery

Type of Incident	RTO [2]	RPO [2]	Restoration Priority
Environmental Disasters such as Fire, Flood.	72 hours	24 hours	High
Recovery from Virus/Malware attack	24 hours	24 hours	High
Recovery from user account compromise	24 hours	24 hours	Medium
Recovery from Data Breach	48 hours	24 hours	High
Hardware failure, System Parts Replacement	48 hours	24 hours	High

Westman's Incident Response (IR) Team will consists of the following individuals.

ROLE	RESPONSIBILITIES
Director of Operations	• Lead and oversee the entire IR process • Contact any Contractors/Vendors for assistance as needed. • Making sure that all employees understand their roles and responsibilities. • Update this document as per the Maintenance policy • Notify the CEO for any escalation issues.
CEO / President	• Assist the IR Lead (Director) in their role as required. • Make any Business decisions that are out of scope for the Director. • Serve as point of escalation for any issues.

Control Engineers, IT Staff	• Install, implement or assist in implementing any tools, hardware software and systems as required • Escalate any issues related to recovery to the Director. • Complying with this plan.
OT Contractors, Vendors	• Assist in Recovery, Troubleshooting and resolving any OT related incident summoned for • Advising the Director for any recommendations to procedures, policies and best practices. • Complying with this plan

2192

2193 ### 3.6.4 Contact Information

Name	Title	Contact Type	Contact Information
Employee A	ABC	Work	555-555-5555 ext 2
		Mobile	
		Alternate	
		Email	
Employee B	ABC	Work	555-555-5555 ext 3
		Mobile	
		Alternate	
		Email	
Employee C	ABC	Work	555-555-5555 ext 4
		Mobile	
		Alternate	
		Email	

2194

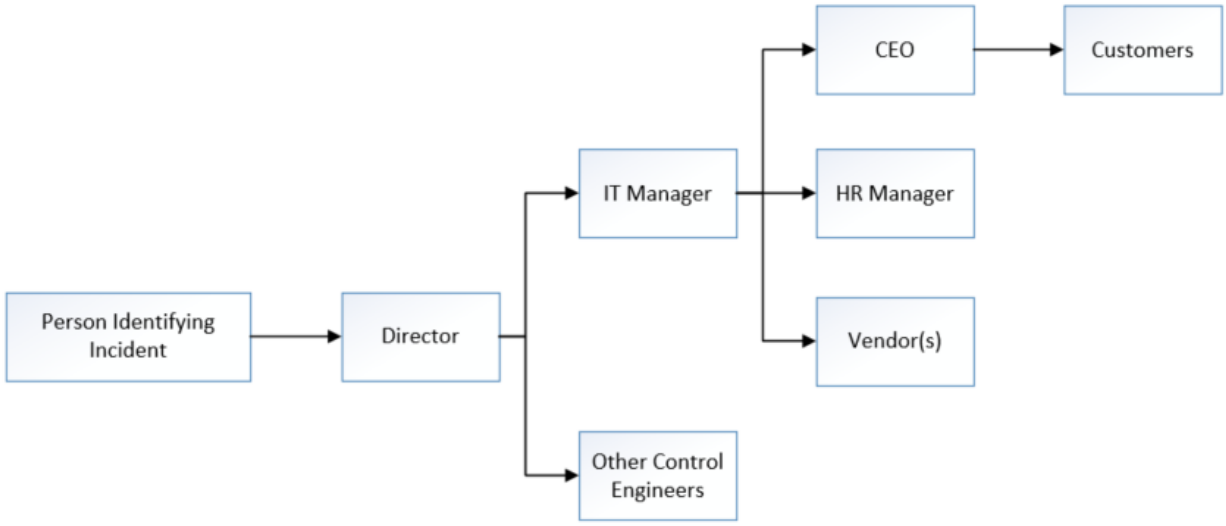
2195

2196 **External Contacts**

Name	Title	Contact Type	Contact Information
Account #		Mobile	
		Alternate	
		Email	
IT Contractor		Work	
Account #		Mobile	
		Alternate	
		Email	
OT Contractor		Work	
Account #		Mobile	
		Alternate	
		Email	
Network Provider		Work	
Account #		Mobile	
		Alternate	
		Email	
Telecom Carrier		Work	
Account #		Mobile	
		Alternate	
		Email	
Insurance Provider		Work	
Account #		Mobile	
		Alternate	
		Email	
Hardware Provider		Work	
Account #		Mobile	
		Email	

2197

3.6.5 Notification Calling Tree



3.6.6 Communications

Notification

- The Director of Operations in consultation with the IT manager and Control Engineers will periodically update the CEO, Executives on the progress of Recovery Activities.
- General Counsel will oversee notification planning since the potential for legal actions against Westman arising from security incident in question.
- If required, an outside Public Relations firm may be required depending on the severity level of the incident to help with crafting a response.
- General Counsel approval is required for work with any outside agency.

Communications

- CEO/General Manager will contact primary partners/customers via phone call to inform them about Recovery activities. This should be done once all information has been gathered and a corporate response has been prepared.
- Director of Operations, Director of Marketing, Controller/Finance, General Counsel and IT Manager are the **ONLY** Westman employees authorized to call partners/vendors not already contacted by CEO/General Manager.
- Responses to partners/vendors should be scripted to ensure the delivered message is consistent, while ensuring only information regarding security incident are discussed.
- Email communication will be completed as a follow-up to a phone.
- Any email communications being sent will have additional proof reading completed by either Director of Operations, Controller/Finance, General Counsel, IT Manager.

- Depending on the impact of security incident a Public Relation firm may be required to help with a response when providing communications via electronic or verbal.
- Media communication can **ONLY** be approved by CEO/General Manager and General Counsel.

Restoring Trust

- Westman's CEO or Director of Operations with the advice consultants and Forensic experts will notify partners/vendors and customers with the steps being taken to restore and strength system security.
- Westman's IT Manager, Director of Operations will discuss with employees what caused security incident and what is being done to avoid a similar issue in the future.
- Once the security incident has been resolved and all fact are known Westman leadership team will provide a full report which will be made publicly available containing facts relating to the security incident, along with the steps being taking to safe guard IT infrastructure ensuring this and future events don't happen again.

3.6.7 Plan Testing and Maintenance

Maintenance

- The IRP will be revised and updated after every recovery executed following a cybersecurity incident, Organizational changes, Manufacturing changes and/or after any problems discovered during implementation, execution or testing.
- The Director of Operations will be responsible for updating the document in consultation with Machine Operators and other personnel as required.
- During Maintenance periods, any changes to the IR Team must be accounted for.
- The plan will be updated after any Organizational or Manufacturing System changes.

Testing

- Walkthroughs- IR Team members will verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps or other weaknesses. The team should be familiar with procedures, equipment and operations.
- Simulations- An incident is simulated so that normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation and utilities should be thoroughly tested in a simulation test.
- Full-Interruption Testing- IR Team members will perform a full-interruption test to activate a total IRP scenario. Caution must be exercised as this type of test disrupts normal operations.

3.6.8 Hardware Information

SYSTEM TYPE	HARDWARE INFORMATION	
IT Servers	Hostname: FGS-47631EHH System Model: HP Z230 IP Address: 172.16.3.10 Network: Engineering LAN Location: Cabinet 101 Type: Physical Other: Eng. Workstation, Windows 7	Hostname: FGS-61338PSH System Model: Supermicro Z97X IP Address: 172.16.2.3 Network: Supervisory LAN Location: Cabinet 101 Type: Physical Other: Plant Simulator, Windows 7
	Hostname: FGS-613380SH System Model: Supermicro Z97X IP Address: 172.16.2.5 Network: Supervisory LAN Location: Cabinet 101 Type: Physical Other: OPC Server, Windows 7	Hostname: FGS-61338CH System Model: Supermicro Z97X IP Address: 172.16.1.5 Network: Control LAN Location: Cabinet 101 Type: Physical Other: Controller, Windows 7
	Hostname: FGS-61338HH System Model: Supermicro Z97X IP Address: 172.16.1.4 Network: Control LAN Location: Cabinet 101 Type: Physical Other: HMI Server, Windows 7	Hostname: WIN-FPVTDCDEUCR System Model: Supermicro Z97X IP Address: 172.16.2.14 Network: Supervisory LAN Location: Cabinet 101 Type: Virtual Other: Controller, Windows 2008
Network Devices	Model: Allen Bradley 8300 Management IP: 10.100.2.8 Location: Cabinet 101 Function: Boundary Router	Model: Allen Bradly 5700 Management IP: N/A Location: Cabinet 101 Function: Supervisory LAN Switch
	Model: Allen Bradly 5700 Management IP: N/A Location: Cabinet 101 Function: Control LAN SW	
OT Devices	Model: Allen Bradley Logix 5571 IP Address: 172.16.2.102 Location: Cabinet 101 Function: PLC	

3.6.9 Backup Strategy

SYSTEM TYPE	BACKUP STRATEGY
IT Servers	**Frequency** Weekdays (M-F): Directory level backup using Veeam Quarterly: Full system image backup using Veeam
Application Code	Source code is checked into a secure central network share. Server hosting the network share is backed up using Veeam.
Network Devices **Boundary Router**	**Frequency**: Quarterly - Manual using Manufacturer Instructions Note: All Allen Bradley devices support Cisco IOS Command line. 1.SSH into the network switch/router from a Windows workstation which has a TFTP server installed. 2. Log in > Enter "**enable**" mode > Issue a "**copy running-config tftp**" command > Supply the IP address of TFTP Server > Give the backup file a meaningful name > Hit Enter. 3.The backup file will then be transferred over to the Windows workstation. Once done, copy the file over to a central secure location.
OT Devices	**Frequency**: Quarterly - Manual using Manufacturer Instructions. 1.Control Engineer to either download the current image off the PLC using RSLINX Configuration Utility installed on the Workstation or pull out the MicroSD Card from the PLC and access the image using a card reader. For instructions on using RSLINX, refer to the product manual [3]

	2.Copy over the image to the central secure location before making any change or upgrading the program.

3.6.10 Recovery Procedures

- The Incident Recovery plan will be executed following a cybersecurity incident.
- Any exceptions or issues during the Recovery process must be communicated to the Director and/or IT Manager.
- Depending on the incident, and on the number and nature of the IT services affected, one or more of the following IR procedures may be activated by the IR team:

Type of Incident	Plan of Action
Environment Disaster – Fire, Flooding	1. Identify root cause, co-ordinate initial response 2. Remove damaged systems from the work cell. 3. Evaluate damage 4. Review Insurance policies and reach out to Insurance companies. 5. Procure new hardware systems as required. Reach out to a Data recovery company for data recovery from damaged hard drives.
Virus / Malware – IT / OT Systems	1. Disconnect the affected systems from the network. 2. Reach out to the IT/OT Contractor for assistance. 3. Perform a full manual Anti-virus scan on the system 4. If the Anti-virus software cannot detect or quarantine the infection, you may need to reinstall or restore the entire Operating System. Use Veeam to restore a full image backup, if the system in question is an IT system.

	5. Upon reinstalling the operating system, install all the appropriate patches to fix known vulnerabilities. 6. Depending on the nature of the virus attack, change your original passwords as these could have been compromised during the infection.
Data Theft	1. Fulfill all legal obligations. The CEO/General Manager to inform law enforcement and other customer protection agencies notifying them of breach. 2. Immediately change system credentials, account passwords to public websites (if personal data is involved) 3.Monitor in-house security controls or tools for any signs of new activity. 4. Identify and erase any new files or programs that may have been installed as part of this attack. Use system baselines for reference. 5. Engage a Contractor or other professional to conduct security audit.
Data Loss - IT Systems	1. Browse through the list of directory level backups captured by Veeam for that host to select the backup to restore data from. 2. Initiate a restore of the file or directory from the affected system using Veeam. If the system in question is a virtual machine, restore the most recent full VM image as it is using Veeam. 3. Verify the file, folders and their permissions upon completion of the restore.

Hardware failure – IT Systems	1. Follow up with the vendor for getting the faulty hardware replaced. 2. Install and setup the new hardware as per the original baseline configuration. 3. Refer to File system table below to configure any File system dependencies such as NFS mount points. 4. Initiate a Restore operation from the most recent backup using Veeam. The restore procedure varies depending on if the system is physical or virtual. For more details, refer to the Veeam Backup guide. 5. Upon completion of restore, verify connectivity and operations.
Hardware failure –Network Devices	1. Order a replacement from a vendor. 2. Setup and configure the new device as per its original counterpart. For more details, refer to the asset inventory database and/or any supporting documentation to reference the original baseline config such as Firewall rules, ACLS, Vlan, etc. 3. Restore system configuration using Manufacturer instructions from the secure central repository. 4. Verify connectivity between devices. Run operations to confirm.

Hardware failure / Configuration Restore- OT Systems	1. Order a replacement from a vendor. 2. Setup the new device by assigning it the original static IP address and restore the configuration on it as per manufacturers manual. Following are high level instructions for config restore of the Allen Bradley PLC ➢ Pull out the microSD card from the PLC and load a previously saved image on it using a card reader. A working image can be pulled from the central secure location used to save backups. Alternatively, a new base image can also be obtained from the manufacturer. ➢ Insert the microSD card back into the PLC and power on the device. ➢ Test Connectivity and operations.

Filesystems as of Sep 2018

Host	Local Drives	Size	Network Drives
FGS-47631EHH	C:\	465GB (500GB HDD)	
FGS-61338PSH	C:\	233GB (250GB HDD)	
FGS-613380SH	C:\	465GB (500GB HDD)	H:\ HMI_Share (\\172.16.1.4)
FGS-61338CH	C:\	233GB (250GB HDD)	
FGS-61338HH	C:\	233GB (250GB HDD)	O:\ OPC_Share (\\172.16.2.5)
FGS-61338LHH	C:\	465GB (500GB HDD)	
WIN-FPVTDCDEUCR	C:\	50GB	W:\ Eng_Workstation (\\172.16.3.10)

3.6.11 Restoration Priorities

Should an incident occur and Westman need to exercise this plan, this section will be referred to reference restoration priorities in bringing systems online.

2273 **IT Systems**

Priority	IT System	Description
High	LAN-AD	Active Directory / DNS Server
High	Veeam	Veeam Backups Server
High	FGS-613380SH	OPC Server
High	FGS-61338CH	Controller Server
High	FGS-61338HH	HMI Server
High	FGS-61338LHH	Local Historian Host server
High	WIN-FPVTDCDEUCR	Local Historian Database Virtual Machine
Medium	FGS-61338PSH	Plant Simulator
Medium	FGS-47631EHH	Engineering Workstation
Medium	PI-DMZ	DMZ Historian Database Server
Medium	SymantecMgr	Symantec Antivirus
Low	Security Onion	Snort IDS
Low	Graylog	Syslog server
Low	GTB Inspector	DLP
Low	Hive	Incident Response Server

2274

2275

Networking Equipment

Priority	Device Info	Description
High	Boundary Router	Allen Bradley Router 8300
High	Supervisory LAN Switch	Allen Bradley Stratix 5700
High	Control LAN Switch	Allen Bradley Stratix 5700

OT Systems

Priority	OT System	Description
High	PLC	Allen Bradley Control Logix 5571
High	HMI Server	Factory Talk View Studio

3.6.12 Definitions and Acronyms

SLA	Service Level Agreement
Recovery Time Objective (RTO)	RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the Maximum Tolerable Downtime. [2]
Recovery Point Objective (RPO)	The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. [2]

3.6.13 References

1. SANS Guide for DR: https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564
2. NIST SP 800-34 Contingency planning guide for Federal Systems https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf

3. Allen Bradley ControlLogix 5571 Manual
https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um001_-en-p.pdf

4. Technical Solution Implementations

4.1 Introduction

This section includes proof-of-concept technical solution implementations developed for the fictional company Westman. An overview of these technical solutions is discussed in Section 6 of Volume 1 and potential technical solutions are discussed in Section 7 of Volume 1. Each organization's information security experts should identify the technical solutions that will best integrate with their existing cybersecurity program and manufacturing system infrastructure.

There are five main areas of performance indicators being collected in the Process Control System:

1. Manufacturing process performance: measures the performance of the manufacturing process, i.e. the chemical continuous process.
2. Network performance: measures the performance of the underlying TCP/IP network.
3. Computing resources performance: measures the performance of the computers, hardware, and software processes.
4. Industrial protocol performance: measures the performance of the industrial communication protocol, i.e. the DeviceNet in the PCS.
5. OPC Data Exchange performance: measures the performance of the data exchange mechanism of the system.

Measurements in different areas provide insight of the entire system performance from different perspectives. The manufacturing process performance provides indicators on how well the high-level manufacturing process and overall system perform. However, this may not be able to provide enough detail on the performance of the sub-systems, therefore measurements are also performed at sub-system levels. For example, a typical chemical continuous manufacturing is a relatively slow process in comparison with computer networking. Therefore, a moderate TCP/IP network delay may not reflect in the measurement of the high-level manufacturing process performance. However, such TCP/IP delay may have significant impact on the sub-systems. The effects will not be reflected in the high-level measurement until significant delays are accumulated in sub-systems. Measurements in multiple levels provide details and in-depth understanding to key performance areas of the entire system. It helps to understand how the aggregate effects will impact the performance. Aggregate effects will be important to the high-level manufacturing performance.

Each of the technical solution implementation is organized as an experiment. For the measurement purpose, each experiment has a fixed runtime of 4 hours (14,400 seconds). Performance metrics and network packet capture are collected during the entire experiment run.

After the experiment is completed, all the collected metrics and network packet capture will go through the post processing stage to filter, sort and rearrange data in proper order. The last step is to compute the key performance indicators from the sorted dataset using a set of Python scripts developed by NIST.

More technical detail of the Process Control System and the measurement process is described in NISTIR 8188: Key Performance Indicators for Process Control System Cybersecurity Performance Analysis.

4.1.1 Implementation Note – Due Diligence Implementing Technical Solutions

It is important to note that the procedures used during this implementation (i.e., install a tool, then measure the impact) should not be used in a production system. Care must be taken before using any technical solutions, especially those that actively scan the manufacturing system network and its devices; manufacturers should first conduct an assessment of how these tools work and what impact they might have on the connected control equipment [3]. Technology evaluations may include testing in similar, non-production control system environments to ensure that the tools do not adversely impact the production systems. Impact could be due to the nature of the information or the volume of network traffic. While this impact may be acceptable in IT systems, it may not be acceptable in a manufacturing system. In general, any operation that actively scans the manufacturing network should be scheduled to occur only during planned downtimes. [3]

4.2 Open-AudIT

4.2.1 Technical Solution Overview

Open-AudIT is an asset inventory tool providing scanning of hardware and software within the manufacturing environment. Open-AudIT scans are highly customizable to each environment, depending on the level required. The cost depends on the level of functionality desired for your environment. Editions offered by Open-AudIT vary from entry level community edition which is free, all the way up to enterprise edition. Enterprise was chosen since it contains the ability to setup schedule scanning, dashboards, and baselining of equipment.

Open-AudIT is a downloadable OVA which is easy to install. OVA install allows installation in a Hyper-Visor environment allowing for installation within an existing virtual environment without requiring purchasing additional hardware. Configure for initial discovery scans are straight forward and easy to configure and perform.

4.2.2 Technical Capabilities Provided by Solution

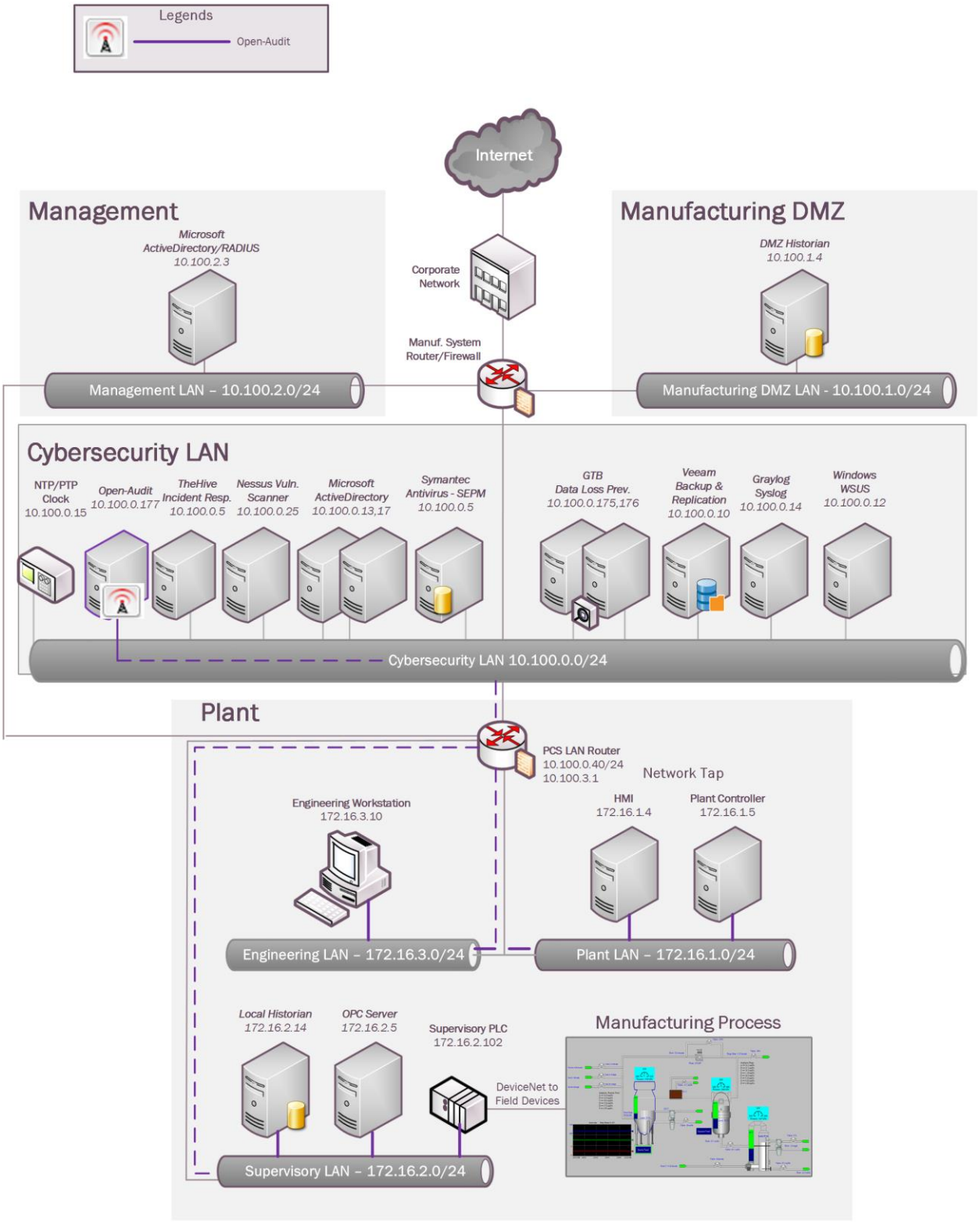
Open-AudIT provides components of the following Technical Capabilities:

- Hardware Inventory
- Software Inventory
- System Development Lifecycle Management
- Configuration Management
- Baseline Establishment (Enterprise Edition)
- Change Control

4.2.3 Subcategories Addressed by Implementing Solution

ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, PR.DS-3, PR.IP-1, PR.IP-2, PR.IP-3, PR.IP-4, PR.IP-6, PR.MA-1, DE.AE-1, DE.CM-7

4.2.4 Architecture Map of Where Solution was Implemented



4.2.5 Installation Instructions and Configurations

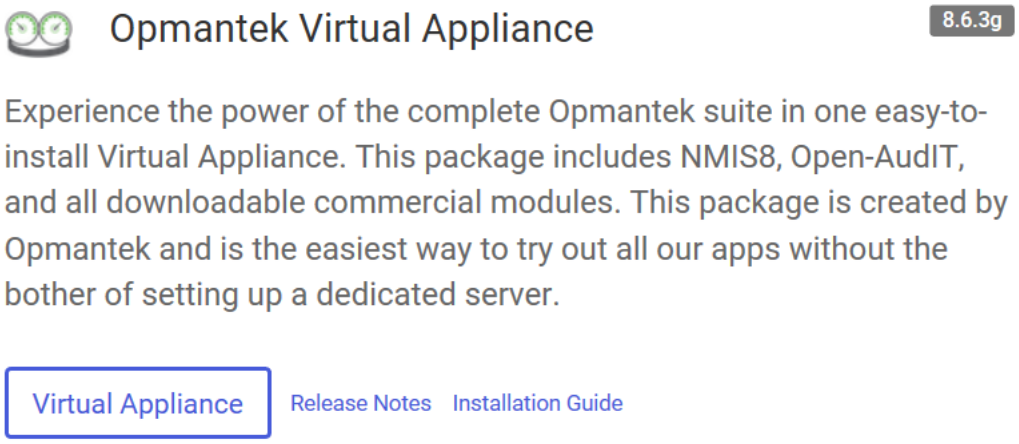
Prerequisites:

- Identify if physical hardware or virtual machine will be used
- Requirements from Opmantek who developed **"Open-AudIT"** indicate the specification required are low. Please see this link for exact details provided by the vendor link.

Instructions:

Download:

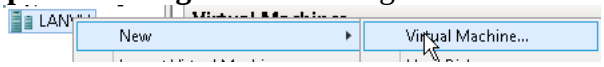
1. Download and save **Opmantek Virtual Appliance** from Opmantek website.[11]



- Once download has completed ".**ova**" file will need to be extracted to view the contents and move to the next step (any tool supporting extracting .ova and .gz can be used).
- Open the folder where the files were extracted too. There should be a total of four files.
- Next, extract the two files with extension (.vmdk.gz) since this file is still compressed. Once completed two files with the same extension (**.vmdk**) should now exist.
- Now two files just extracted need to be convert to "**VHDX**" format, so we can run these disk in a Hyper-V environment. See this link for instruction and additional information useful for converting virtual drive format.
- Once both drives have been converted to "VHDX" format proceed to next section.

Virtual Machine Setup:

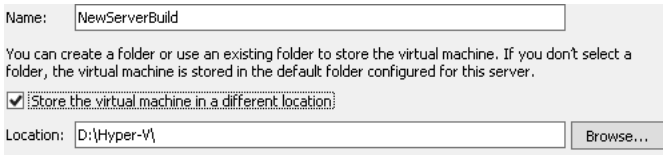
1. On the virtual server host open "**Hyper-V Manager**" and then right click on server name selecting **New Virtual Machine**



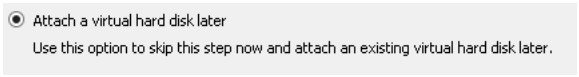
2. Now type in the name you going to give this server.

[11] Opmantek Intelligent Network Management Software https://opmantek.com/

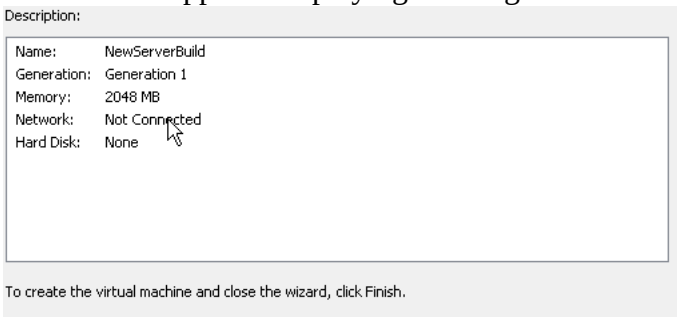
3. Place a check in the box "**Store the virtual machine in a different location**" click N**ext**.



4. The step above will place the configuration and hard drive files for the newly create Virtual Machine in D:\Hyper-V\NewServerBuild (See Screenshot**)**
5. Leave **Generation 1** selected and click Next. This machine doesn't require additional features provided from **Generation 2**.
6. Now assign how much memory your new machine will be given for use. For our environment we are using **"2048"** Click next to continue.
7. Select the network this virtual machine will be using and click **Next**.
8. Now select **"Attach a virtual disk later"** and click **Next**.

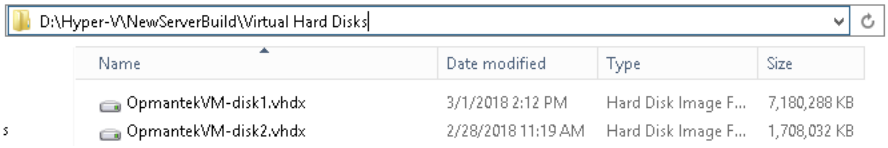


9. Now a screen appears displaying a configuration summary, click **Finish** to complete.

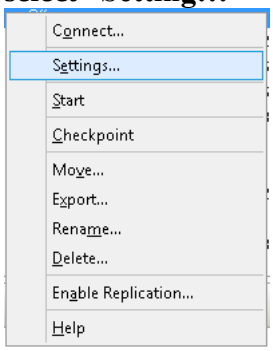


10. Next, open Windows Explorer and navigate to the location of your newly created virtual machine and create a new folder labeled **"Virtual Hard Disk"**

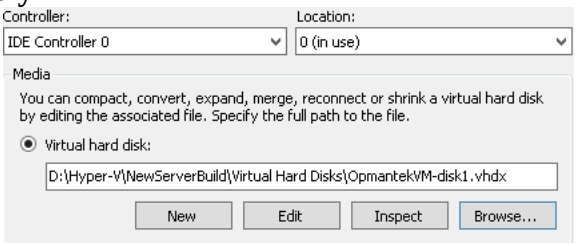
11. Now moves the hard drive files converted earlier to this new folder location just created.



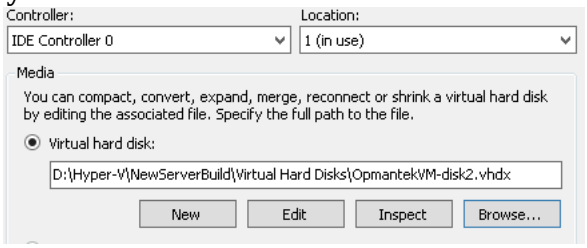
12. Open Hyper-V Manager and right click on Virtual Machine just created and select **"Setting…"**



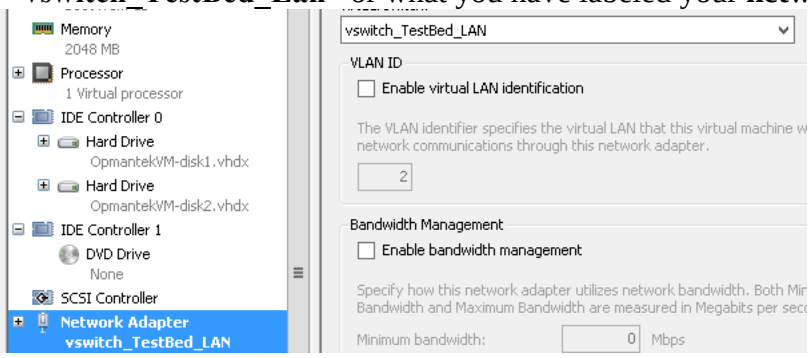
13. Memory should be configured for **"2048"**
14. Virtual Processor **"2"**
15. Click on **"IDE Controller 0"** then click on "**Add"** button to attach a virtual hard.
16. Click browse button and select the first virtual drive that was moved earlier, click **Apply**.



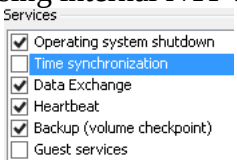
17. Now click on **"IDE Controller 0"** again and click "**Add"** button to attach a virtual hard.
18. Click browse button and select the second virtual drive that was moved earlier, click **Apply**.



19. Now, select Network adapter and click the drop down and select **"vswitch_TestBed_Lan"** or what you have labeled your **network**.



20. Click on Name and make sure to add some descriptive information that will allow other to easily see this information without having to login into machine.
21. Select Integration Service and remove check from **"Time Synchronization"** Time will sync using internal NTP server via DNS pointer. Click **"Apply"** and then **"OK"**.



Configure Virtual Machine Networking:

1. Open Hyper-V Manager and then right click on newly created machine and select start.
2. Double click on machine being configured to open a Console window.

3. Now type in **"root"** and then hit enter. Now type in Password which is →**"NM1$88"** without the quotes. Additional information for default login credentials can be found here.
4. Now type this command without the quotes to copy a static configuration for networking. **cp ifcfg-eth0.static /etc./sysconfig/network-scripts/ifcfg-eth0** if prompted to overwrite file type **"Yes"**
5. Now type this command without the quotes **"sudo nano /etc./sysconfig/network-scripts/ifcfg-eth0"**
6. Now use the arrow keys to change the highlighted fields to your desired network configuration.

```
DEVICE="eth0"
NM_CONTROLLED="yes"
ONBOOT=yes
TYPE=Ethernet
BOOTPROTO=static
IPADDR=192.168.1.7
NETMASK=255.255.255.0
BROADCAST=192.168.1.255
GATEWAY=192.168.1.1
IPV4_FAILURE_FATAL=yes
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=yes
NAME=eth0
```

7. Once all fields have been updated use **Ctrl + O "^O"** to write the file and then **Ctrl + X "^X"** to exit.

```
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

8. Now type **"service network restart"** These restarts networking services with the newly configured settings.

Complete Additional Setup via Web Browser:

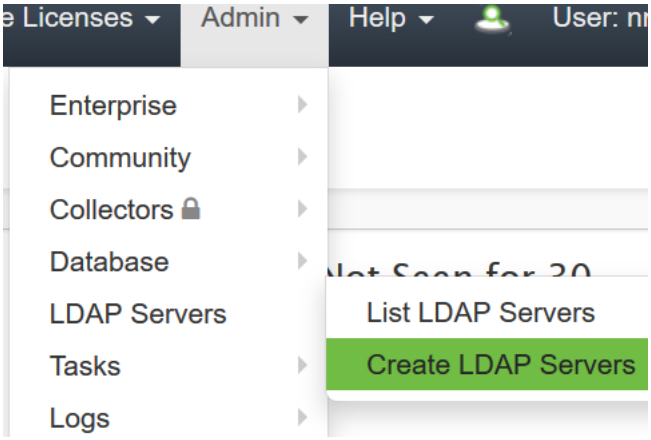
1. Now with any web browser navigate to **"IP Configured Earlier"** example would be **"10.100.0.177"**
2. If prompted to proceed to untrusted site, select **"Yes"**. This error is produce since SSL has not been configured and Open-AudIT redirects HTTP sessions over to HTTPS.
3. Once this page opens you'll see lots of different options this tool provides. We're using "**Open-AudIT Enterprise"** This version allows for up to 20 nodes to be audited / monitored for free.

Opmantek Documentation and Community

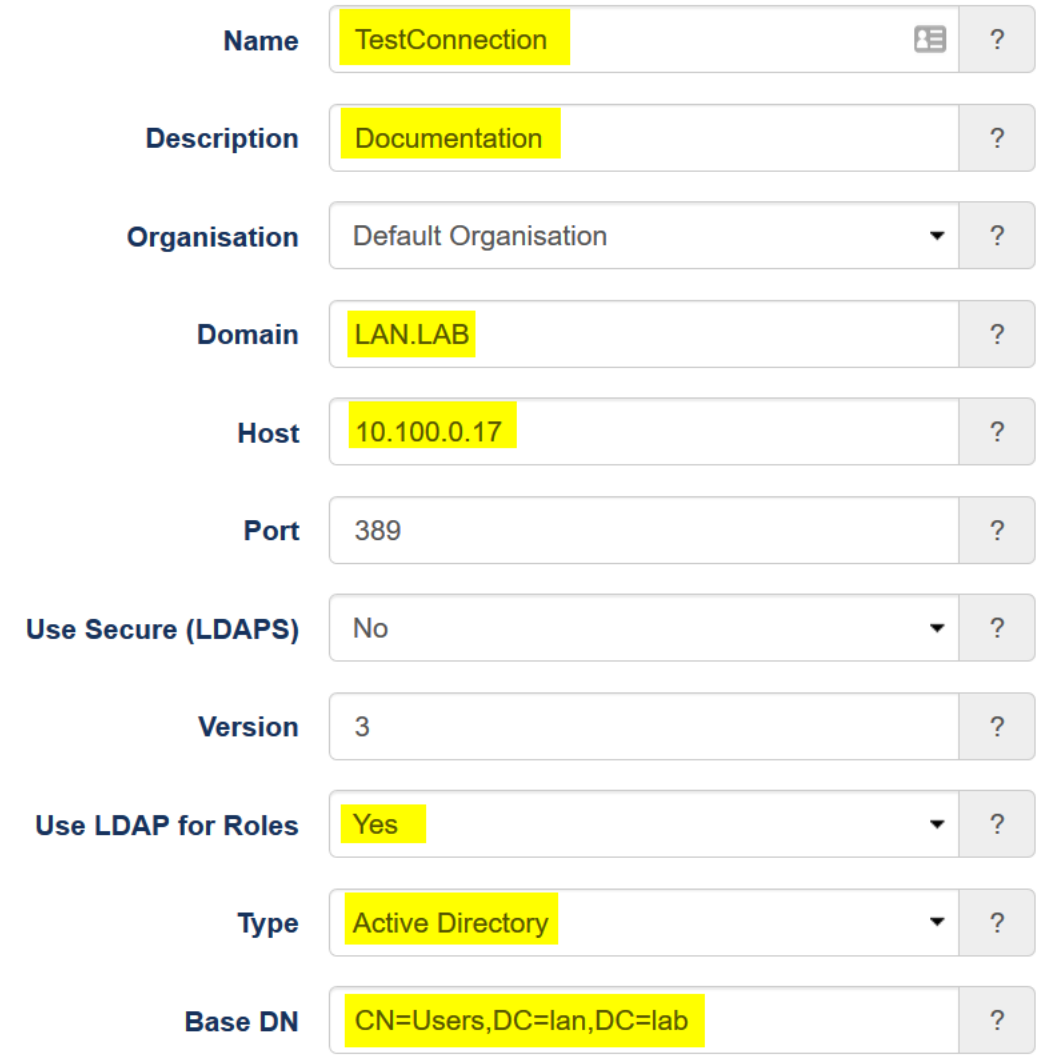
NMIS8 Dashboard
opCharts - interactive Charts and Dashboards
opEvents - Event Management
opFlow - NetFlow Analysis
opConfig - Configuration and Compliance Management
opReports 3.0 - Network Reporting
Open-AudIT Enterprise

Open-AudIT V2 Dashboard
Open-AudIT Documentation and Community

4. You'll now be prompted for login with username and password. This default information is provided above **"username / password"**.
5. Once logged in we need to make some required changes to allow this produce to function in our environment.
6. Click on **"Admin → LDAP Server → Create LDAP Servers"** This will allow integration with Active Directory using LDAP authentication for logging into this application.



7. Required setting for LDAP server connection. Screen shot provide for reference.



   a. Name – **TestConnection**
   b. Description -- **Documentation**
   c. Domain – **LAN.LAB**
   d. Host – **10.100.0.17**
   e. Use LDAP Roles -- **Yes** (Additional configuration is required in AD Groups. See section below in this document for additional steps.
   f. Base DN – **"cn=user,dc=lan,DC=lab"**

8. Click **"Submit"** once all information has been entered.

Active Directory Groups for LDAP Integration:

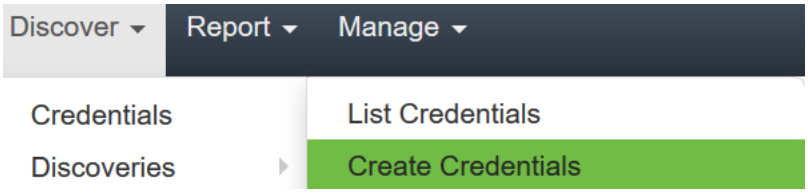
1. Groups listed below are required for integration to work with Open-AudIT and Active Directory.
   a. **Admin "open-audit_roles_admin"**
   b. **org_admin "open-audit_roles_org_admin"**
   c. **reporter "open-audit_roles_reporter"**

d. **user "open-audit_roles_user"**
e. **Default Organization "open-audit_orgs_default_organisation"**

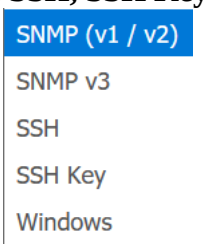
2. Create each group listed within quotes in your Active Directory. Each group should be created with Group Scope (**Global**) Group Type (**Security**)
3. Once each group has been created and the appropriate users add you can now login with your Active Directory credentials.

Discover Credentials and Discover Scans

1. From the home screen click on **Discover >> Discoveries >> Create Credentials.**



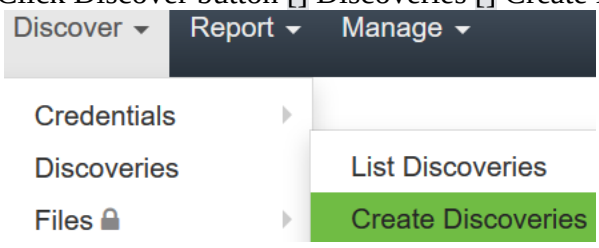
2. Now enter in the requested information.
   a. Name – Name of the Credentials being used. Example (**SSH**)
   b. Organization – Default Organization is selected. Pickup another if your configuring more the one organization.
   c. Description – Description of item being added.
   d. Type – Select which type of credentials will be used**. (SNMP (v1 / v2), SNMP v3, SSH, SSH Key, or Windows)**



   e. Credentials – enter the appropriate credentials for the select type from above.
   f. Click submit to save this entry.

Discovered Scan:

1. Click Discover button [] Discoveries [] Create Discoveries.



2. Name – The name for this scan which should be unique.
3. Subnet – The network discovery will be performed on.
4. Click submit to save and return to main discovery screen.
5. Main discovery screen allows you to start a scan at any time. Scans can also be configured to run on a schedule interval.

Useful information and links:

1. Default password were not changed, so remember to change all default password before this is put into production. **(THIS IS VERY IMPORTANT)**
2. Software Vendor webpage. → https://opmantek.com
3. Community forums. → https://community.opmantek.com
4. Software is Open Source. Your able to use Professional Edition for up to 20 machines after that there is a cost which is relatively inexpensive.
5. Comparison Chart

Both the community and enterprise products share a common code base, however, Open-AudIT Enterprise includes additional modules that improve discovery, simplify administration and increase reporting ability. Use the comparison chart below to decide which version best suits your organization's requirements.

	Community	Professional	Enterprise
Network Discovery	Yes	Yes	Yes
Device and Software Auditing (including Device Port and Storage Appliances)	Yes	Yes	Yes
Configuration Changes Detection and Reporting	Yes	Yes	Yes
Hardware Warranty Status	Yes	Yes	Yes
Inventory Management	Yes	Yes	Yes
Custom Fields	Yes	Yes	Yes
Interactive Dashboard		Yes	Yes
Geographical Maps		Yes	Yes
Devices Export		Yes	Yes
Scheduling – discovery and reporting		Yes	Yes
Enhanced Reports including Tine based, Historical and Multi Reporting		Yes	Yes
High Scale			Yes
High Availability			Yes
File Auditing			Yes
Baselines			Yes
Configurable Role Based Access Control including Active Directory and LDAP			Yes
Integration with agents and CMDB			Yes
Commercial Support		Yes	Yes

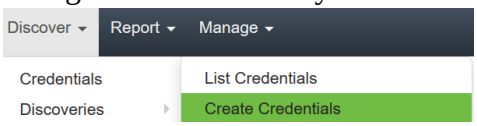
6. Ability to perform baseline scan on devices is provided by Enterprise edition. This could be very useful for determining changes over a period of time.

Install Steps for Process Control

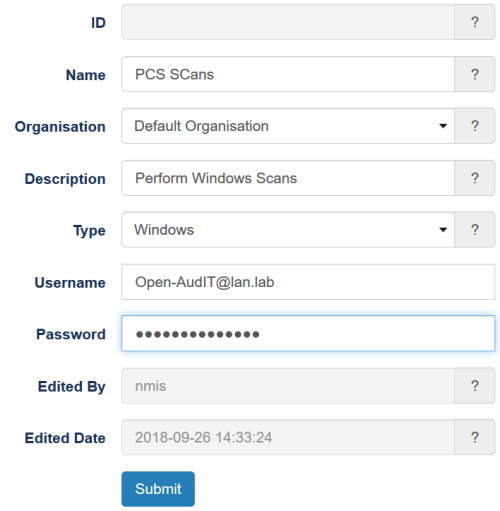
Open-Audit Configuration steps within Process Control System once system has been installed

Initial Configuration:

- Login via web portal
- Navigate to → Discovery → Credentials → Create Credentials

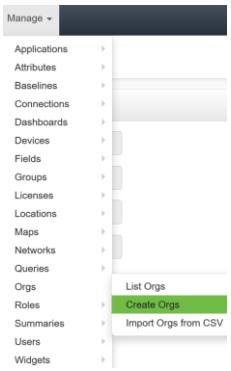


- Credentials can be assigned to any organization that has already been created. If you want credentials to only apply to specific organizational group, then select that from the appropriate drop down during credential creation and select the desired group these credentials will apply to.
- Our environment consists of mainly Windows machine, so Windows will be used for connection type.
- Now create a credential and select **Windows** for the type. Once completed click **Submit**.



Organization Groups Creation:

- Click on Manage → Orgs → Create Orgs

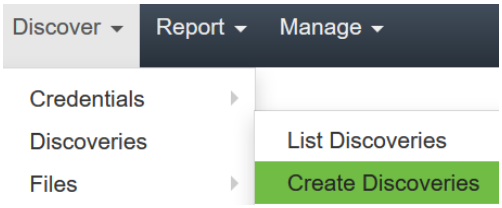


- Now enter **Name**: **Description**: and click submit at the bottom of the page to save.

- If you have multiple machines / equipment in different locations you can make Organizational groups based based on business units, or related task.

Configure Discovery Scan:

- Now click on Discover → Discoveries → Create Discoveries



- Enter a meaningful name for discover being created

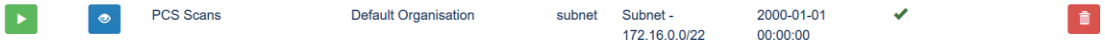
- Next, enter the subnet that'll be used for performing this scan. This scan is using 172.16.0.0/22

Search online for additional subnetting information / calculators if you'd like to learn more.
- **Network address:** should already be defaulted to Open-AudIT installed location, if this is not true, click the drop-down arrow and select your installed location.
- Now, click on the advanced button to see more options. 

- Once **Advanced** has been expaned you'll have additional options to select if desired. These options are **Org, Type, Devices Assigned to Org,** and **Devices Assigned to Location**. These options aren't required, but allow you to place found devices into different Organzations groups.
- Once all selection have been made click on **Submit** button to continue.

Discoveries:

- Once the steps above have been completed clicking on **Submit** button you'll be taken to a new webpage that'll allow you to run discovery process created in the previous step.
- To start discovering devices click on **green** arrow button. If you need to verify details for this scan click on the button that looks like an **eye**: finally, if you need to delete this scan click on the **trash** can icon to the right. See screen shot for details.



- Once discovery has started you'll be taken to a new page allowing you to view status, or cancel if needed.
- Newly found devices are added to **My Devices** which is found on the home screen.

Lesson Learned:

Ensure default password are changed

Use Secure LDAP (LDAPS) If unable to use LDAPS make sure account being used for syncing groups has least privilege rights. (Not an Administrator and not a Domain Administrator)

When configuring SNMP make sure to use SNMP V3 if possible

4.2.6 Highlighted Performance Impacts

The following performance measurement experiment was performed for the Open-AudIT tool while the manufacturing system was operational:

Experiment PL003.1- Open-AudIT asset inventory tool network scan and authenticated scan

A small performance impact to the network behavior was observed in the PCS system during the Open-AudIT scan. The network traffic was slightly increased in part of the PCS system during the scan. For example, the path delay from PLC to OPC was slightly higher especially in the latter part of the experience when Open-AudIT was performing the authenticated scan. However, the round trip time from the Controller to the OPC was mostly the same throughout the scan. It appears that some part of the system has a more noticeable impact than the other parts.

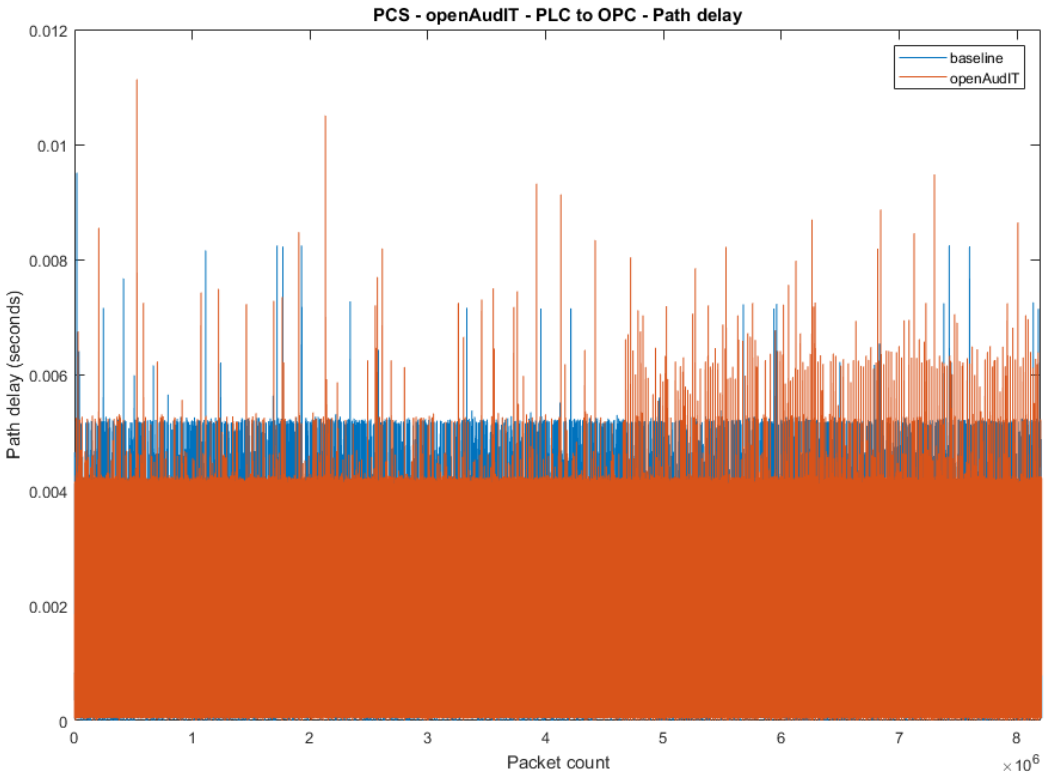


Figure 4-1 Plot showing the path delay from the PLC to OPC server

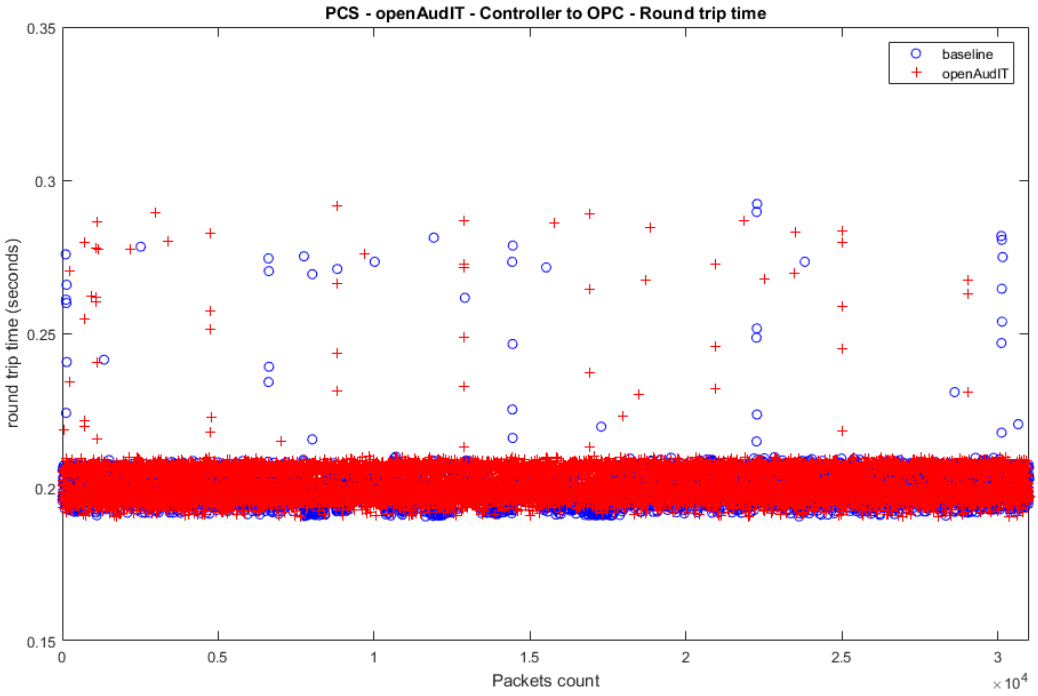


Figure 4-2 Plot of the packet round trip time from Controller to OPC

A small impact to the manufacturing process was observed. The product flow of the manufacturing process was slightly higher than the optimal level. The reactor pressure was slightly higher than the optimal level specially at the latter part of the experiment when Open-AudIT was performing the authenticated scan. However, the impact was small within the tolerance of the system.

It is hypothesized that the impacts were caused by increased network delays between the hosts of the system. There is a time delay before the network impact will start impacting the manufacturing process due to the iterative nature of the process simulation and sensor and actuator values exchange.

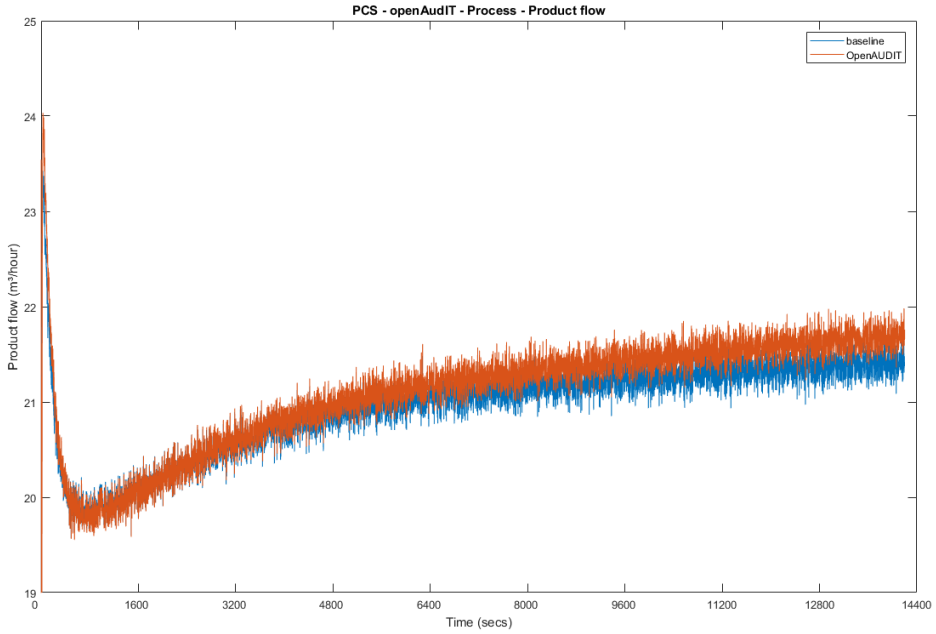


Figure 4-3 Plot of the production flow of the manufacturing process

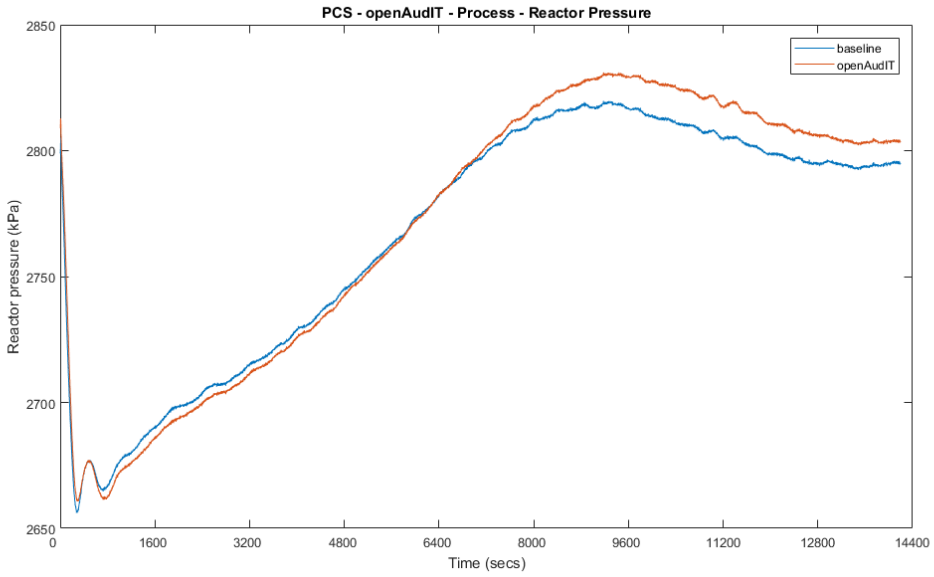


Figure 4-4 Plot of the reactor pressure of the manufacturing process

4.2.7 Link to Entire Performance Measurement Data Set

Open-AudIT KPI data

Open-AudIT measurement data

4.3 CSET

4.3.1 Technical Solution Overview

Cyber Security Evaluation Tool (CSET) is a tool provide by Department of Homeland Security for performing Cybersecurity evaluation against an organization. This evaluation is completely manual process of answering multiple questions to determine organizational security posture in regard to implemented current cybersecurity practices against current security status. This evaluation will help identify area within the organization that required more attention and resources.

4.3.2 Technical Capabilities Provided by Solution

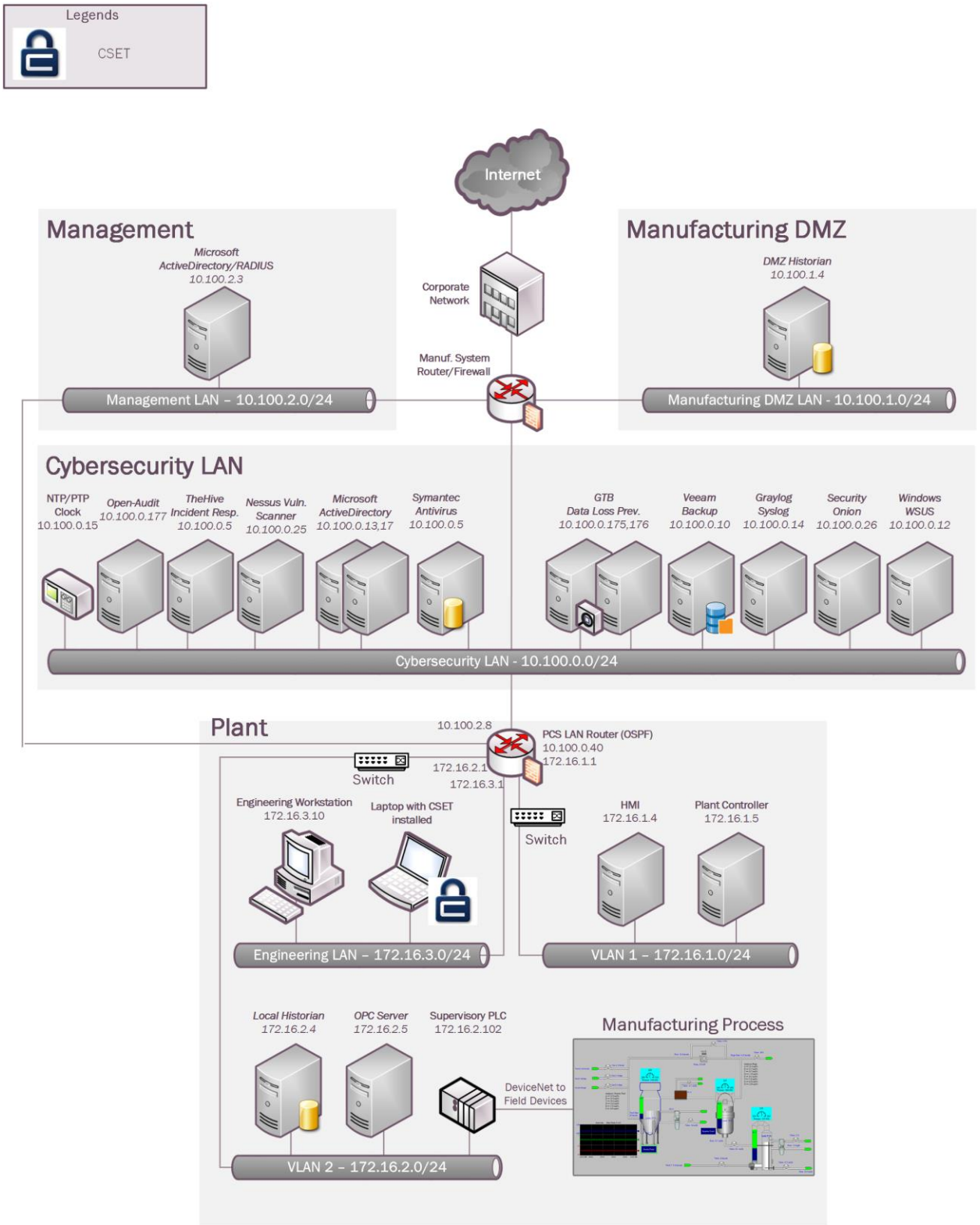
CSET provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Network Architecture Documentation
- Risk Assessment

4.3.3 Subcategories Addressed by Implementing Solution

ID.RA-1

4.3.4 Architecture Map of Where Solution was Implemented



4.3.5 Installation Instructions and Configurations

CSET Installation and Configuration

Download and Installation Instructions: Provided by DHS

Download CSET using the link at the bottom of this page or by clicking here. After clicking the link, you will be asked to identify yourself and will then be given the opportunity to download the file *CSET_x.x.iso (where x.x represents the download version)*.

The CSET download is in a file format known as "ISO." This file is an "image" of the equivalent installation files included on the CSET CD. Because of this format, it is necessary to process the download using one of the following methods:

1. **Decompressing the File** - Open the file using any one of the newer compression utility software programs.
2. **Mounting the File** - this method loads the ISO file using utility software to make the file appear like a virtual drive with the original CD loaded.
3. **Burning the file to CD** - this method uses CD-burn software and the ISO file to burn the files onto your own CD to create a physical disk identical to the CSET original.

These methods require separate software utilities. There are a variety of both free and purchased utility programs available through the Internet that will work with the ISO file format. As DHS does not recommend any specific application or vendor, it will be necessary for you to find a product that provides the necessary functionality. Step by step instructions for each method are provided below:

Decompressing the File

1. CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
2. SAVE the file to your hard drive of choice (i.e., your computer hard drive or USB drive) maintaining the file name and extension (.iso).
3. OPEN the ISO file with a compression utility program and SAVE the files to your hard drive of choice maintaining the original names and file extensions.
4. COMPLETE the *Installing the CSET Program* instructions below.

Mounting the File

1. CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
2. SAVE the file to your hard drive of choice (i.e., your computer hard drive or USB drive) maintaining the file name and extension (.iso).
3. RUN your ISO-specific utility program that is capable of mounting the file. COMPLETE the instructions within the utility software to create a virtual drive using the ISO file. If

you do not have an ISO utility application, you will need to find and install one before continuing with these instructions.

4. COMPLETE the *Installing the CSET Program* instructions below.

Burning the file to CD

1. CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
2. SAVE the file to the hard drive on your computer maintaining the filename and extension (.iso).
3. INSERT a blank, writable CD into the computer's CD drive.
4. RUN your CD-burn utility program. COMPLETE the instructions on your utility program to burn the ISO image to your DVD. (If you do not have an application that can do this, then you will need to find and install one before continuing with these instructions.)
5. COMPLETE the *Installing CSET Program* instructions below.

Installing the CSET Program

1. FIND the CSET_Setup.exe file in the folder, virtual drive, or CD containing the CSET files.
2. DOUBLE-CLICK the CSET_Setup.exe file to execute. This will initiate the installer program.
3. COMPLETE the instructions in the installation wizard to install the CSET program.
4. READ the material within the ReadMe document for a summary explanation of how to use the tool. Help is also available through the User Guide, screen guidance text, and video tutorials.

Video Tutorials

A number of video tutorials are available to help you better understand how to use this tool. They are designed to play within YouTube, therefore, you must have an active internet connection to view them. You can access these videos by navigating to the CSET YouTube channel (https://www.youtube.com/c/CSETCyberSecurityEvaluationTool).

To view close captioning in YouTube, click on the "cc" icon on the video window.

System Requirements

In order to execute CSET, the following minimum system hardware and software is required:

- Pentium dual core 2.2 GHz processor (Intel x86 compatible)
- CD-ROM drive if creating a physical CD
- 5 GB free disk space
- 3 GB of RAM

- Microsoft Windows 7* or higher
- A Microsoft Office compatible (.docx) document reader is required to view reports in .docx format
- A Portable Document Format (PDF) reader such as Adobe Reader is required to view supporting documentation. The latest free version of Adobe Reader may be downloaded from http://get.adobe.com/reader/
- Microsoft .NET Framework 4.6 Runtime (included in CSET installation)
- SQL Server 2012 Express LocalDB (included in CSET installation)

NOTE: For all platforms, we recommend that you upgrade to the latest Windows Service Pack and install critical updates available from the Windows Update website to ensure the best compatibility and security.

CSET Hash Values

SHA-256:
B7061B169E3461A298E58B99FADC9978D9F6CE22A0747669A538BDAF39C214ED

MD5: 53f2f71eb6e3bb54471e75318eaa64ee

SHA-1: f2b020e3a73db9b72ff85bd9b5e158449f6c003a

To download CSET, select the following link:

Download CSET

If you are unable to download or install CSET from the link, you may request a copy be shipped. To request a copy, please send an email to: cset@hq.dhs.gov. Please insert "CSET" in the subject line and include the following in your email request:

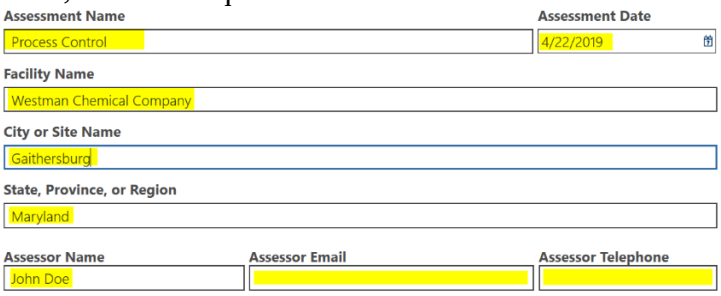
- Your name
- Organization name
- Complete street address (no P.O. boxes)
- Telephone number
- The error or installation issue you encountered when attempting the download

Running CSET for First time:

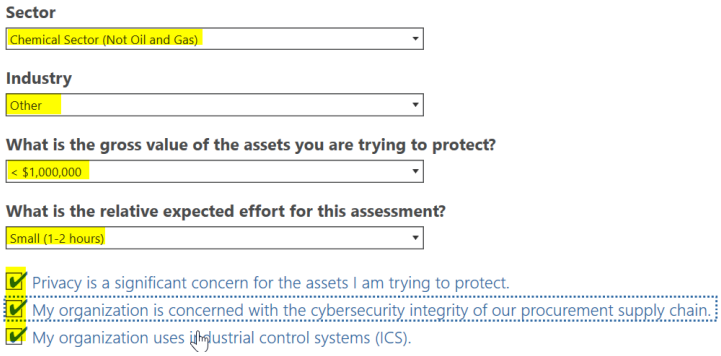
1. Once install of CSET has been completed find the application just installed and double click to run. 
2. Once program has launched you will see the home screen.
3. Click on File and select **"New Assetment"** 

4. Now, click on Start Here button in the lower right corner of program. 

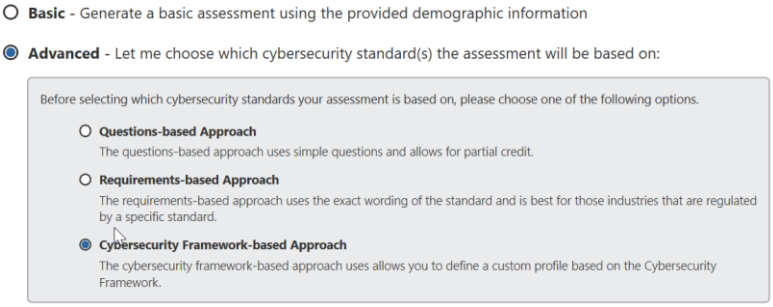
5. Next, enter all required information.



6. Click continue to proceed.
7. Now click on drop down menu and select the appropriate choices. Change any highlight options required.



8. Click continue to proceed.
9. If you want to create a network diagram click the button, otherwise click **"Continue"**.
10. Change Mode Selection to **"Advanced"** and **"Cybersecurity Frame-based Approach"**



11. Click continue.
12. Click continue to use default profile or create a new profile.
13. Click continue again.
14. Now answer the questions as they appear.
15. Complete all questions and generate a final report.

Lessons Learned:

- The tool is only as good as information entered. Make sure each answer is thought out before answering.

- Mark any answer for review as needed so there will be follow up.
- When completed your organization will receive a 0 to 100 score depending on readiness.

4.3.6 Highlighted Performance Impacts

No performance measurement experiments were performed for CSET due to its typical installation location (i.e., external to the manufacturing system).

4.3.7 Link to Entire Performance Measurement Data Set

N/A

4.4 GRASSMARLIN

4.4.1 Technical Solution Overview

GRASSMARLIN is an open source, passive network mapper dedicated to industrial networks and developed by the National Security Agency (NSA). GRASSMARLIN gives a snapshot of the industrial system including:

- Devices on the network
- Communications between these devices
- Metadata extracted from these communications

Points to consider:[12]

- Passive IP network mapping tool
- Hardware agnostic portable Java based tool
- Can only see and map hosts where you are capturing data from.

4.4.2 Technical Capabilities Provided by Solution

GRASSMARLIN provides components of the following Technical Capabilities described in Section 6 of Volume 1:

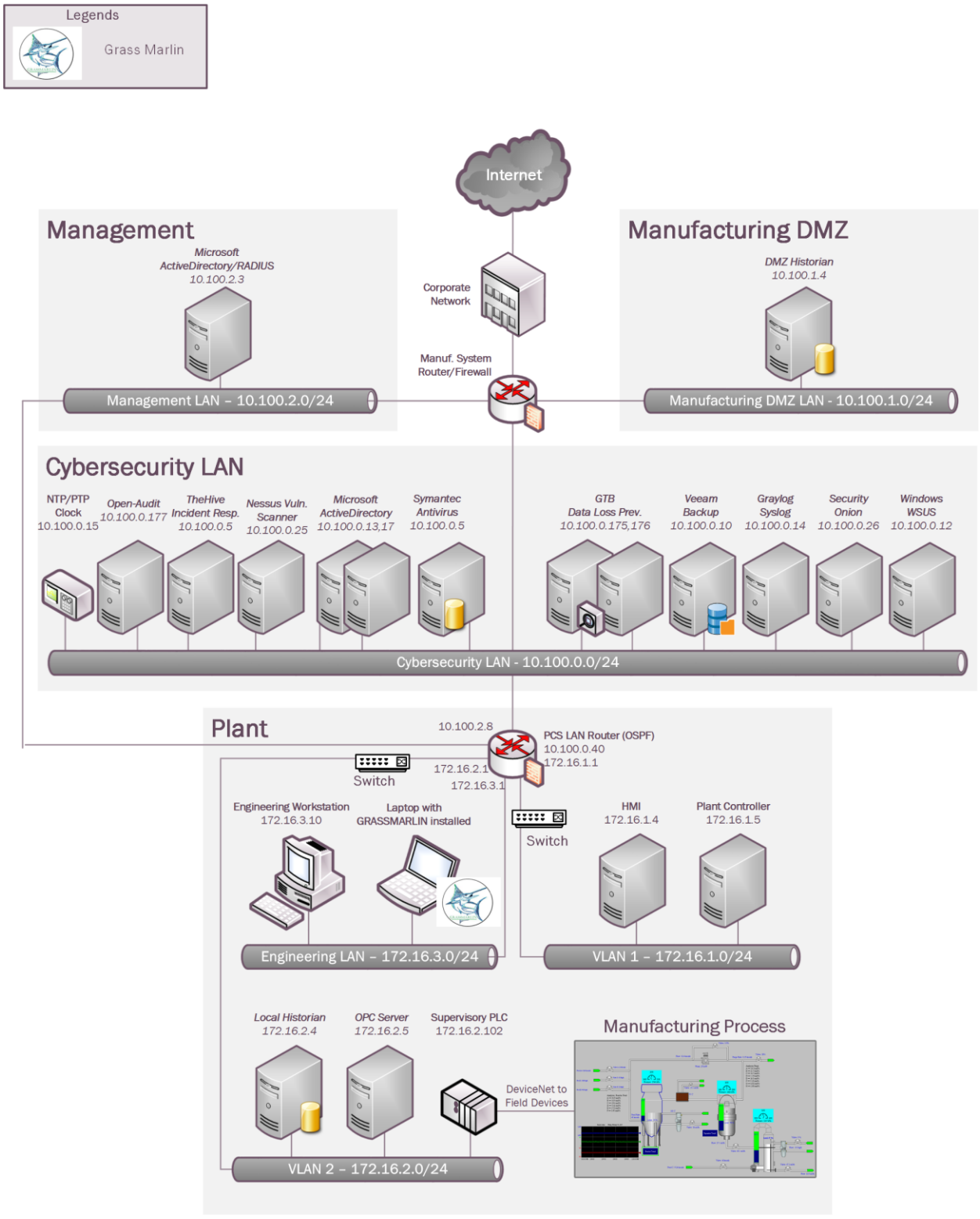
- Network Architecture Documentation
- Baseline Establishment
- Map Data Flows

4.4.3 Subcategories Addressed by Implementing Solution

ID.AM-3, ID.AM-4, PR.AC-5, PR.IP-1, PR.IP-3, PR.MA-1, DE.AE-1, DE.CM-7

[12] GRASSMARLIN Briefing Powerpoint 2017: https://github.com/nsacyber/GRASSMARLIN /blob/master/GRASSMARLIN_Briefing_20170210.pptx

4.4.4 Architecture Map of Where Solution was Implemented



4.4.5 Installation Instructions and Configurations

Details of the solution implemented:

Name	Version
GRASSMARLIN	3.2.1

Setup

- GRASSMARLIN is supported on the following platforms[13]
  Microsoft Windows (64bit, 7 8 and 10)
  Fedora Linux
  Ubuntu (14.04 ,15.10)
  Kali Linux 2.0
  CentOS (6,7)
  Debian (8)

  Download GRASSMARLIN from https://github.com/nsacyber/GRASSMARLIN/releases as per the OS version of your system. Upon download, run the installer. The installer will install additional programs such as Java and Wireshark during the setup.
- GRASSMARLIN can operate in a real time passive mode by sniffing the live traffic or by importing a recorded pcap file. Data in GRASSMARLIN is stored in a Session. The Session contains imported files and visual state information.
- A temporary Windows 10 laptop would be setup in the Process Control System as and when required with GRASSMARLIN installed.

Using the Software:

- A captured pcap file from the system was imported in GRASSMARLIN to generate a network baseline. The pcap was captured by the running the tcpdump command on a Linux system which had a network connection from a Network aggregator device. This Aggregator was configured with mirror port connections in coming from the different network segments such as Supervisory LAN and Control LAN.

  `tcpdump -i <mirror-port interface> -w mypcap.pcap`

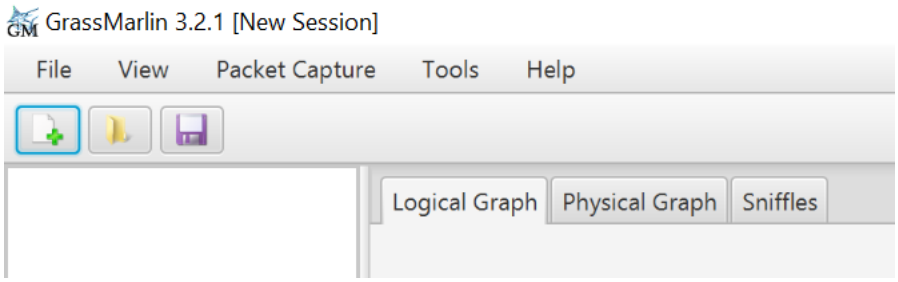
  For example: tcpdump -i eth1 -w /home/icssec/pcs.pcap
  Where eth1 is our mirror port connection

- To run GRASSMARLIN on a Windows or a Linux system with a Desktop, simply double click on the "GRASSMARLIN" shortcut or icon from the Programs Menu. To run it on a

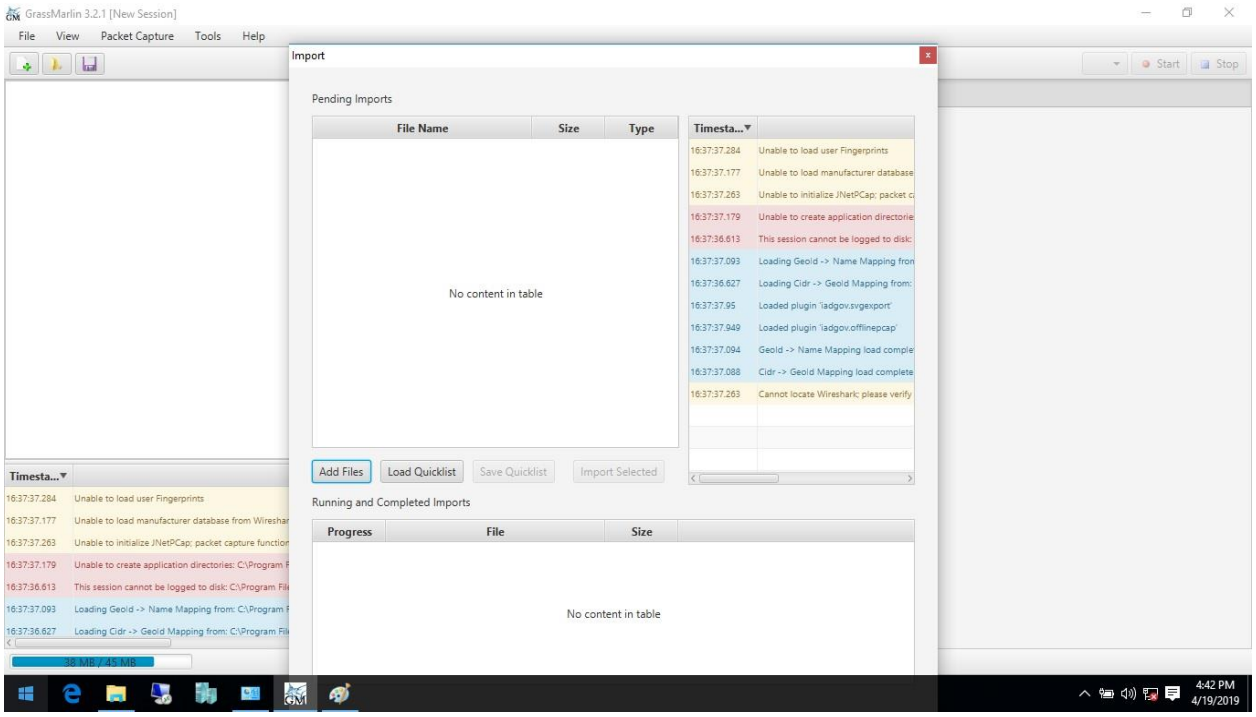
[13] GRASSMARLIN User Guide: https://github.com/nsacyber/GRASSMARLIN

Linux system without a Desktop, type the command "**GRASSMARLIN**" or "**sudo GRASSMARLIN**" and the interface should load up.

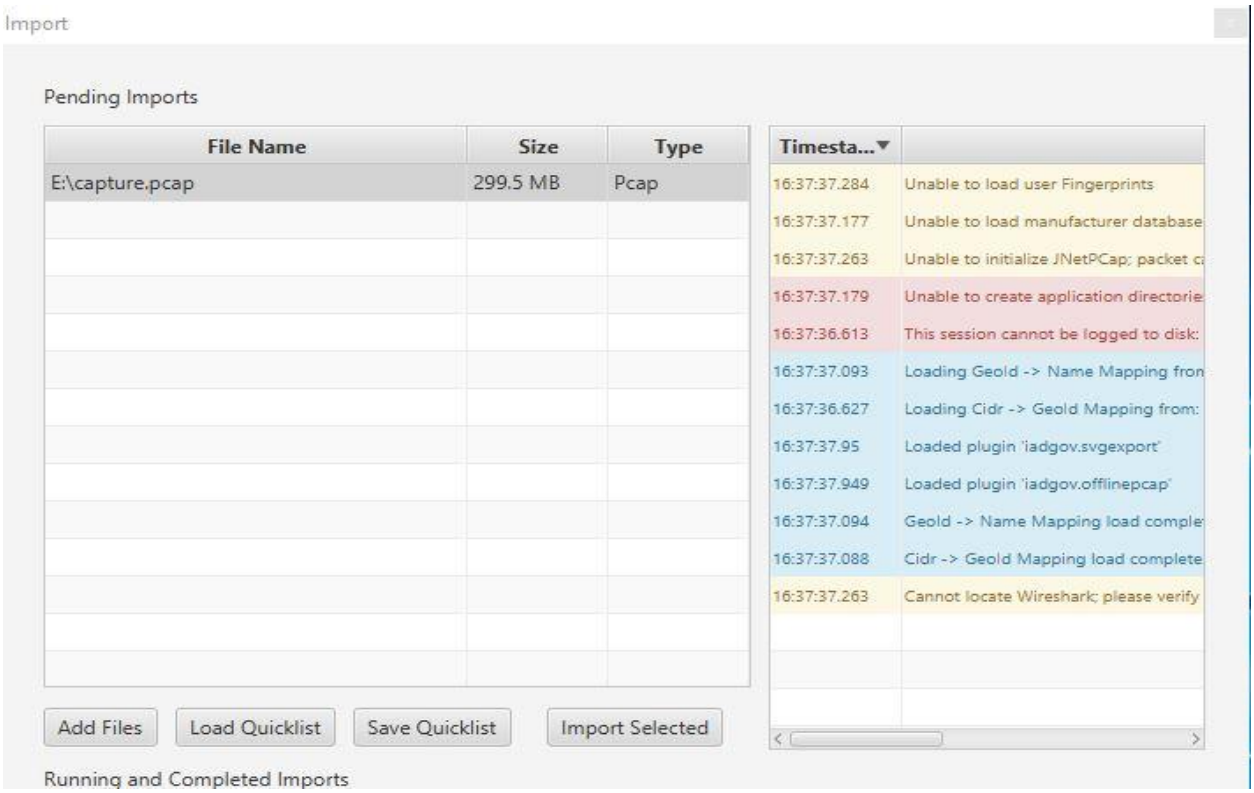
- To Import a pcap in GRASSMARLIN, click on the **Import** icon in the toolbar (or select **Import files** from the File Menu)



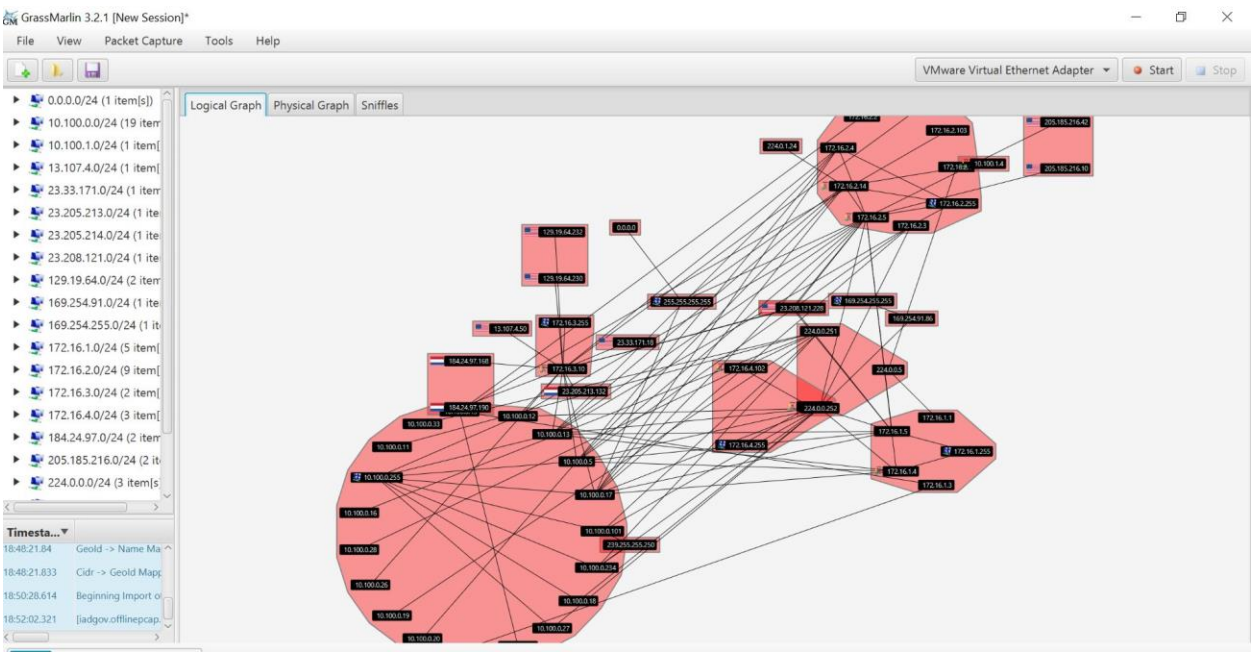
- Click on **Add Files.** Browse to the PCAP



- The Pcap will now show up under Pending Imports**.** Select the file and click on **"Import Selected".** Hit the **Close** button upon completion to back to the Main interface. The Import process can take several minutes to **hours** depending on the size of the pcap file.

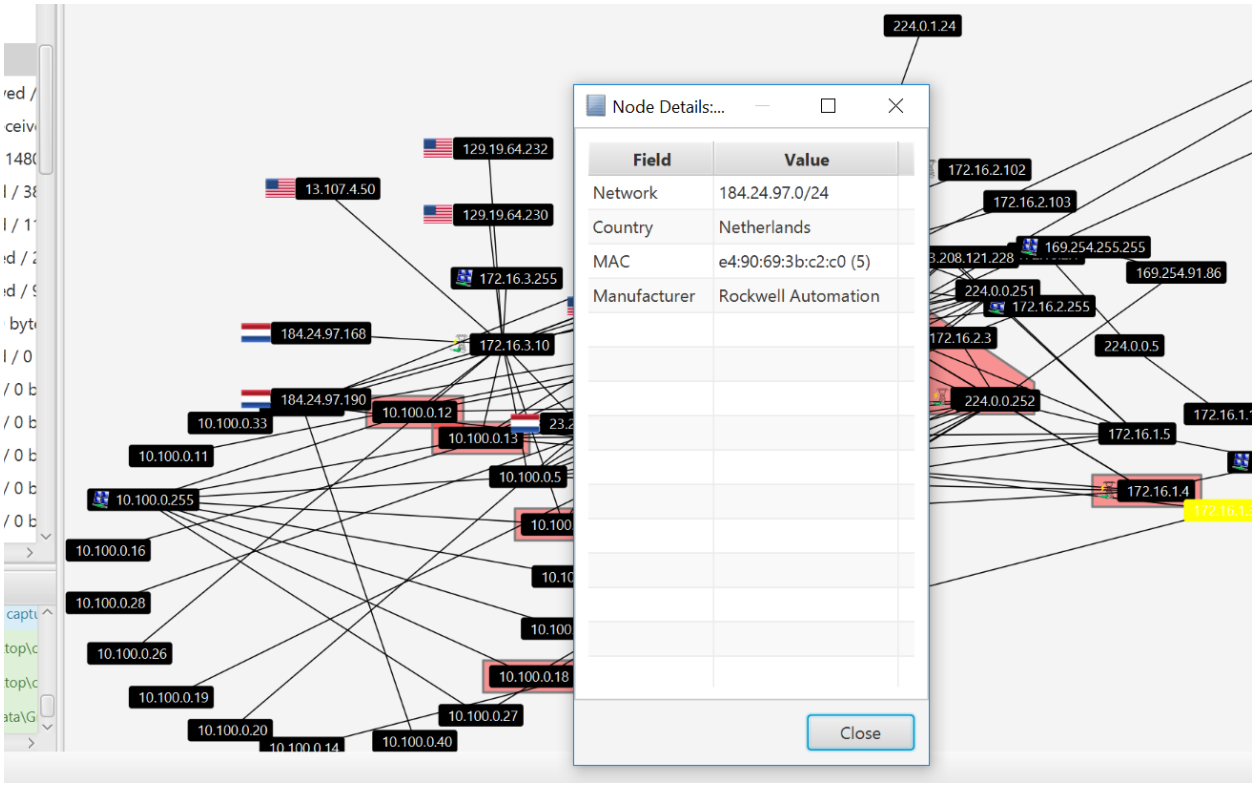


- Upon the completion of Import, the main screen will display a Logical Graph of the network topology as shown below.



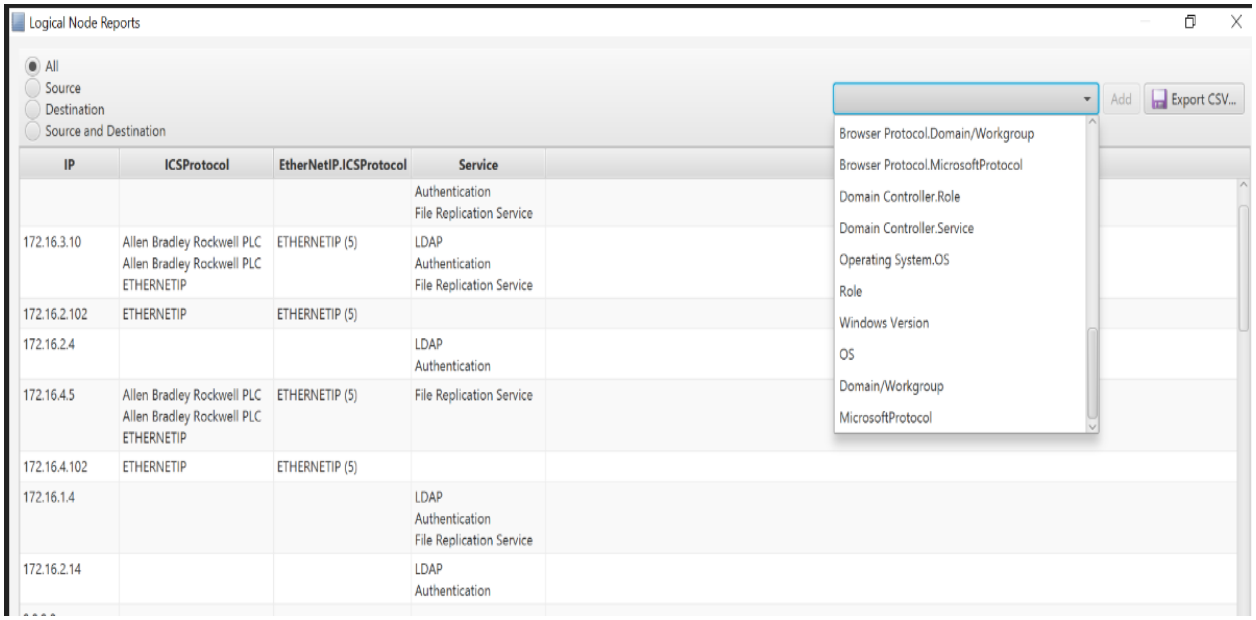
- Take a moment to review the logical graph. The public IP addresses will also be highlighted with their respective Country's flag. This can be useful in finding out information about any external IP's that your network is communicating with.

  Right-click on any external IP address in question >> View Details. For instance, the below image shows a host with ip172.16.3.10 communicating with an IP address from Netherlands.

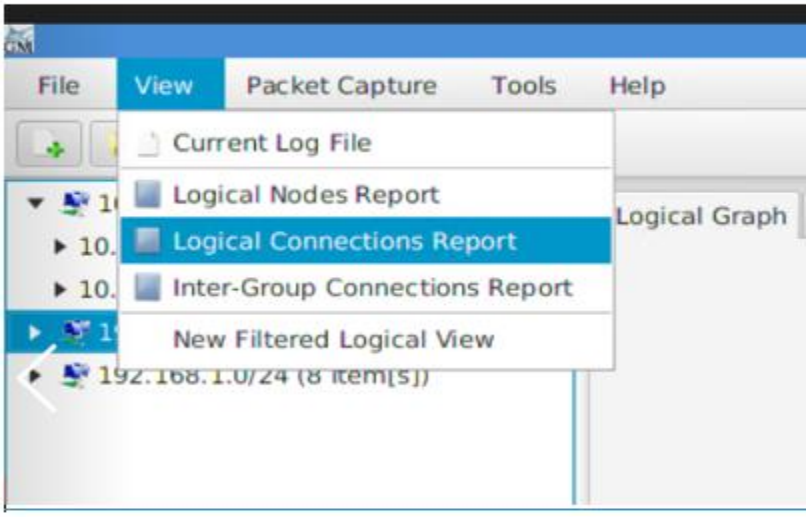


- To Generate a list of all nodes in the Logical Graph, click on **View** (Top Menu) >> **Logical Nodes Report.** By default, only a single column (IP) is present, although additional columns can be added with any Property present in the set of Nodes.

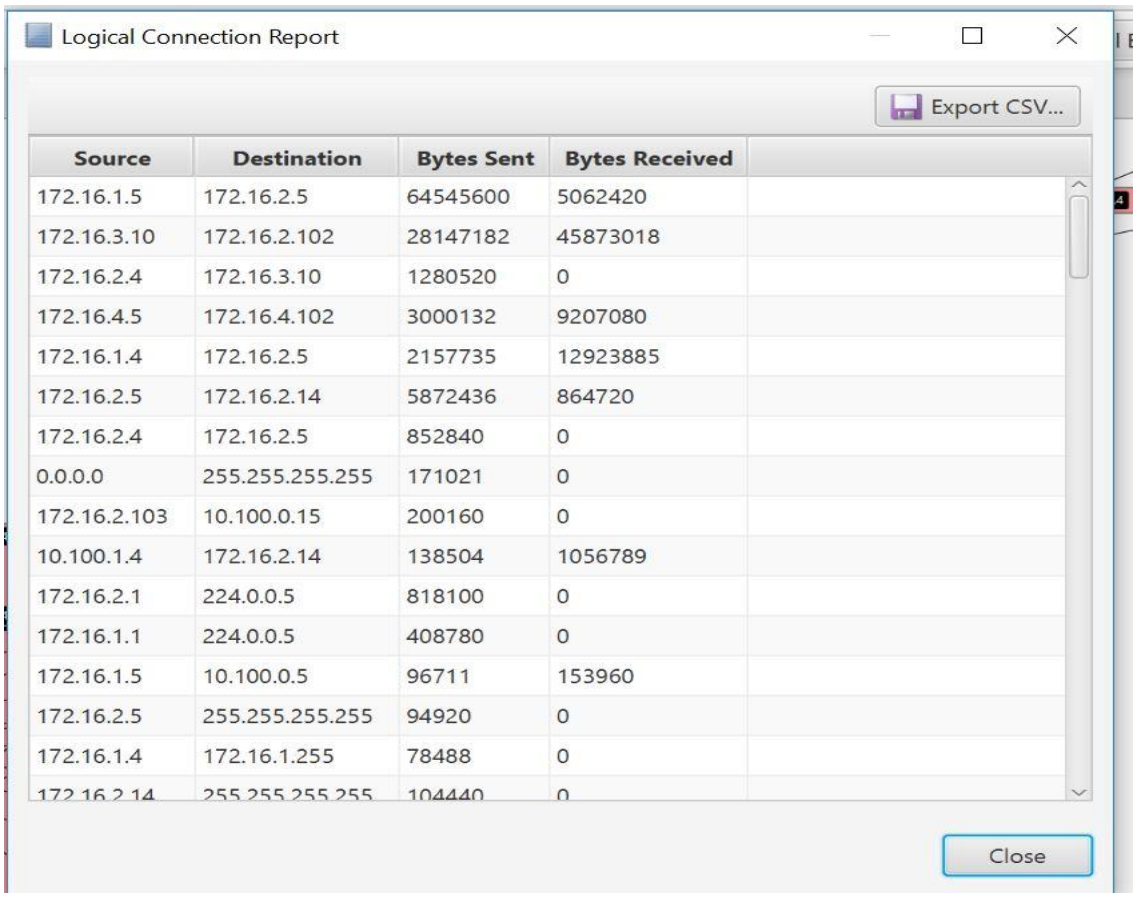
  To add a column, select the Property Name from the drop-down and click the Add button.



- To Generate a Report of all connections in the pcap file, click on **View** (Top Menu)>> **Logical Connections Report**

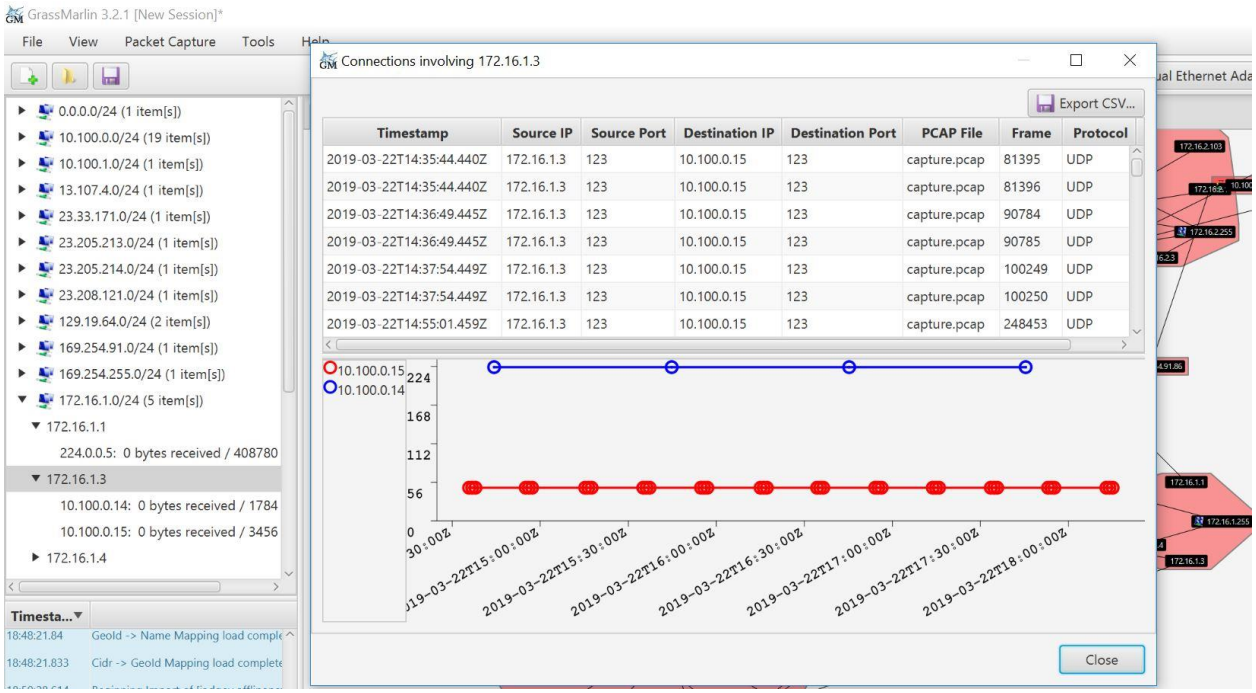


- This will generate an output similar to below shown image. Click on **Export CSV** for further analysis of all the communications happening on your network.

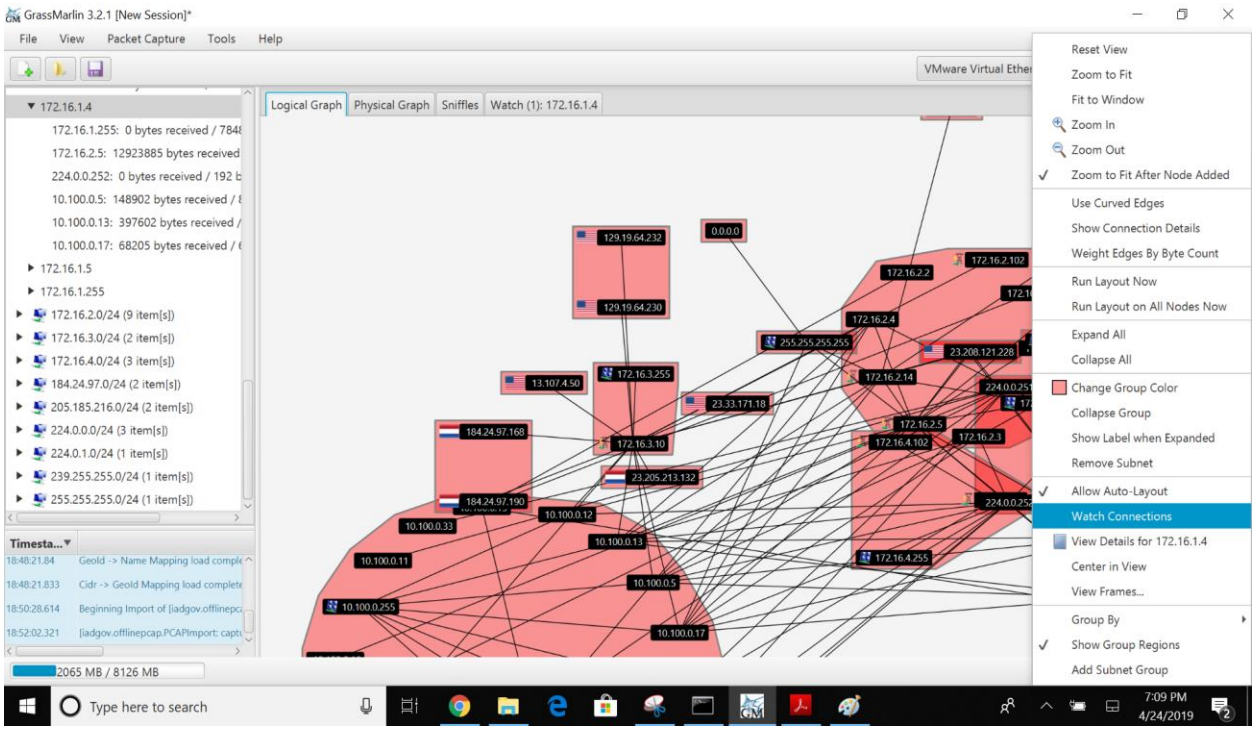


- To view all the logical communications for a specific host for capturing a baseline, under the left-side explorer right-click on a **Node** >> **View Frames**. This opens a new screen as shown below displaying all the different IP addresses that particular host is communicating with including Port and Protocol information. You may click further on "**Export CSV**" button to export this data to a csv file.

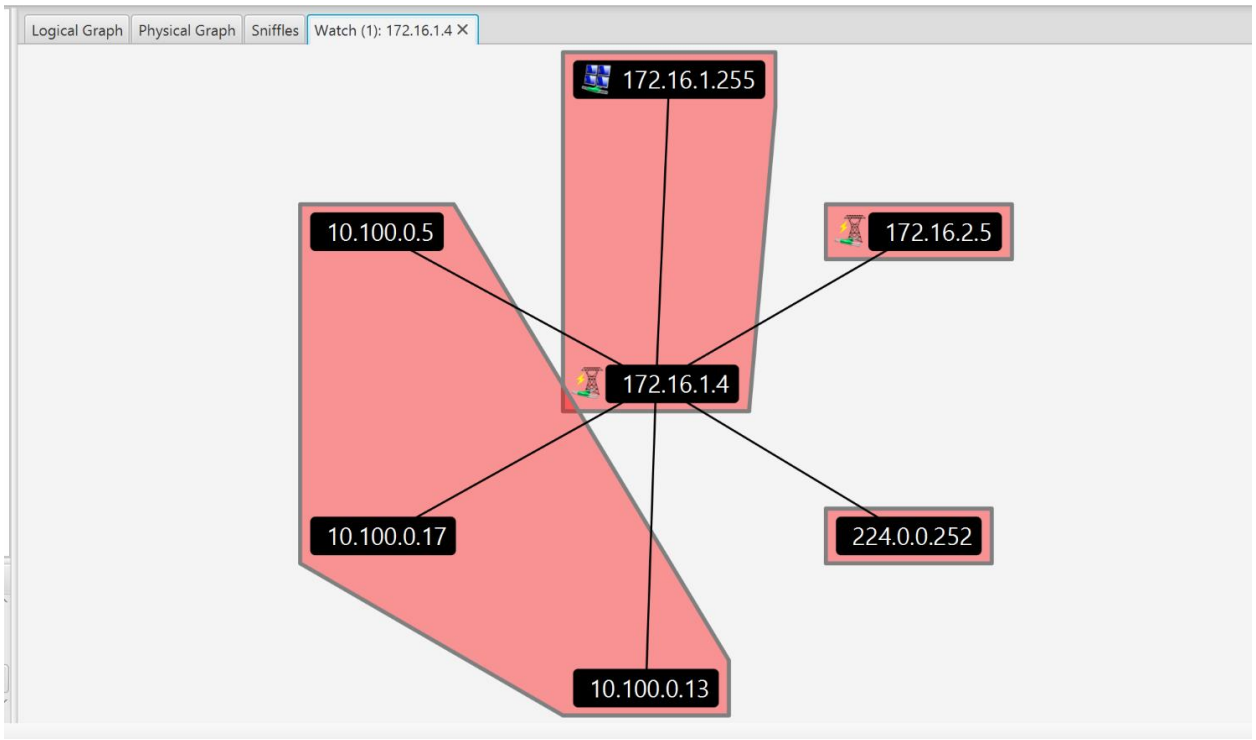
  Note: This process needs to be repeated for every node.



- Another interesting feature is Watch-Graphs. A Watch Graph is a subset of Logical graph, created for a particular node and shows all the different nodes connected to it. This can be generated using **Watch-connections** menu. Right-click a node >> select **Watch Connections**. This will generate a graph in a new window "**Watch <IP address>**"



2885



2886

2887

2888 **4.4.6 Highlighted Performance Impacts**

2889 No performance measurement experiments were performed for the use of GRASSMARLIN due
2890 to its installation location and how it was used (i.e., the software performed offline analysis of
2891 PCAP files captured by other software).

2892 **4.4.7 Link to Entire Performance Measurement Data Set**

2893 N/A

2894

4.5 Wireshark

4.5.1 Technical Solution Overview

Wireshark is a free and open-source packet analyzer. It is user friendly, simple to implement, just need to ensure network connection plugged in is configured to display traffic correctly i.e. Port mirroring.

4.5.2 Technical Capabilities Provided by Solution

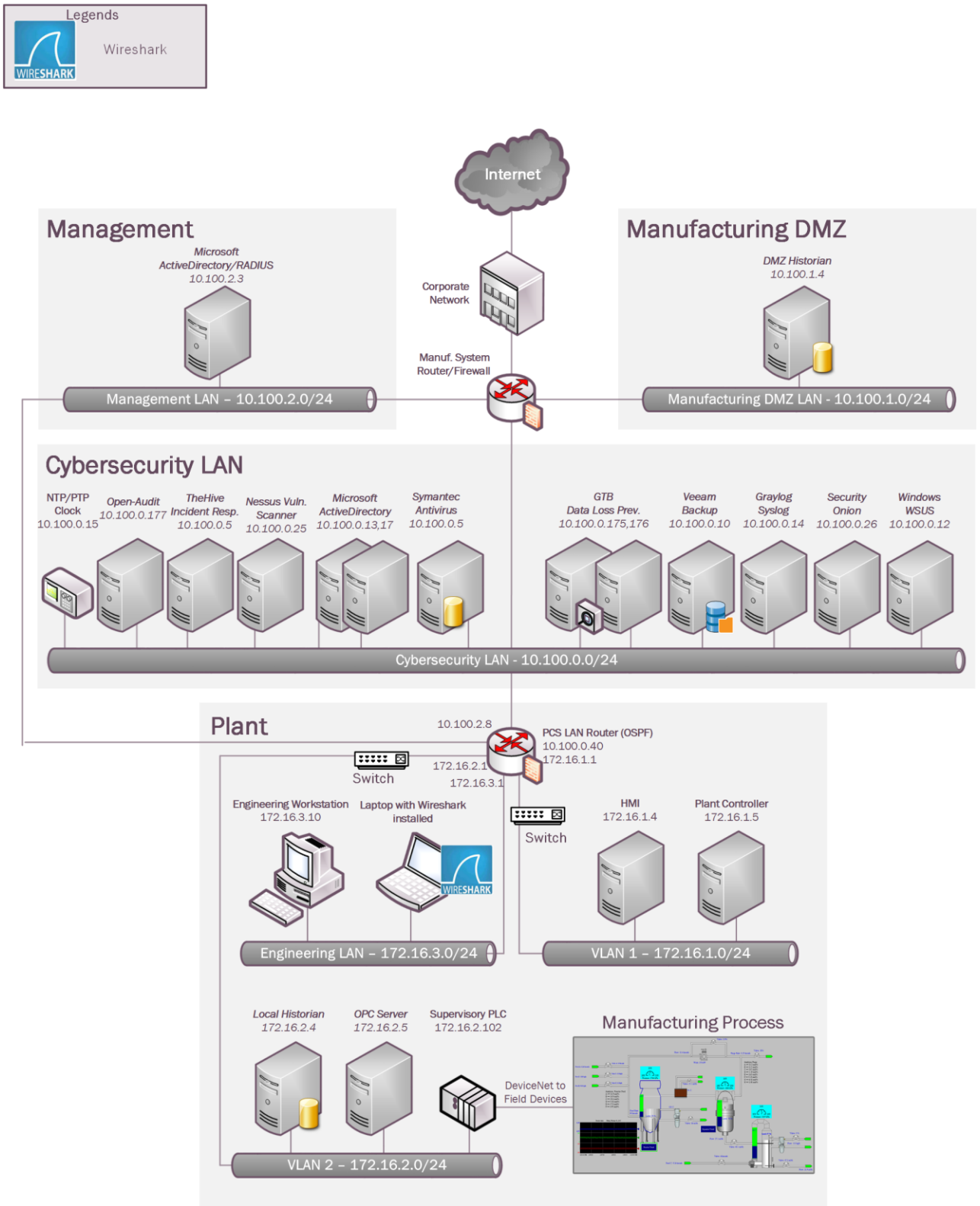
Wireshark provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Network Architecture Documentation
- Baseline Establishment
- Map Data Flows
- Forensics

4.5.3 Subcategories Addressed by Implementing Solution

ID.AM-3, ID.AM-4, PR.AC-5, PR.IP-1, PR.IP-3, PR.MA-1, DE.AE-1, DE.AE-2, DE.CM-7, RS.AN-3

4.5.4 Architecture Map of Where Solution was Implemented

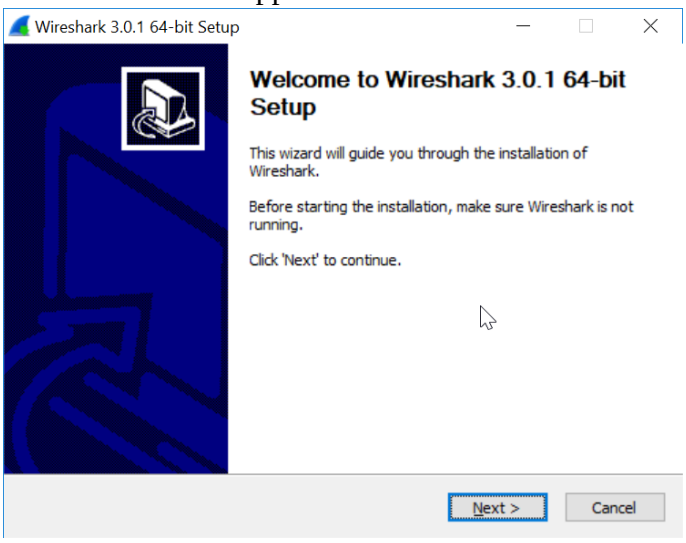


4.5.5 Installation Instructions and Configurations

Steps for installing Wireshark

Download and Installation instructions:

1. Only download Wireshark from https://www.wireshark.org **(Select 32bit or 64 bit)**
2. Once download has completed locate the executable just downloaded and double click to start install process. C:\Users\johndoe\Downloads\Wireshark-win64-3.0.1.exe
3. If prompted for password enter administrator account on local machine.
4. When first Screen appears click **"NEXT"**

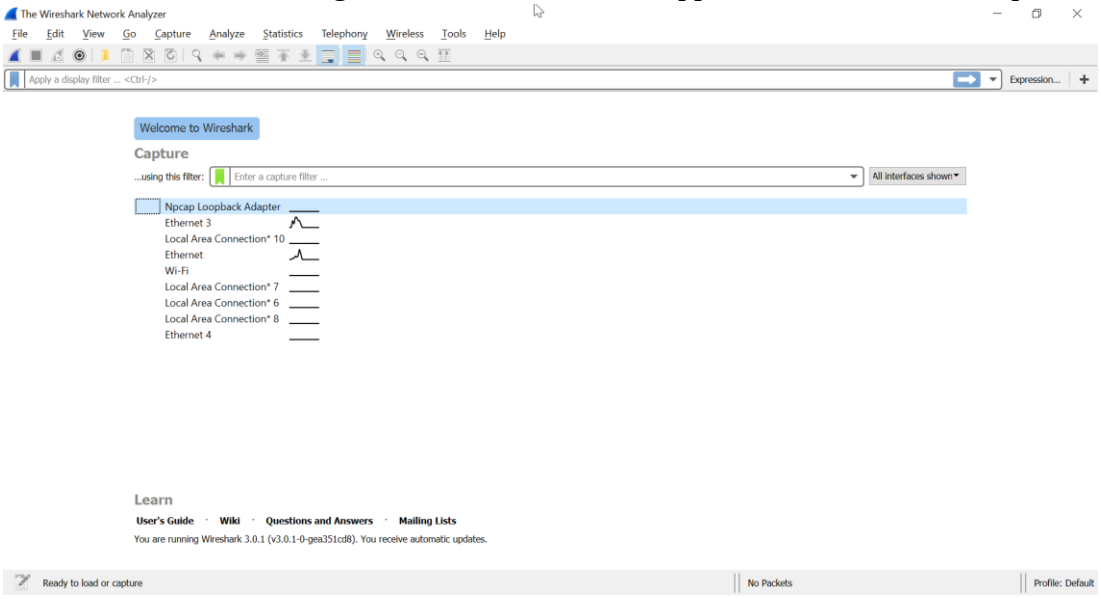


5. Click **"Agree"** to continue.
6. Leave default selected and click **"Next"** five times to continue install. (Make changes if all features aren't required. This will be uncommon)
7. When prompted for Npcap install click **"I Agree"** to continue.
8. Leave default and click **"Install"**.
9. Now click **"Next and Finish"** to start process.
10. Click next and then select **"Reboot Now"** or **"I want to manually reboot later"**
11. Click **"Finish"** to complete.

Running Wireshark and configure

1. Click start button and find program labeled **"Wireshark"**.
2. Once Wireshark is found right click on icon and select **More→Run as Administrator (Windows 10)** Older operating system can just hold down **"Shift + Right Click"** menu will appear for run as, select administrator to continue.
3. Wireshark requires administrative privileges to be fully functional, otherwise there will be undesired results.

4. Once Wireshark is running the initial interface will appear that the screen shot provided.

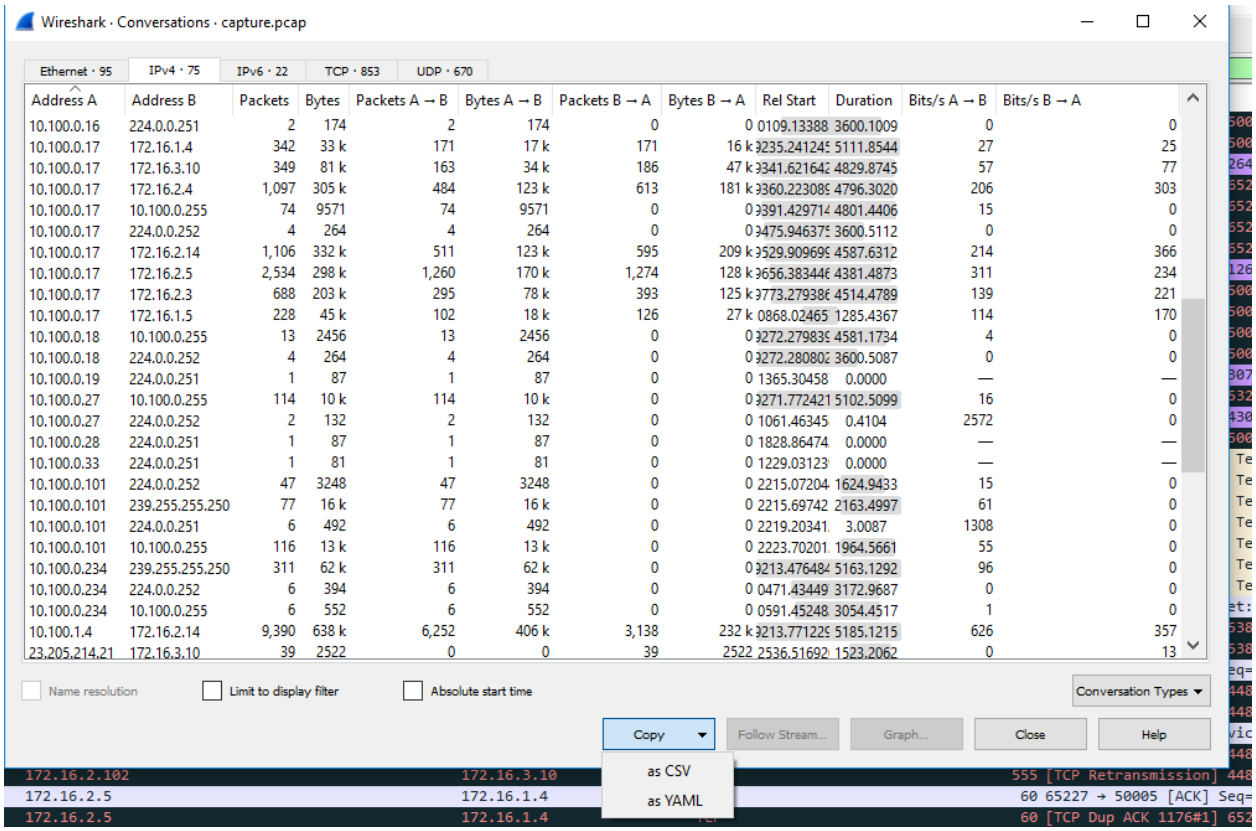


5. Select the interface to be monitored.

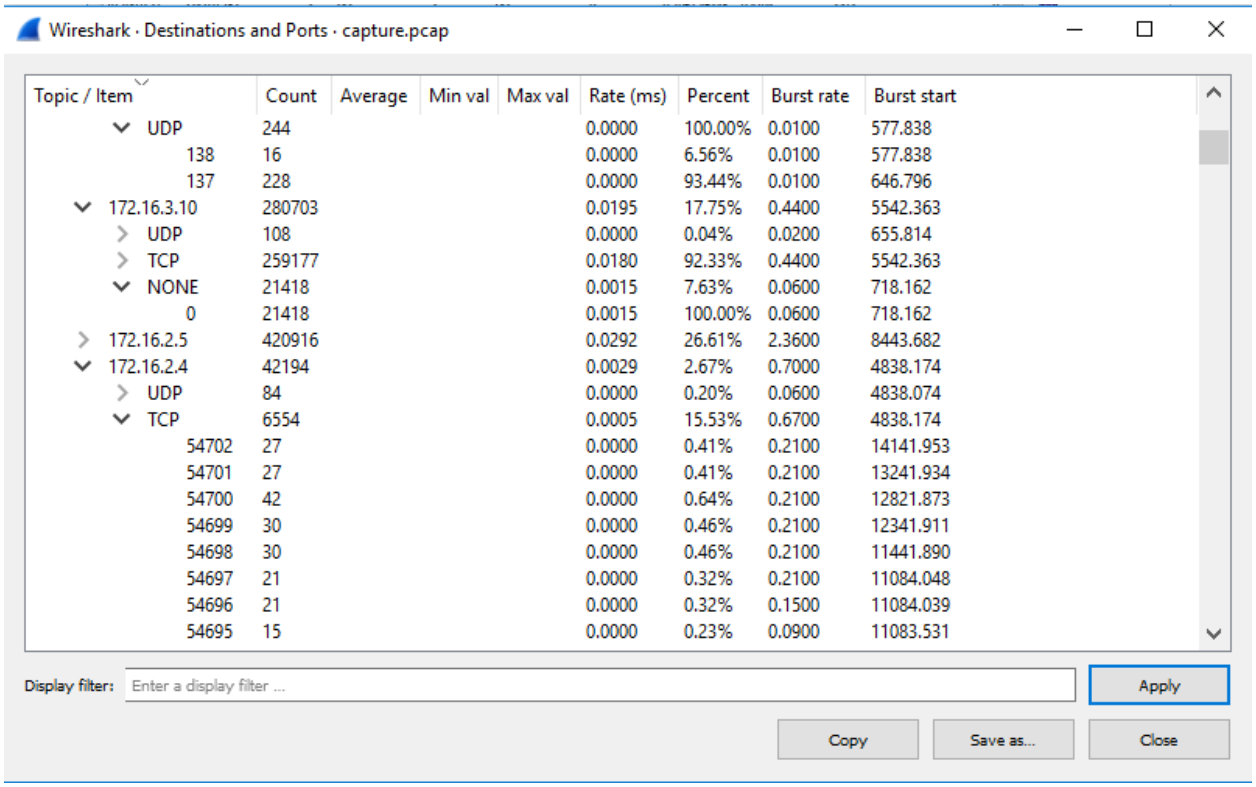
Wireshark provide lots of information and can be hard to decipher https://www.wireshark.org provides documentation along with searches for additional command syntax.

Capturing Network Baseline using Wireshark

1. Launch Wireshark. Click **Open** to load a previously captured pcap file or run a **"Start Capture"** as explained in the previous section to record traffic.
2. Upon loading the pcap or capturing live traffic; click on **Statistics** >> **Conversations**
3. This will generate a window similar to the one below which will list all the different types of communications happening between all endpoints in your traffic. Click **COPY** >> **as Csv** to save this data as a Csv file for further analysis.



4. To get a list of ports used, Click on **Statistics** >> **IPv4 Statistics** >> **Destination and Ports.** This will generate a list of ports used by all the IP addresses in the traffic. Click **Copy**, to copy the results to a word document or click **Save as** to save as a plain text file. Hit **Close** when done.



4.5.6 Highlighted Performance Impacts

The following performance measurement experiment was performed for the Wireshark tool while the manufacturing system was operational:

Experiment PL015.2-wireshark

Significant performance impact on computing resources was observed when using Wireshark for network traffic capture. Both the processor and memory utilization of the host were significantly higher than normal. There was no performance impact to the manufacturing process observed.

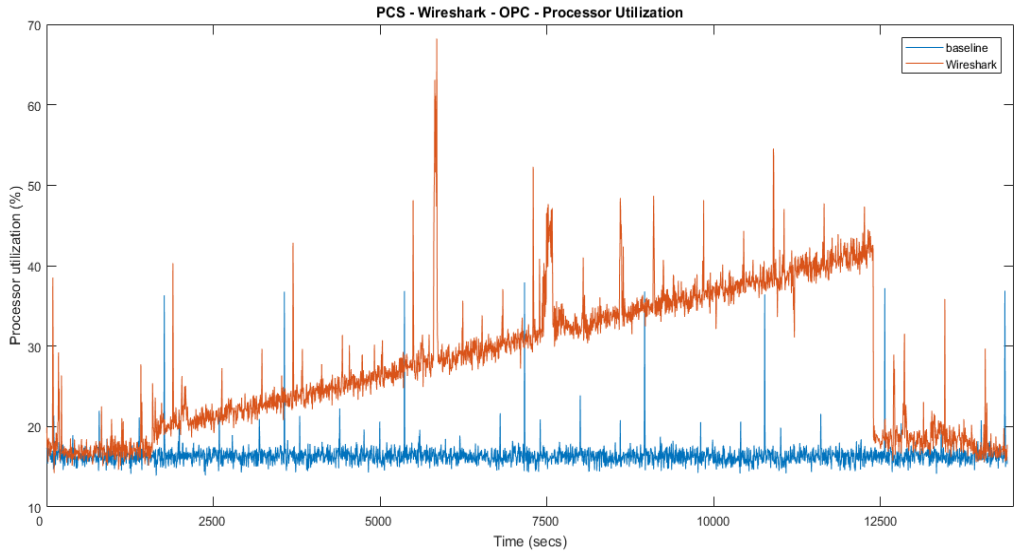


Figure 4-5 Processor utilization of the OPC computer during Wireshark network capture

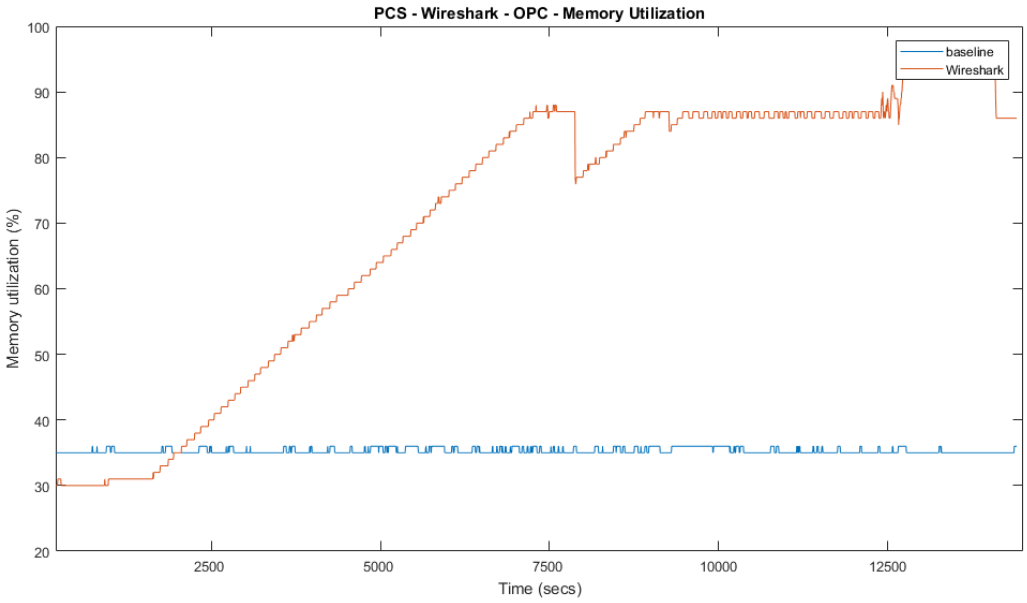


Figure 4-6 Memory utilization of the OPC computer during Wireshark network capture

Wireshark started at around 1900 seconds experiment time and continued to capture network traffic for about 3 hours. During this period of time, the processor utilization of the OPC computer kept going up. Wireshark has a sizeable impact to the processor utilization. The Wireshark data file was about 2.3GB in this case.

The memory utilization has a similar impact to the processor utilization, except the memory utilization stayed high after Wireshark has stopped capturing the network traffic. It is hypothesized that Wireshark stored the captured data in memory until the data was saved into the

hard drive. Therefore, the memory utilization stayed high even after the Wireshark has stopped the network capture. Even though the processor and memory utilization were significantly higher, they were still below the full capability of the computer and therefore did not have major impact to the manufacturing process. However, for the manufacturing system that has a high utilization in normal run time, the use of Wireshark may cause a performance impact.

The PCS system uses an external computer to use Wireshark to perform network traffic capture for this reason. Care should be taken if using Wireshark on a production system.

4.5.7 Link to Entire Performance Measurement Data Set

Wireshark KPI data

Wireshark measurement data

4.6 Veeam Backup and Replication

4.6.1 Technical Solution Overview

Veeam Backup and Replication is a proprietary backup and incident recovery software developed by Veeam for virtual environments. It is built on VMware vSphere and Microsoft Hyper-V hypervisors. The software provides backup, restore and replication functionality for virtual machines. Veeam® Backup and Replication suite delivers availability for all workloads - virtual, physical, cloud (including VMware vSphere and Microsoft Hyper-V) -from a single management console. It provides fast, flexible and reliable recovery of your applications and data, and brings backup and replication together into a single software solution [1].

The Veeam Backup Free Edition lets you back up your VMs on the fly and provides you with flexible storage options, including file-based (NFS) primary storage, for easy archiving and quick recovery. Veeam also has products such as “Veeam agent for Windows” and “Veeam agent for Linux” for backing up physical Windows and Linux servers respectively.

Points to consider:

- Free backup edition available for virtual and physical servers.
- Support for file level backups as well as system image type of backups.
- Backups can be run without having to shut down the system. This can be very critical in ICS/SCADA environments.
- Tech support available for Free edition users.
- Easy to setup and use. Lot of documentation available online to get started.

4.6.2 Technical Capabilities Provided by Solution

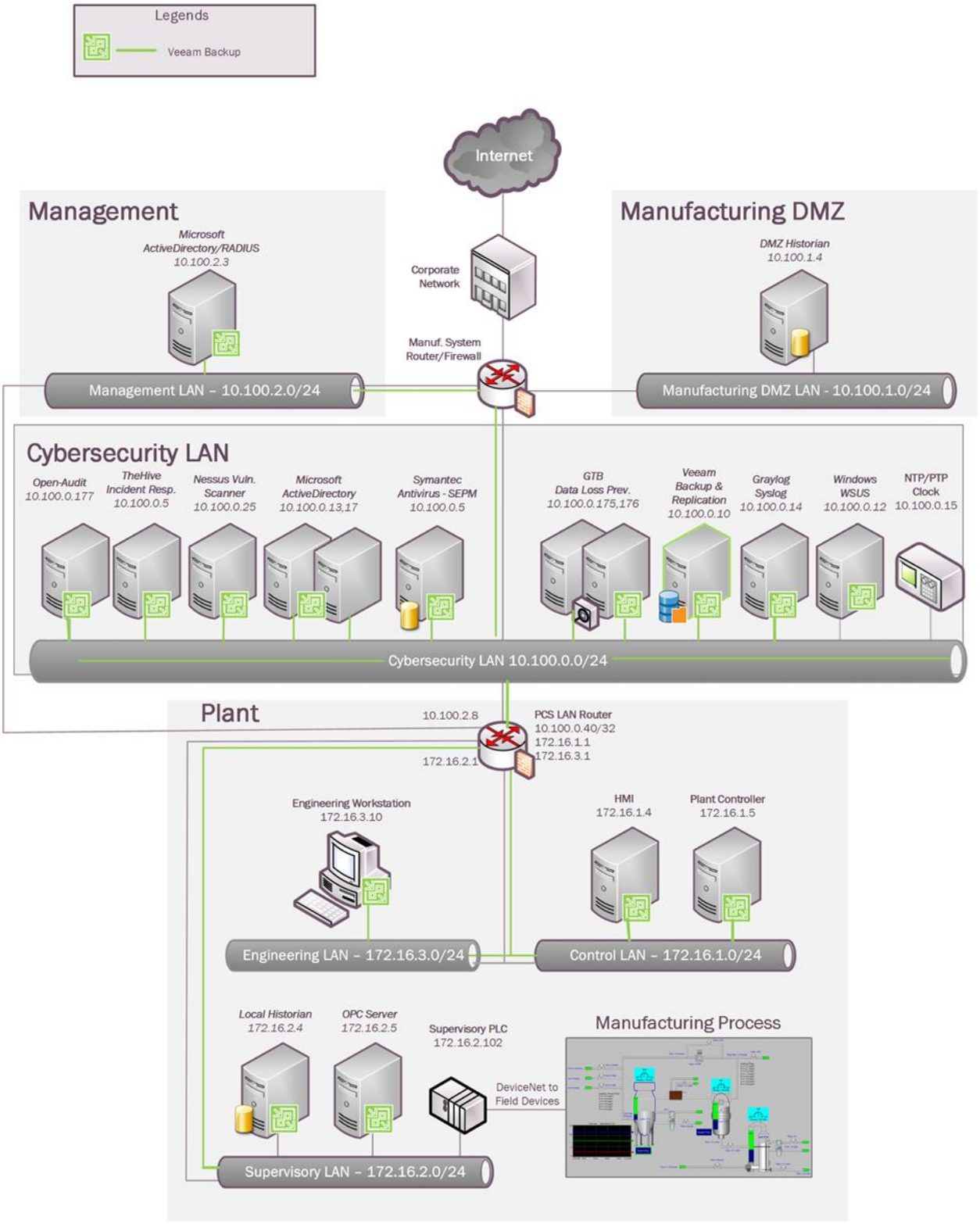
Veeam Backup and Replication provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Data Backup
- Data Replication

4.6.3 Subcategories Addressed by Implementing Solution

PR.IP-4

4.6.4 Architecture Map of Where Solution was Implemented



4.6.5 Installation Instructions and Configurations

Setup

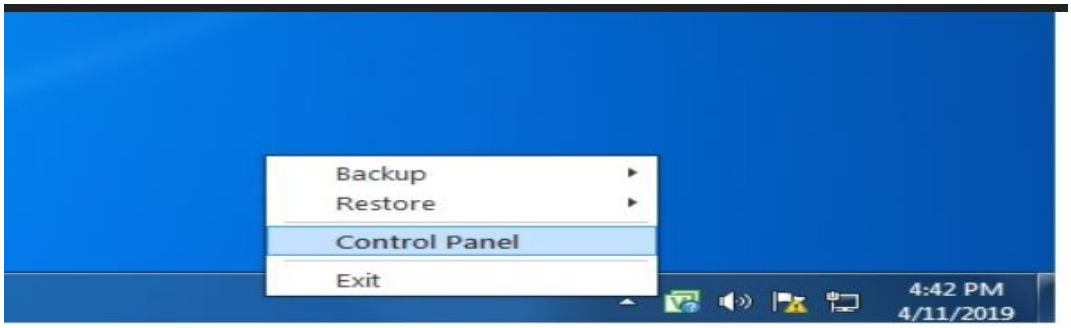
- The following products from Veeam were implemented

Name	Purpose	Version
Veeam Backup and Replication	Veeam Backup Server and Repository	9.5
Veeam Agent for Windows (Free version)	For backup/recovery of Physical Windows Systems in Process Control Network	3.0.0.748

- A Windows 2012 Virtual Machine was setup in the Cybersecurity LAN for installing Veeam Backup and Replication Server. Around 4TB of storage was allocated to this VM for backup storage.
- The Free Edition of Veeam Backup and Replication lets you manage virtual machine backups from the Central Veeam Backup and Replication Console. However, any physical servers configured for backup using the Veeam agent cannot be managed from the Central console in the Free edition. These need to be managed locally on the endpoint or client system itself.
- A parent folder called "**backups"** was created on the 4TB storage drive for saving the backups. Within this folder, different sub folders were created as per the Server names of Process Control System. Each system's backup was configured to save its data into its corresponding server name folder. The backups folder was then configured as a network share.
- A service account named "**veeamuser**" was created in Active Directory (Cybersecurity LAN) for backup and recovery purposes. This user was granted Read/Write permissions on the above share.

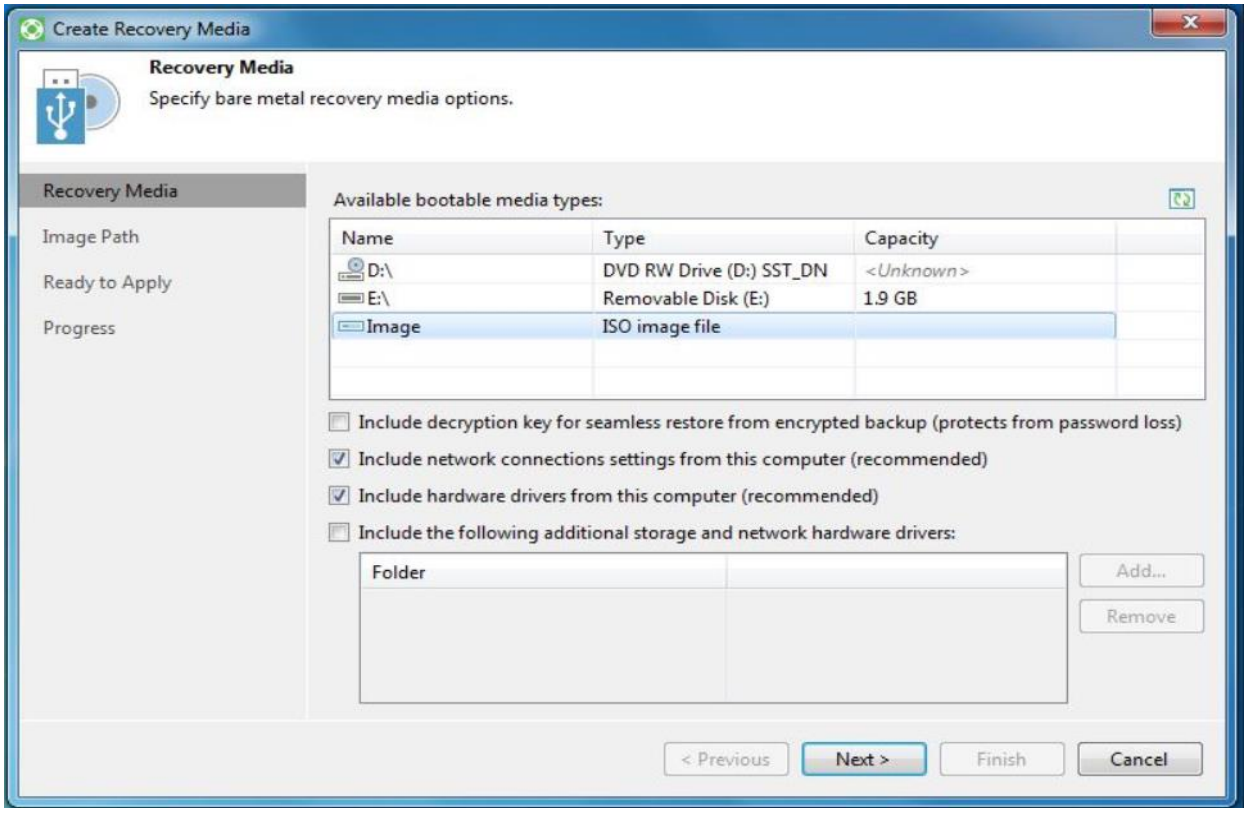
Backups

- All Windows systems of Process Control Network were configured for Backup using Veeam Agent for Microsoft Windows [2].
- The Veeam agent was installed on all Windows clients (systems). Connectivity between each client and the Veeam Server was verified by accessing the "**backups**" share folder (created in the above section) from each client.
- In the Free version, a backup or restore operation needs to be initiated from the client system. Once the agent is installed on the client system, double click the "**Veeam backup icon**" in the System tray to launch the wizard.

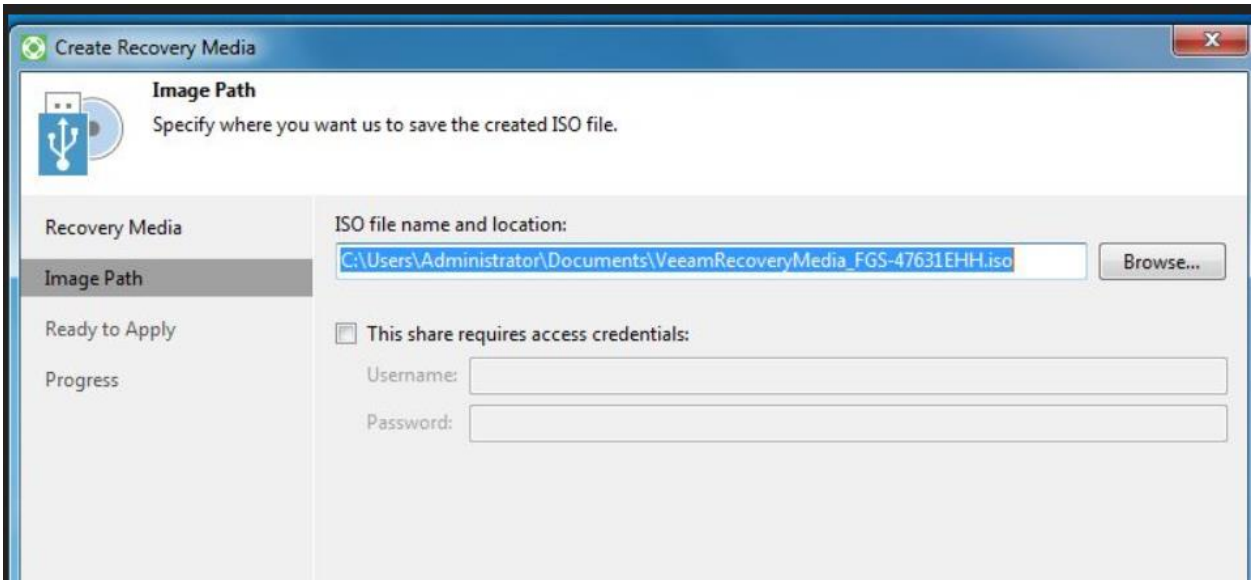


- If this is your first time, the setup wizard will prompt to create a "Recovery Media" which is required for Bare metal backup and restore operations. It is recommended to create this Media if your backup mode is a Full Computer image.

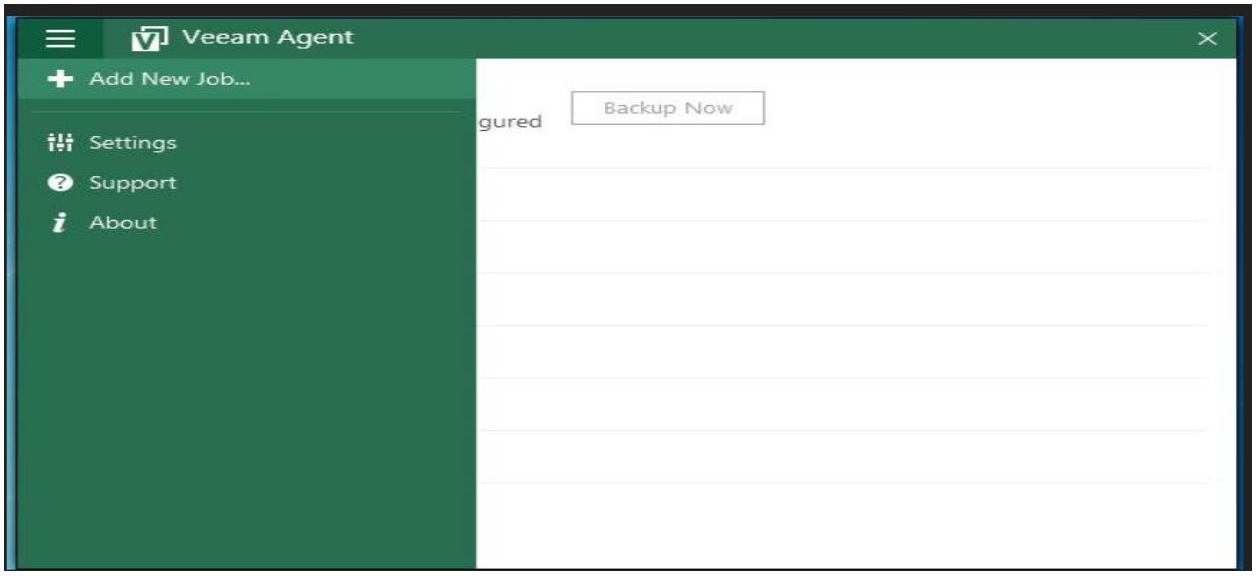
This media creation wizard can also be launched manually by running **Veeam.Endpoint.RecoveryMedia.exe** program under **C:\Program Files\Veeam\Endpoint Backup** directory. Once launched, select one of the 3 options under **Available Bootable Media Types** as per your requirement



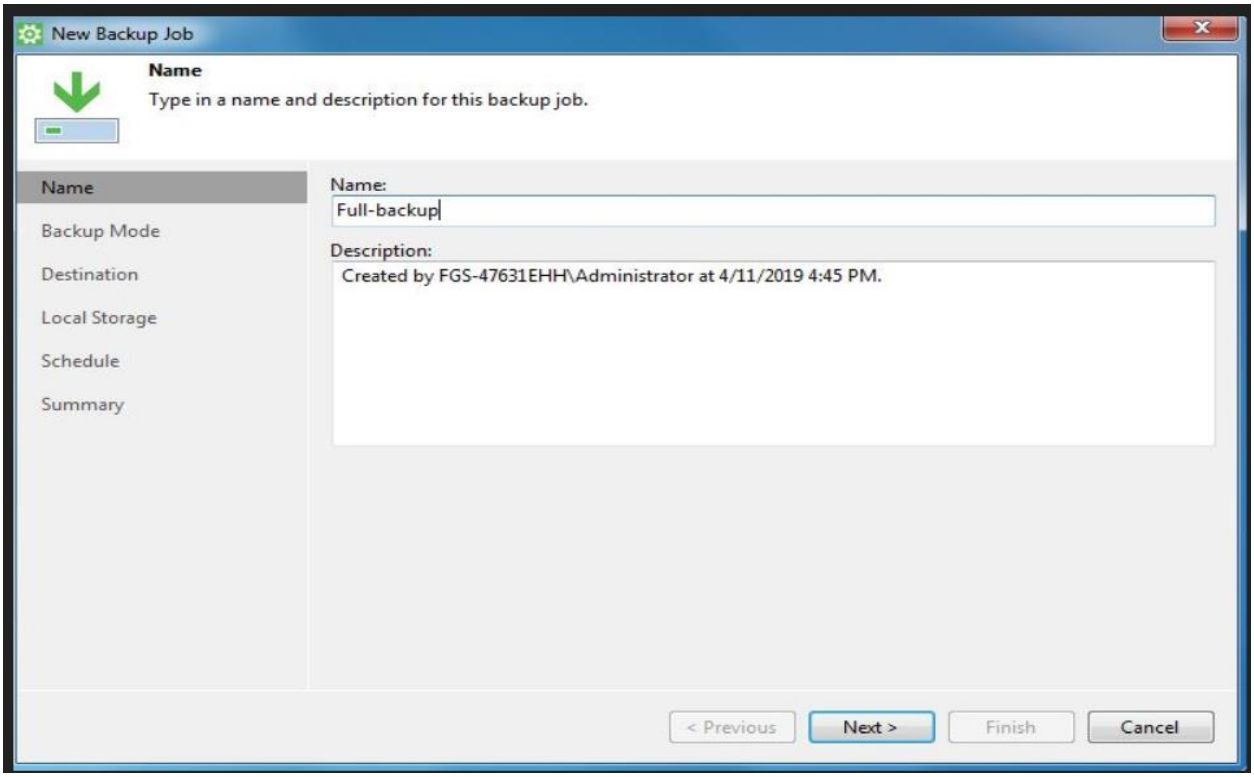
- If ISO option is selected, enter the name and location to save the ISO.



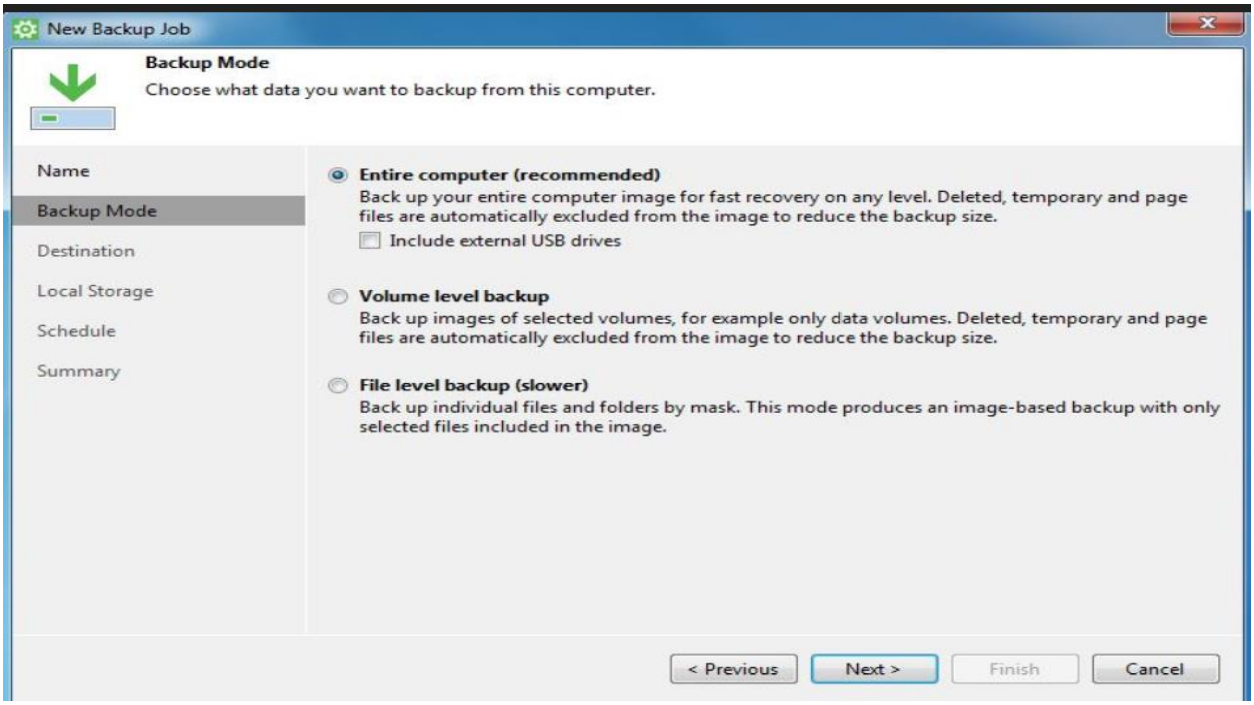
- The system will need to be booted off the ISO when performing a Restore / Recovery option of the Entire Computer or Volume based backups.
- There are 3 types of backup jobs supported –
  (1) Entire Computer which is the system image
  (2) Volume level
  (3) File level backup.
  However, only one type of backup job can be scheduled in the Free version.
- To configure a backup job, Right-click on the Veeam Tray, select "**Control Panel** >> **Backup"** >> Click on **Add New Job**



3076 • Enter a Name for the Backup Job
3077

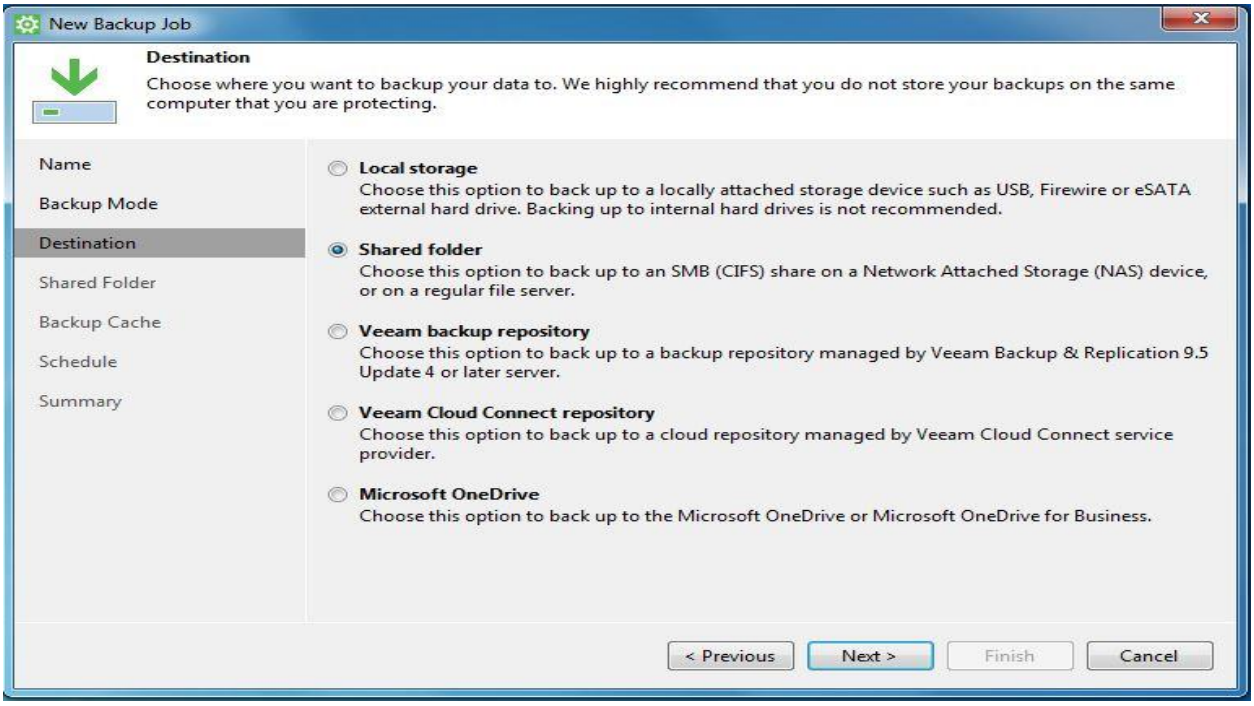


3078
3079
3080 • Select a Backup Mode. For instance: Entire Computer
3081

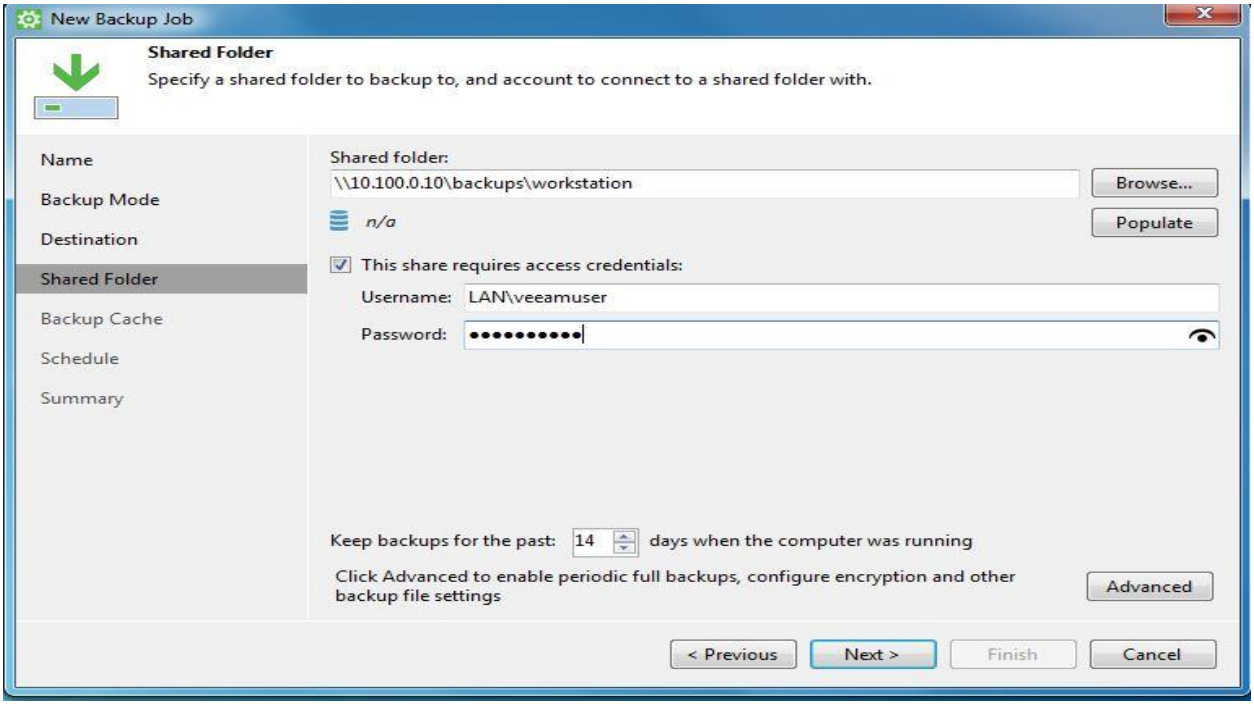


3082

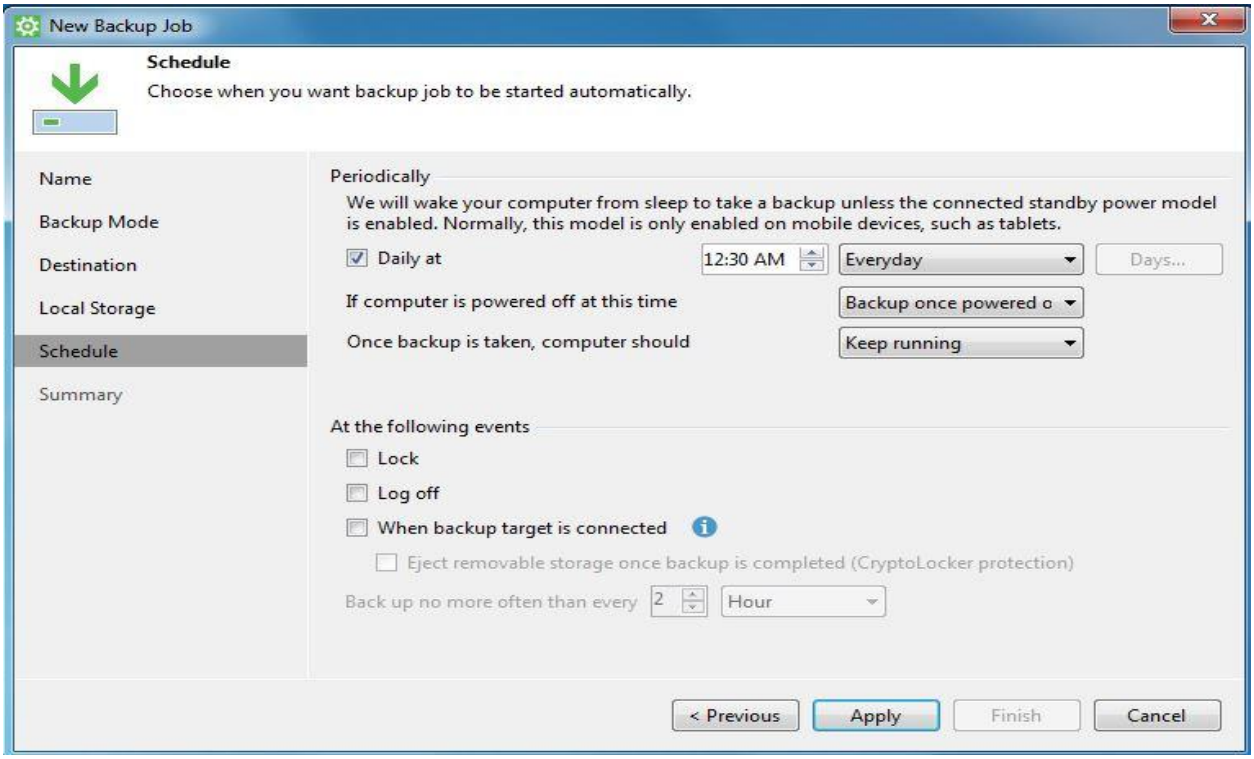
- Select a Backup Destination. Choose "**Shared folder**" if saving the backups to a network share as in our case.



- Enter the path of the Network share and the Active Directory user credentials created earlier. Select the Number of Restore Points as per your retention policy.



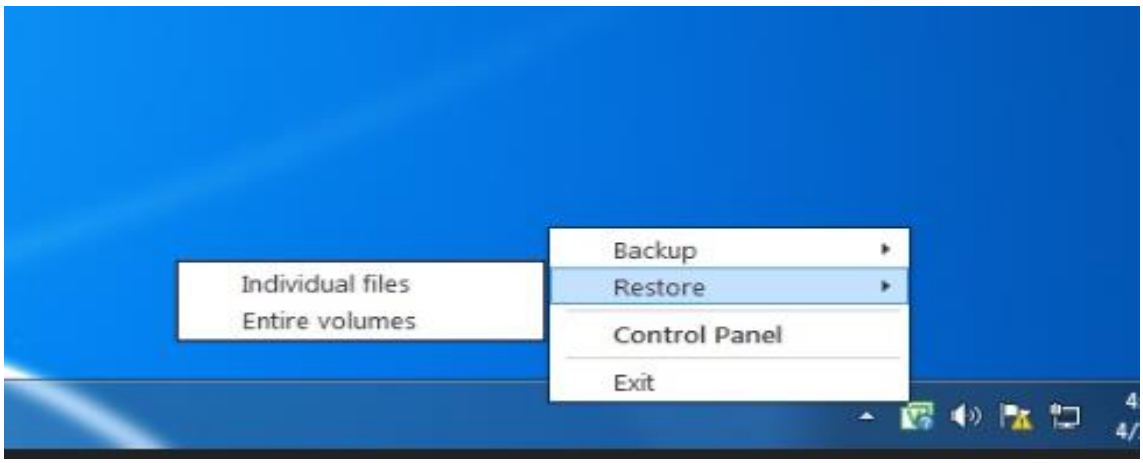
- Configure a Schedule. Hit **Apply** when done.



Recovery:

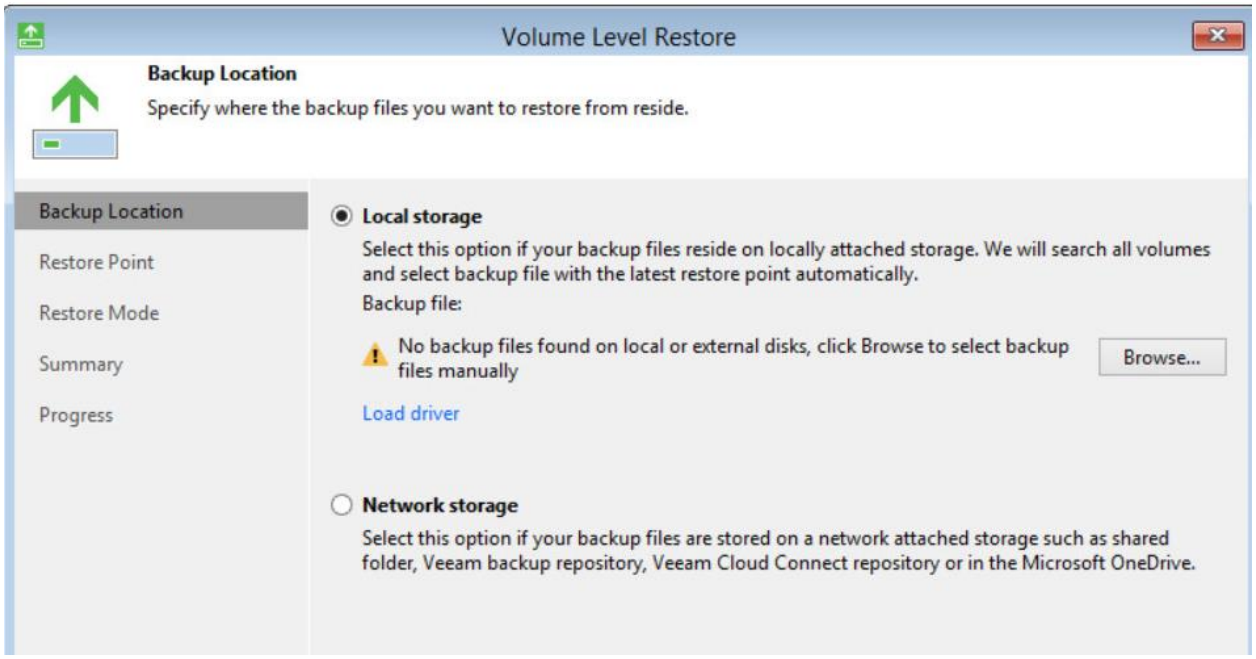
- Recovery of Individual files or Volumes can be done using the Veeam agent in the System Tray itself. Double click on the Agent icon >> **Restore** >> Select <Type> >> Follow the steps.

Note: This is dependent on having a successful File-level or Volume-level Backups captured previously.



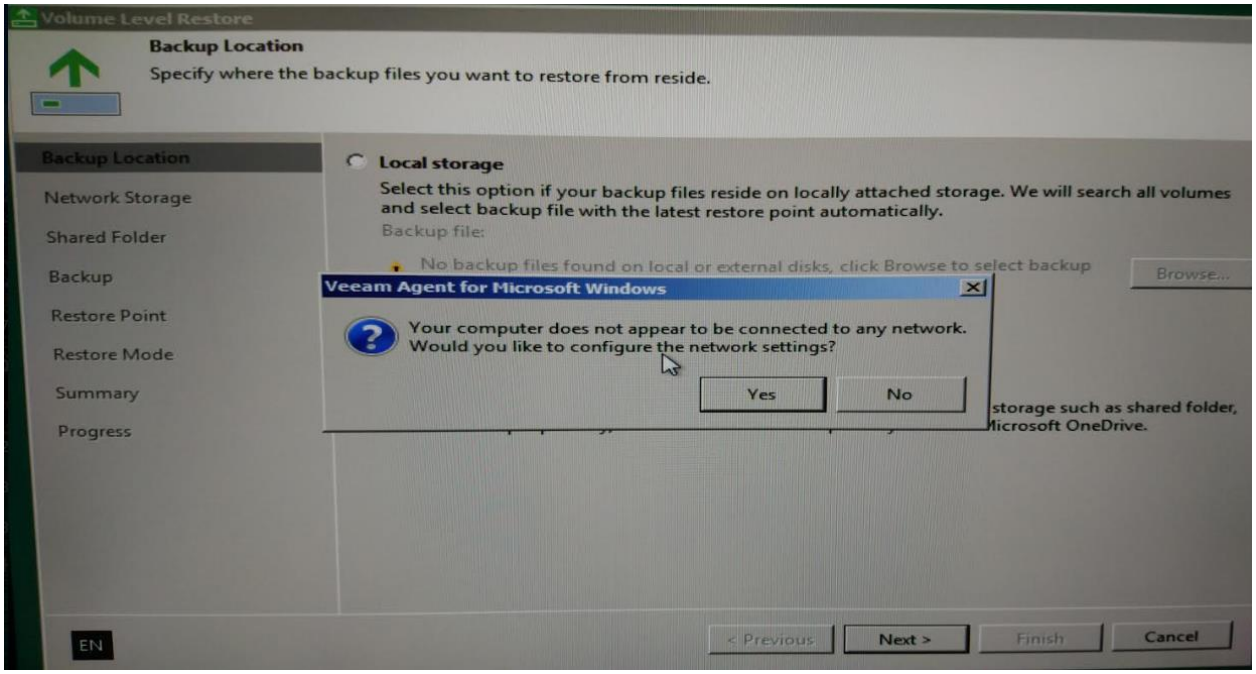
3104 • To perform a Bare Metal restore of the Entire Computer, Boot the system using the
3105 Recovery media created earlier. Click on “Bare Metal Recovery”
3106

3107
3108
3109 • Select “**Local Storage**” if restoring backups from an External USB Drive or “Network
3110 Storage” if restoring from a network share as in our case.

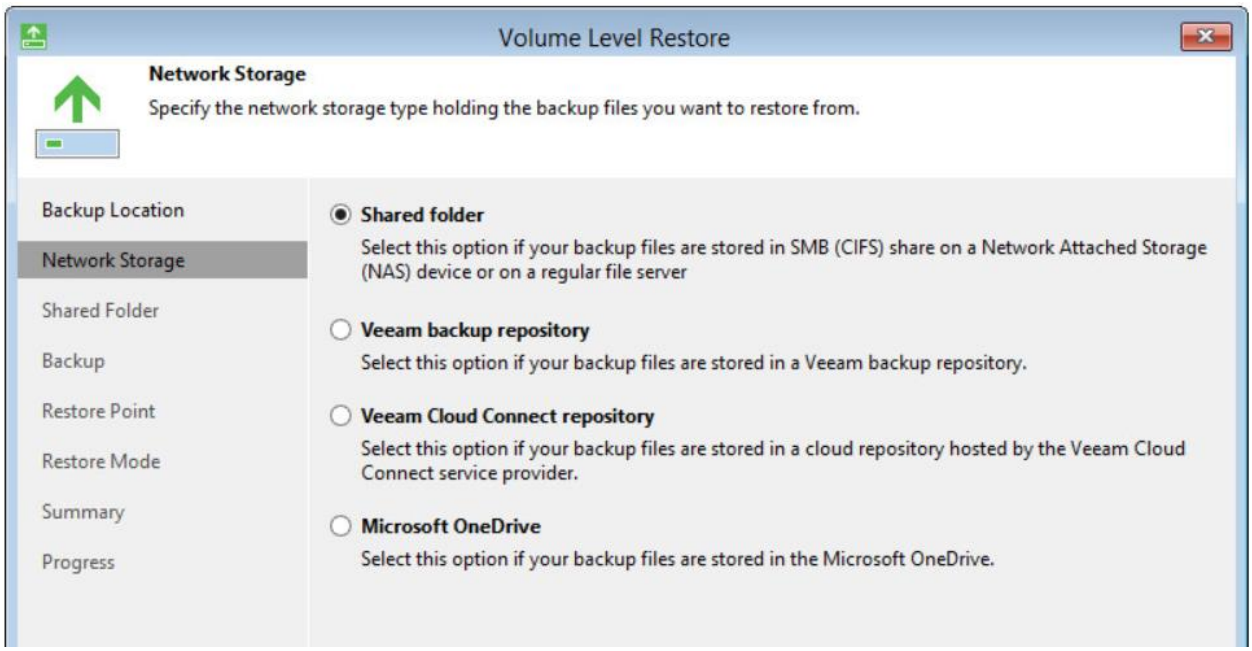


3111

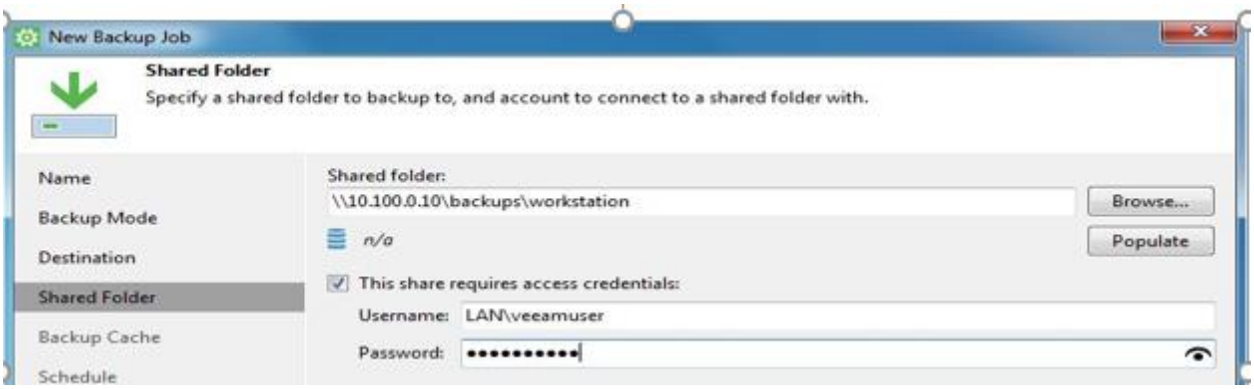
- An option will be presented to configure Network Settings. Choose either DHCP or Static IP and hit Continue.



- Under "Network Storage", select **Share folder**. Hit **Next**

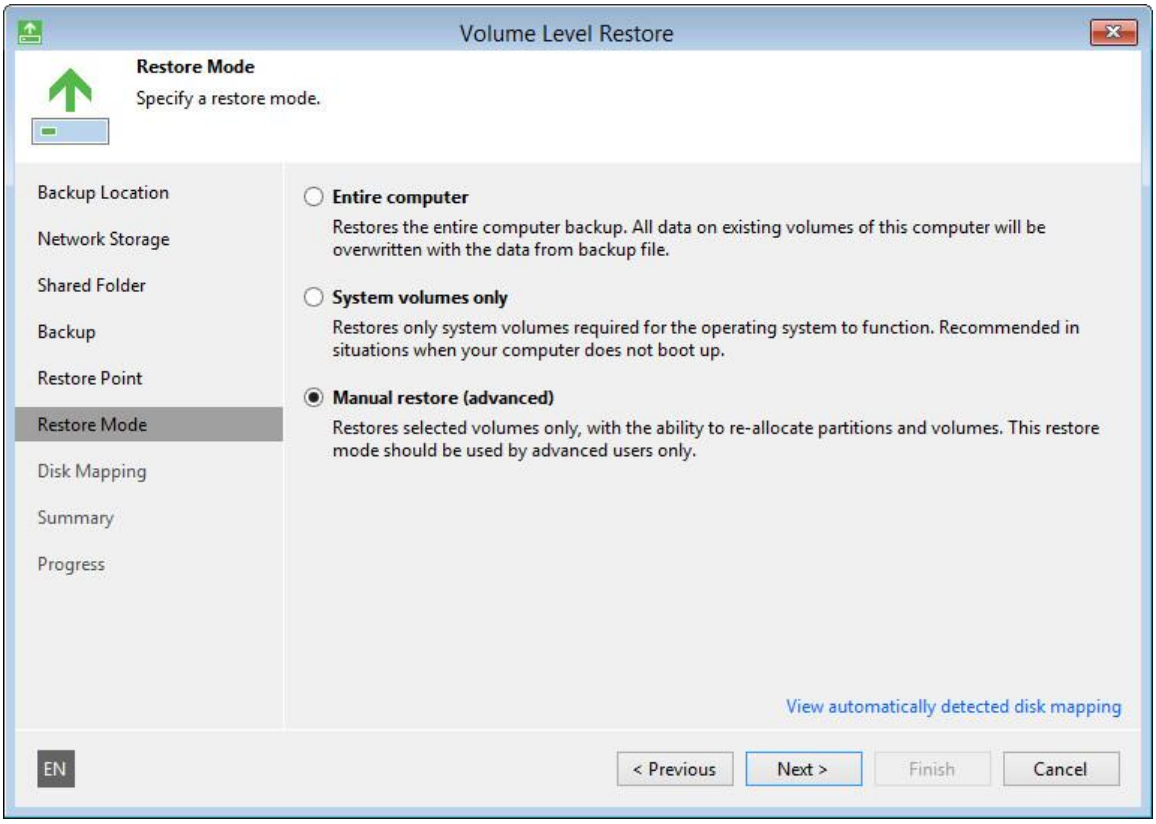


3122 • Enter the path of Share folder to restore from. For instance:
3123



3124

3125 • Next, assuming the wizard is able to connect to the Network share, it will populate a list of
3126 Backups. Select a Backup and hit Next.
3127 • Under **Restore Points** select a restore point from which you want to recover data. Veeam
3128 Agent for Microsoft Windows displays only restore points of volume-level backups.
3129 • Select a Restore Point and hit Next.
3130 • Under **Restore Mode**, choose a Restore Mode. If the disk type and layout on the system has
3131 not changed select "Entire Computer". There is a Manual restore available for advanced
3132 users.



3133

- Under **Disk Mapping**, Map restored drives as per your system layout. For detailed instructions on how to map, refer to https://helpcenter.veeam.com/docs/agentforwindows/userguide/baremetal_disk_mapping.html?ver=30
- Under **Summary** Page, review the summary. Hit **Restore** to start the restore process.

References:

[1] Veeam Backup and Replication https://www.veeam.com/vm-backup-recovery-replication-software.html

[2] Veeam agent for MS Windows Free edition https://www.veeam.com/windows-endpoint-server-backup-free.html

4.6.6 Highlighted Performance Impacts

The following performance measurement experiment was performed for the Veeam Backup tool while the manufacturing system was operational:

Experiment PL009.2- Veeam full backup
Experiment PL010.1- Veeam incremental backup

A small performance impact to the manufacturing process was observed in, however, a more noticeable impact was observed in the network traffic. For example, the round trip time from the Controller to the OPC was increased significantly during the backup. The path delay from the OPC to HMI was also increased significantly during the backup. The amount of backup traffic could take up a large portion of the available bandwidth.

Also, there is storage consideration, example of backup size in the PCS system: HMI: 96GB, OPC: 29GB, Controller: 31GB, Historian: 194GB

Network usage should be taken into consideration on when to perform a full backup, a low network utilization time is likely to reduce the impact to the system One important feature of the Veeam backup is its ability to throttle to adapt to the network utilization in order to avoid taking up all the available bandwidth for the backup traffic.

Incremental backup should be considered for periodic backup instead of full image backup.

During the full backup, the network traffic increased dramatically, in one case, the backup of the HMI and Controller hosts represented 99.6% of the total traffic verse 0.4% of the normal traffic.

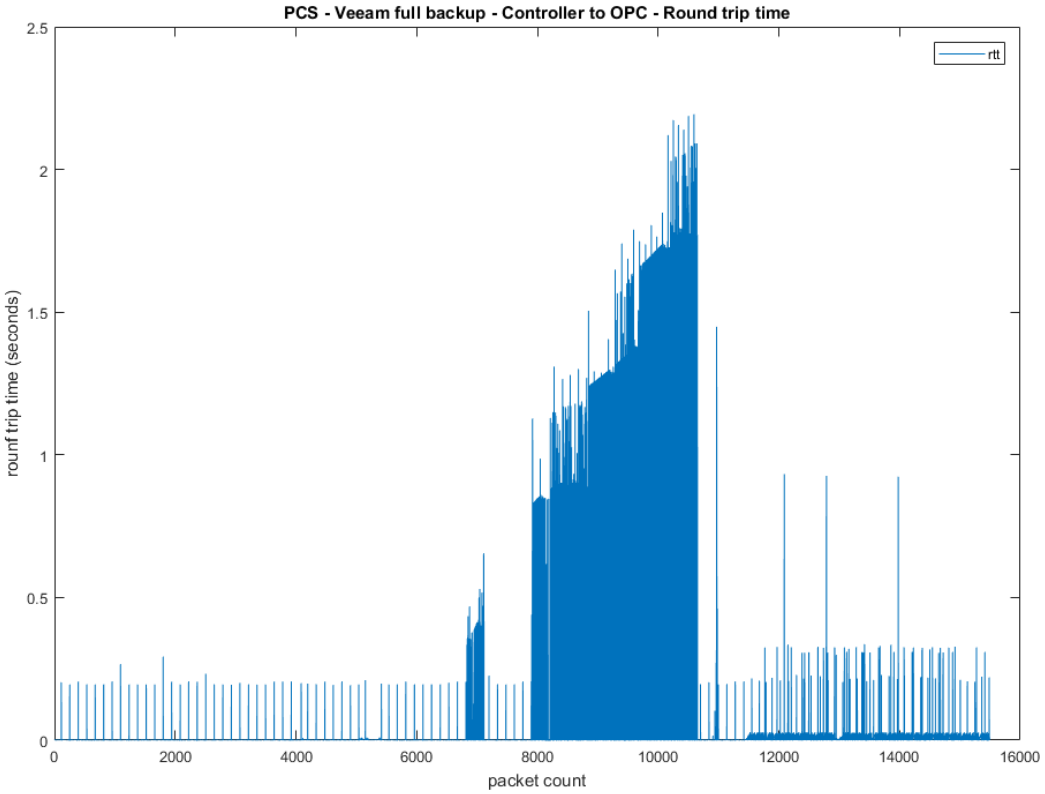


Figure 4-7 Plot of packet round trip time from Controller to OPC during Veeam full backup

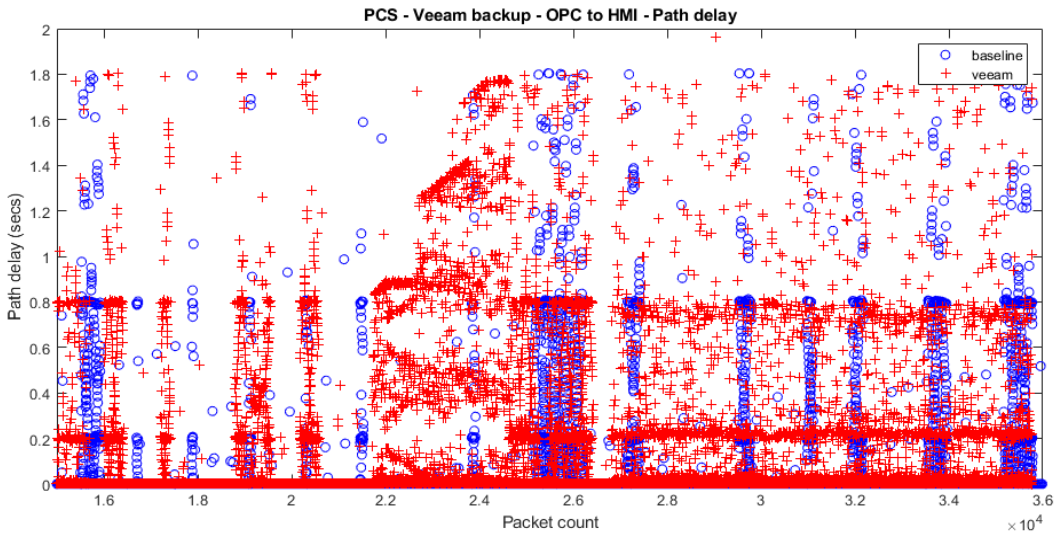


Figure 4-8 Plot of the path delay from OPC to HMI during Veeam full backup

Increment backup should be considered, the amount of network resources consumed was much lower compare with full backup. The round trip time from Controller to OPC during an incremental backup was increased only for a short amount of time.

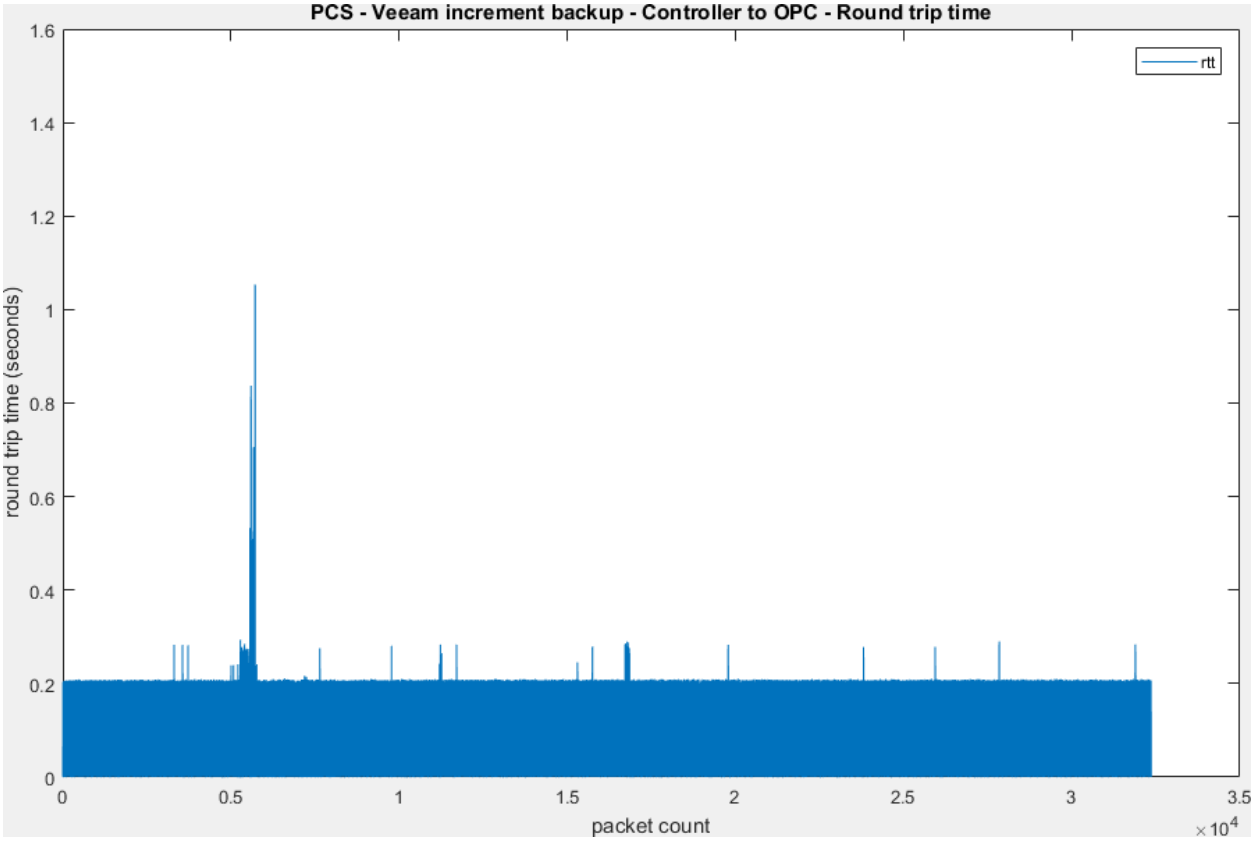
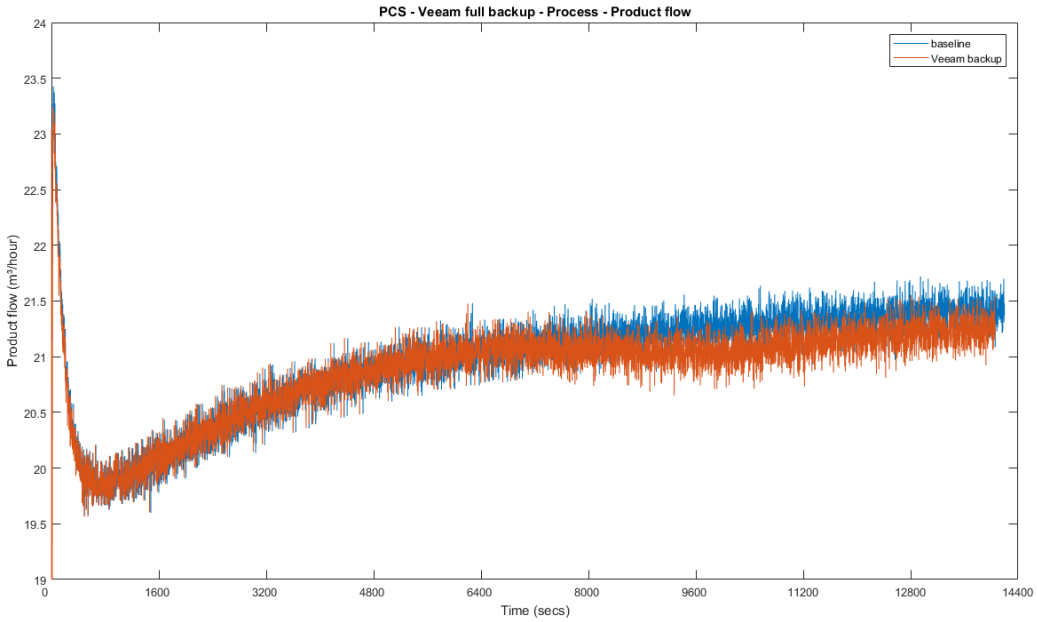


Figure 4-9 Plot of the packet round trip time from Controller to OPC during Veeam incremental backup

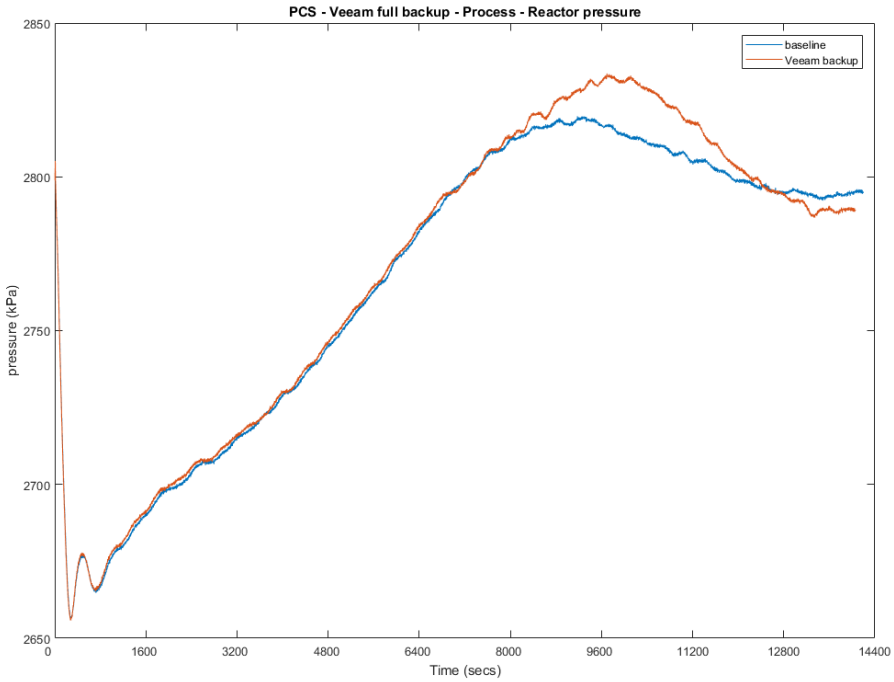
There was a small performance impact to the manufacturing process observed during the full backup. The product flow was slightly lower and the reactor pressure overshot their normal levels in the experiment.

It is hypothesized that the impacts were caused by increased network latency and traffic which caused a delay of the sensor and actuator information exchange between the Controller and the simulated plant. Therefore, a degrade performance of the control loop causing a slight impact to the performance of the system. The ability of the Veeam backup to throttle the rate of backup according to the network condition helped reduce the impact to the network traffic and latency during the full backup.



3185

3186 **Figure 4-10 Plot of the production flow of the manufacturing process during Veeam full backup**



3187

3188 **Figure 4-11 Plot of the reactor pressure of the manufacturing process during Veeam full backup**

3189

4.6.7 Link to Entire Performance Measurement Data Set

Veeam full backup KPI data

Veeam full backup measurement data

Veeam incremental backup KPI data

Veeam incremental backup measurement data

4.7 Security Onion

4.7.1 Technical Solution Overview

Security Onion is a free and open source Linux distribution for intrusion detection, enterprise security monitoring, and log management. It includes Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, OSSEC, Sguil, Squert, NetworkMiner, and many other security tools.[14] Security Onion combines three core functions:

- full packet capture;
- network-based and host-based intrusion detection systems (NIDS and HIDS, respectively);
- and powerful analysis tools

Points to consider:

- Open source software, available as an ISO distribution to deploy in any type of environment (physical or virtual).
- Collection of different open-source tools such as SNORT, BRO, OSSEC SGQUIL, KIBANA, ELSA etc. integrated into one product which otherwise would require lot of manual work to integrate.
- Support for standalone instance and distributed deployment for large organizations.
- Provides a front-end to Snort and BRO IDS which natively are command line-based tools.
- Fully customizable rule-set. Has inbuilt detection rules to detect a variety of cyber-attacks and anomalies for both IT and OT environments.
- Learning curve associated. Familiarity with SNORT and BRO IDS rule-set.
- Hardware Resource intensive.
- No reporting capabilities out of the box.

4.7.2 Technical Capabilities Provided by Solution

Security Onion provides components of the following Technical Capabilities described in Section 6 of Volume 1:

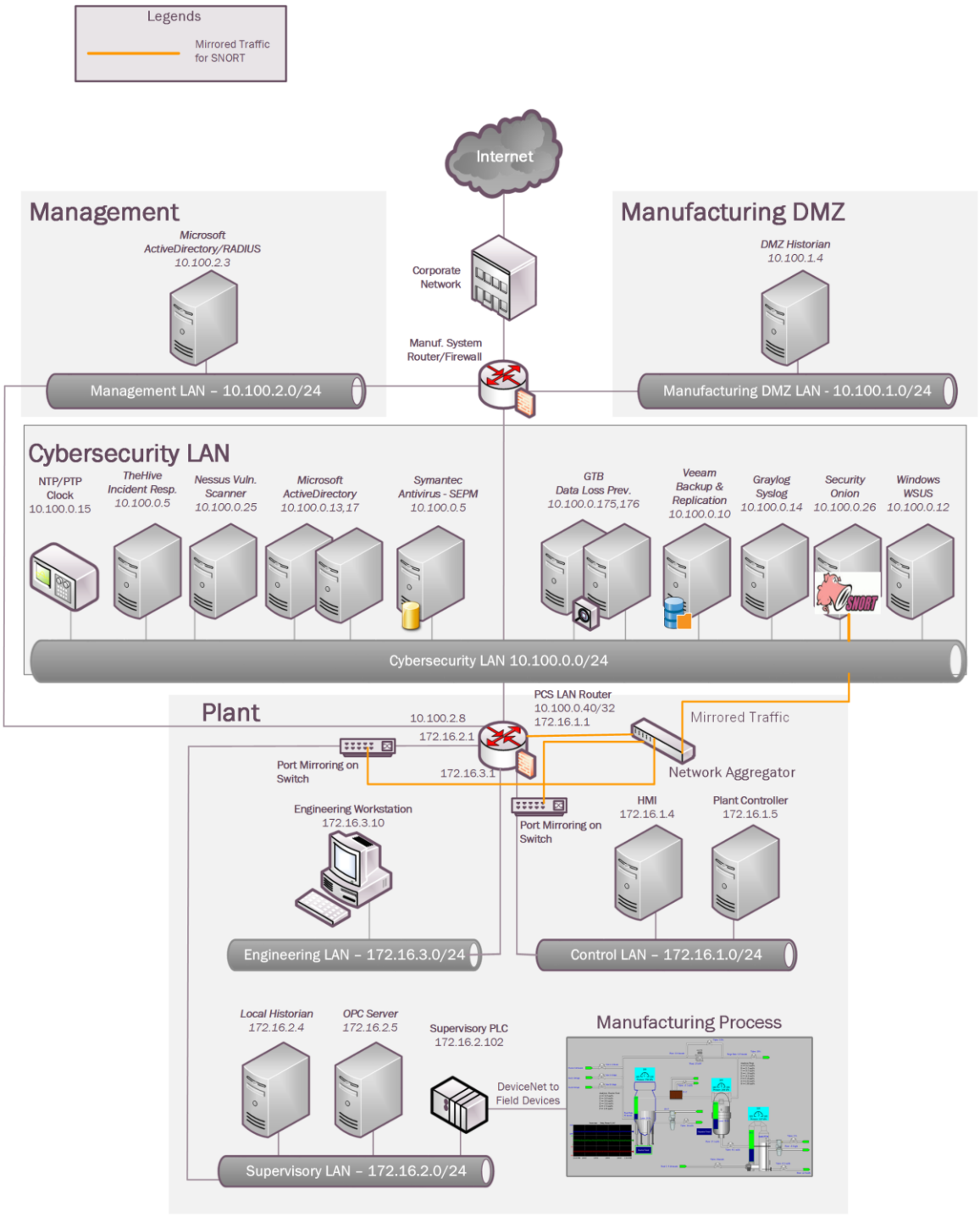
- Network Boundary Protection
- Network Monitoring
- Event Logging
- Forensics

[14] Security Onion: https://securityonion.net/

Subcategories Addressed by Implementing Solution

PR.DS-5, PR.PT-4, DE.AE-2, DE.CM-1, DE.CM-6, DE.CM-7

4.7.3 Architecture Map of Where Solution was Implemented



4.7.4 Installation Instructions and Configurations

Setup

- An ISO image of the Security Onion was downloaded from their website (https://securityonion.net/) and deployed on a Microsoft Hyper-V virtual host in the Cybersecurity LAN network. Ensure to assign appropriate hardware resources as recommended in the product documentation.[15]

Details of the solutions implemented:

Name	Version	Hardware details
Security Onion	16.04.5.2	Virtual Machine with 4 virtual cores, 20GB Memory, 400GB Disk

- Ours is a standalone single server deployment. For larger environments, Security Onion supports a distributed deployment mode consisting of multiple remote sensors. Detailed setup documentation is available on their wiki.[16]

- Security Onion requires 2 physical network connections as follows –

(i) **(eth0)** for management IP address
(ii) **(eth1**) for the monitoring interface. This interface needs to be configured in promiscuous mode to leverage the SNORT and BRO IDS components for monitoring network traffic.

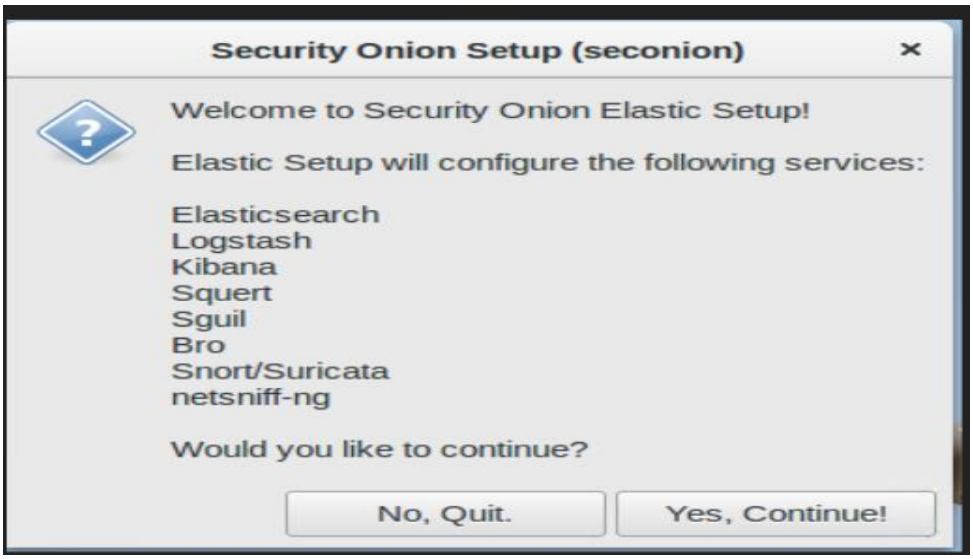
For (i) a virtual switch connection was provisioned from the Cybersecurity LAN and assigned to the Security Onion VM. This is for setting up an IP address to login to Security Onion interface or the server itself.

For (ii) Port Mirroring was configured on the two network switches and the Boundary Firewall. These mirrored port(s) were further connected to a Network Aggregator device.

The Network Aggregator device is used for aggregating traffic from these network devices of the Process Control System. An outbound connection from its Aggregated interface was made to the **monitoring interface (eth1)** of the Security Onion VM. Figure 1 below shows the setup of security onion in our environment.

[15] Security Onion Documentation: https://securityonion.readthedocs.io/en/latest/
[16] Security Onion WIKI: https://github.com/Security-Onion-Solutions/security-onion/wiki

- Once the two network connections are connected, power on the virtual machine and complete the default Linux OS setup as per the instructions on the screen. Upon a system reboot, login to the console locally and click on the **Setup** icon on the "**Desktop**" to configure the network interfaces. This step includes assigning a static IP address for management and setting up the monitoring port of the instance. Ensure to select the correct interfaces for each role. A Reboot is required upon completion.
- Reboot the system and click on the Setup icon again to complete the next phase of the setup. It will display the below message. Click **YES, Continue!** and then select **Evaluation Mode** in the next screen for standalone deployments.



- Follow the on-screen options and complete the wizard. A system reboot would again be required.
- Security Onion by default allows SSH only from localhost. To connect to it remotely, run the command "**sudo so-allow**" to configure the appropriate firewall rules for remote connectivity. Select "**a – analyst**" option and whitelist the IP address or ip-range of client-pc where you intend to access security onion interface from. Instructions to setup the firewall can be found here: https://github.com/Security-Onion-Solutions/security-onion/wiki/Firewall
- Upon completion of both setup phases, security onion should now be accessible using any of the 3 methods below:
- SQUERT Web Interface: This is the web interface to the backend Sguil database. The URL is https://IP address-of-security-onion/
- Kibana: Kibana is an open source data visualization plugin for Elasticsearch. It can be accessed via https://ip-address-of-security-onion/app/kibana
- Sguil client: A windows-based client is available for querying the Sguil database at https://bammv.github.io/sguil/index.html for installing on a remote workstation.
- The credentials to login to the above URLs should be the one that were created earlier during the setup process.

- Ensure to set the OS time-zone to UTC as Security Onion uses UTC by default. Changing time-zone can cause other issues.
- The command **sudo nsm_sensor_ps-status** can be used to check the status of each Security Onion component/service.

Configuring Updates:

- Register on SNORT.org for an account to be eligible for downloading the "Registered" Rule set. Upon registration, note down the OINK code tied to your account. Copy-paste the OINK code in the "rule_url" parameter in **/etc./nsm/pulledpork/pulledpork.conf** file of the server and save the changes.
  rule_url=https://www.snort.org/reg-rules/|snortrules-snapshot.tar.gz|**<oink-code>**

  Security Onion by default requires internet access to download Snort signatures. If your Security Onion server has internet access, uncomment and set "LOCAL_NIDS_RULE_TUNING=no" in **/etc./nsm/securityonion.conf** file. Run the "**sudo rule-update**" command to update the rule set. This will download new rules from Snort.org and save them in **/etc./nsm/rules/downloaded.rules** file.

- For Air-Gapped environments (w/o Internet), set LOCAL_NIDS_RULE_TUNING=yes in the securityonion.conf file and the snort updates would have to be manually downloaded on a different system and transferred via USB device or network to **/tmp** folder on the Security Onion server. Once done run the **sudo rule-update** command.

SNORT IDS Setup:

- Define the network variables such as $HOME_NET, $EXTERNAL_NET etc. as per your environment in the snort configuration file (snort.conf) located at **/etc./nsm/<hostname-MonitorInterface>/**. Once done, the snort service should be restarted by running the command**:**
  sudo nsm_sensor_ps-restart --only-snort

  Below is a snippet of the **snort.conf** in our instance

```
###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
ipvar HOME_NET [192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]

ipvar NETWORK_DEVICES [172.16.1.3,172.16.3.1,172.16.2.2,192.168.0.239,192.168.0.2,192.168.1.2]
ipvar ICS_DEVICES [172.16.2.102,172.16.4.102,192.168.0.30,192.168.0.60]
ipvar PCS_ICS_DEVICES [172.16.2.100/30]
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS [10.100.0.17]

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET
```

- The Snort module uses the downloaded.rules under **/etc./nsm/rules/ directory** for its IDS rule set in addition to any local rules defined under **/etc./nsm/rules/local.rules** file. All custom rules should be defined under this l**ocal.rules** file. Upon adding a custom rule, the snort rule set must be updated using this command: **sudo rule-update**

  This command will also result in local rules getting merged into downloaded.rules file. Additionally, you can manually verify the same by running **tail -n 100 downloaded.rules**. If the defined local rules do not appear in the downloaded.rules file; the **/etc./nsm/<interface>/snortu-1.log** file must be reviewed for any syntax errors.

  Below are some of the rules we setup to detect common IT and ICS-specific anomalies.

```
# Detect NMAP scan, ICMP attack , TCP-SYN Flood attack
alert UDP any any -> $PCS_ICS_DEVICES any (msg: "Nmap UDP Scan"; sid:10000002; rev:1;)
alert icmp any any -> $HOME_NET any (msg: "NMAP ping sweep Scan"; dsize:0; sid:10000004;
rev:1;)
alert icmp any any -> $HOME_NET any (msg: "Ping Large ICMP Packet"; dsize:>800; classtype:bad-
unknown; sid:10000030; rev:1;)
alert tcp any any -> $HOME_NET [80,22,443] (msg: "TCP SYN flood attack detected"; flow: stateless;
flags:S,12; detection_filter:track by_dst, count 100, seconds 10; classtype: attempted-recon;
sid:10000005; rev:1;)
```

```
# Detect FTP Attempt to Public IP-address & other FTP events
alert tcp $HOME_NET any -> $EXTERNAL_NET 21 (msg: "FTP attempt to Public IP"; sid:10000003;
rev:1;)
alert tcp $HOME_NET any -> any 21 (msg: "FTP upload attempt"; content: "|53 54 4f 52|";
sid:10000020; rev:1;)
alert tcp  any 21 -> $HOME_NET any (msg: "FTP file successfully uploaded"; content: "|54 72 61 6e 73
66 65 72 20 63 6f 6d 70 6c 65 74 65|"; sid:10000027; rev:1;)
alert tcp  any 21 -> $HOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf";
sid:10000031; rev:1;)

# Detect Credit card number in cleartext
alert tcp any any <> any any (pcre:"/5\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}/"; msg: "MasterCard
number detected in clear text"; content:"number"; nocase; sid:10000013; rev:1;)
alert tcp any any <> any any (pcre:"/3\d{3}(\s|-)?\d{6}(\s|-)?\d{5}/"; msg: "American Express number
detected in clear text"; content:"number";nocase; sid:10000014; rev:1;)
alert tcp any any <> any any (pcre:"/4\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}/"; msg: "Visa number
detected in clear text"; content:"number";nocase; sid:10000015; rev:1;)

# Telnet activity monitoring
alert tcp $TELNET_SERVERS 23 ->  $HOME_NET any (msg: "Telnet Password in Clear text"; content:
"Password"; sid:10000010;rev:1;)
alert tcp $HOME_NET any -> $TELNET_SERVERS 23 (msg: "TELNET login attempt";
classtype:default-login-attempt; sid:10000007; rev:1;)
alert tcp $HOME_NET any ->  $TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default
Password"; content: "|73 77 69 74 63 68|"; sid:10000008;rev:1;)
alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Login
failed"; fast_pattern:only; nocase; classtype:bad-unknown; sid:10000038; rev:
```

3343 Snort Rules for ICS/ SCADA[17]

3344

```
#ICS-SCADA specific rules [4]
alert tcp $HOME_NET any -> $ICS_DEVICES 44818 (msg: "PROTOCOL-SCADA Rockwell firmware
change attempt"; flow:to_server,established; content:"|6F 00|"; content:"|00 00 00 00|"; within:4; distance:6;
content:"|00 00 00 00|"; within:4; distance:8; pcre:"/(\x20\xa1|\x21\x00\xa1\x00)(\x24[\x01-
\xff]|\x25\x00[\x01-\xff]\x00)/smi"; reference:cve,2012-6437;
reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=27868; classtype:policy-violation;
sid:10000019; rev:1;)
alert tcp $HOME_NET any ->  $ICS_DEVICES $HTTP_PORTS (msg: "ICS-SCADA PLC Web access
attempted "; sid:10000033; rev:1;)
alert tcp any any -> $HOME_NET 22350 (msg: "PROTOCOL-SCADA TwinCAT PLC DOS attempt";
flow:to_server,established; dsize:>2000; content:"|A2 1D CB AA AA 75 48 B4 91 DB F4 06 B0 B0 2D|";
fast_pattern:only; metadata:policy max-detect-ips drop, policy security-ips drop;
reference:url,www.beckhoff.com/english.asp?twincat/overvw.htm; classtype:attempted-dos; sid:41743;
rev:2;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus user-defined function code
- 65 to 72"; flow:to_server,established; byte_test:1,>,64,7; byte_test:1,<,73,7;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:15074; rev:5;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus user-defined function code
- 100 to 110"; flow:to_server,established; byte_test:1,>,99,7; byte_test:1,<,111,7;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:15075; rev:5;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus read multiple coils - too
many inputs"; flow:to_server, established; modbus_func:read_coils; byte_test:2,>,2000,10;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:15077; rev:6;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus write multiple registers
from external source"; flow:to_server,established; modbus_func:write_multiple_registers;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:17782; rev:4;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus write single coil from
external source"; flow:to_server,established; modbus_func:write_single_coil;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:17784; rev:4;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus write multiple coils from
external source"; flow:to_server,established; modbus_func:write_multiple_coils;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:17785; rev:4;)
```

3345

[17] Snort Rules for ICS/ SCADA: https://github.com/ITI/ICS-Security-Tools/blob/master/configurations/rules/talos-snort.rules

```
# Accessing switch via Web URL & use of default password
alert tcp  any ->  $NETWORK_DEVICES 80 (msg: " WEBAPP Netgear Default Password";
flow:established,to_server; content:"POST"; nocase; http_method;
uricontent:"/base/cheetah_login.html"; content:"password"; nocase; sid:1000009; rev:1;)
alert tcp $HOME_NET any -> $NETWORK_DEVICES $HTTP_PORTS (msg: "WEBAPP Rockwell
Automation default password login attempt"; flow:to_server,established; content:"Authorization|3A|";
nocase; http_header; content:"YWRtaW5pc3RyYXRvcjptbDE0MDA="; fast_pattern:only; http_header;
metadata:service http; classtype:default-login-attempt; sid:10000011; rev:1;)

# SSH Activity monitoring
alert tcp any any -> $EXTERNAL_NET 22 (msg: "SSH Attempt to Public Host"; sid:10000018; rev:1;)
alert tcp any any -> $HOME_NET 22 (msg: "Potential SSH Brute Force Attack"; flow:to_server,
established; flags:S+; detection_filter:track by_src, count 30 , seconds 10; classtype:attempted-dos;
priority:1; sid:10000006; rev:1;)

# DNS traffic to social media websites
alert udp $HOME_NET any -> $DNS_SERVERS 53 (msg: "DNS Request to Twitter.com Detected";
content: "|6e 69 73 74|"; sid:10000016; rev:1;)
alert udp $HOME_NET any -> $DNS_SERVERS 53 (msg: "DNS Request to Facebook.com Detected";
content: "|66 61 63 65 62 6f 6f 6b|"; sid:10000017; rev:1;)

# File upload activity to a public web server
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "WEB-PHP file upload
attempt"; flow:to_server, established; uricontent:"/upload.php"; nocase; content:"filename=";
reference:bugtraq,3361; reference:cve,2001-1032; classtype:attempted-admin; sid:10000029; rev:1;)
alert tcp $Robotics_devices any -> $EXTERNAL_NET $HTTP_PORTS (msg: "Web Access to Public
IP attempted"; sid:10000039; rev:1;)
```

Tuning Security Onion:

- The default database retention period for Sguil database is 30 days. This can be changed by editing the **DAYSTOKEEP** parameter in the **/etc./nsm/securityonion.conf** file.
- A number of rules defined in the **downloaded.rules** file are commented out by default. This is intentional to reduce the volume of alerts and leaving the onus on the end user to customize it depending on the environment. To use any of the commented-out rules from downloaded.rules file, note down the Generator ID (GID) and Signature ID (SID) value defined in the rule that's commented out and list them in **/etc./nsm/pulledpork/enablesid.conf** file**.** Avoid directly uncommenting them**.** This will enable that rule and will be persistent next time when the **downloaded.rules** gets updated.
- Likewise, to silence any false alerts note down the Generator ID (GID) and Signature ID (SID) value of the rule that is generating the alert and define them in the **/etc./nsm/pulledpork/disablesid.conf** file. Detailed instructions are available on the Snort documentation [5] under "Managing alerts".
- Shown below is a snippet from our **disablesid.conf** file showing the SIDs we have disabled.

```
# example disablesid.conf V3.1

# Example of modifying state for individual rules
# 1:1034,1:9837,1:1270,1:3390,1:710,1:1249,3:13010
3:19187
119:19 # http_inspect: LONG HEADER
123:8 # frag3: Fragmentation overlap
128:4 # ssh: Protocol mismatch
129:4 # stream5: TCP Timestamp is outside of PAWS window
129:5 # stream5: Bad segment, overlap adjusted size less than/equal 0
129:7 # stream5: Limit on number of overlapping TCP packets reached
129:12 # stream5: TCP Small Segment Threshold Exceeded
```

- PCAPS can fill up the storage space on server. Follow the instructions on the wiki to manage the pcap files.

BRO IDS Setup:

- Security Onion also uses BRO IDS alongside SNORT for network monitoring. The BRO logs are stored in **/nsm/bro/logs** directory. Similar to local.rules in SNORT, any custom scripts for BRO must be placed in **/opt/bro/share/bro/policy/** directory. Please refer to the security onion wiki [3] for additional reference on BRO.
- To leverage BRO capabilities for Windows SMB File share monitoring, add the below line at the end of **/opt/bro/share/bro/site/local.bro** file

  `@load policy/protocols/smb`

  Once done restart BRO using the command: `sudo nsm_sensor_ps-restart --only-bro`

OSSEC Setup:

- OSSEC server (now replaced with **Wazuh**) comes along with Security Onion. Ossec is a Host Intrusion Detection System (HIDS). The OSSEC server module is installed and running by default in the Security Onion server. OSSEC alerts can be viewed either from Kibana or Squert web interface.
- To configure additional client systems for monitoring using OSSEC, download the agent installer from OSSEC website (http://www.ossec.net/) specific to your Operating System, copy over the agent to the client system and run the setup process using the instructions mentioned on the Ossec website. During the install, mention the IP address of Security Onion server as the IP address of Ossec server. Ensure to open firewall ports on Security Onion server to receive data from Ossec clients.

- It is beyond the scope of this document to explain detailed working of the OSSEC product. The Ossec official website and other documentation links under References can be a useful source.
  Similar to Snort and Bro, any custom OSSEC rules for monitoring should be added in **local_rules.xml** file under **/var/ossec/rules** directory. If a decoder is required to parse custom logs, it should be defined under in **local_decoder.xml** file under **/var/ossec/etc.** directory.
- On Windows systems, OSSEC agents can be configured to monitor Event Viewer logs, Rootkit Detection, File Integrity Monitoring (FIM), Registry changes and any other custom application logs. Instructions are available on OSSEC website.
- Similarly, on Linux systems, OSSEC can perform File Integrity Monitoring, Process Monitoring, Rootkit changes and any other host intrusion attempts such as failed SSH logins.
- Ossec agent was installed on the **Engineering workstation** in Process Control System to detect following anomalies:
  - USB Drive detection [5].
  - Allen Bradley Factory Talk Administration Console login failures.
  - Monitoring Unauthorized Assets.

USB Drive Detection:

- The following lines were added to the local **ossec.conf** file on the Agent side (Engineering Workstation) where an USB drive would be monitored for

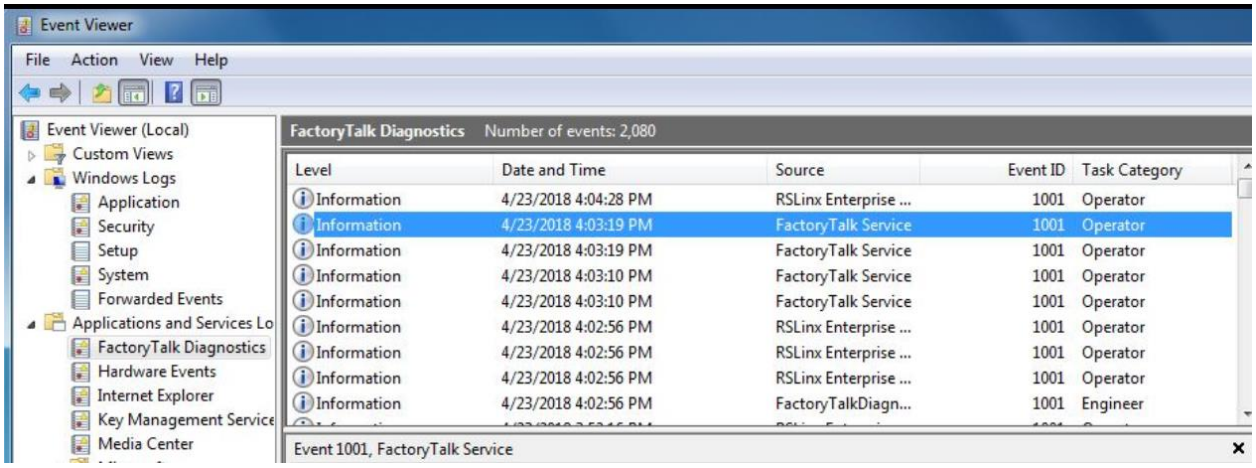
```
<agent_config os="Windows">
 <localfile>
  <log_format>full_command</log_format>
       <command>reg QUERY
       HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR</command>
  <alias>usb-check</alias>
 </localfile>
</agent_config>
```

- Next, the following lines were added to the **/var/ossec/rules /local_rules.xml** file on the Security Onion server to generate an alert

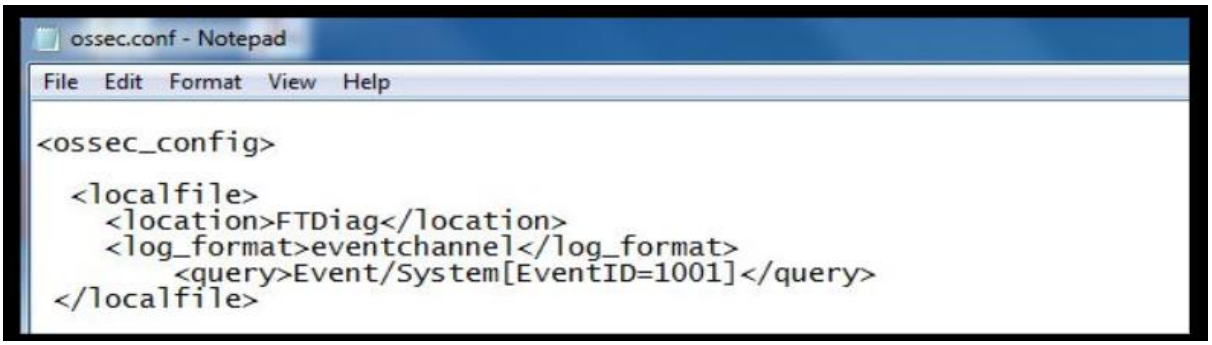
```
<rule id="140125" level="7">
  <if_sid>530</if_sid>
  <match>ossec: output: 'usb-check':</match>
  <check_diff />
  <description>New USB device connected</description>
</rule>
```

Detecting Allen Bradley-Factory Talk Login failures:

- The Factory Talk Administration Console (installed on the Engineering Workstation) logs all authentication attempts and other diagnostic events under Windows Event Viewer as shown below.



- To alert on login failures from Factory Talk Admin console, the below config was placed in the local **ossec.conf** file of the windows workstation. This line tells Ossec to look for event ID 1001 under "**Factory Talk Diagnostics**" category also referenced as "**FTDiag**" in Event Viewer and forward those events to Ossec server.



- Next on the Ossec server, the following lines were added in **local_rules.xml** file to generate an alert.

```
<group name="syslog,">
<rule id="110001" level="0">
  <if_sid>18104</if_sid>
   <match>FactoryTalkDiagnostics</match>
  <description>FactoryTalk Audit Event</description>
 </rule>
 <rule id="110002" level="7">
  <if_sid>110001</if_sid>
  <match>failure</match>
  <description>FactoryTalk Administration Console login failure</description>
 </rule>
```

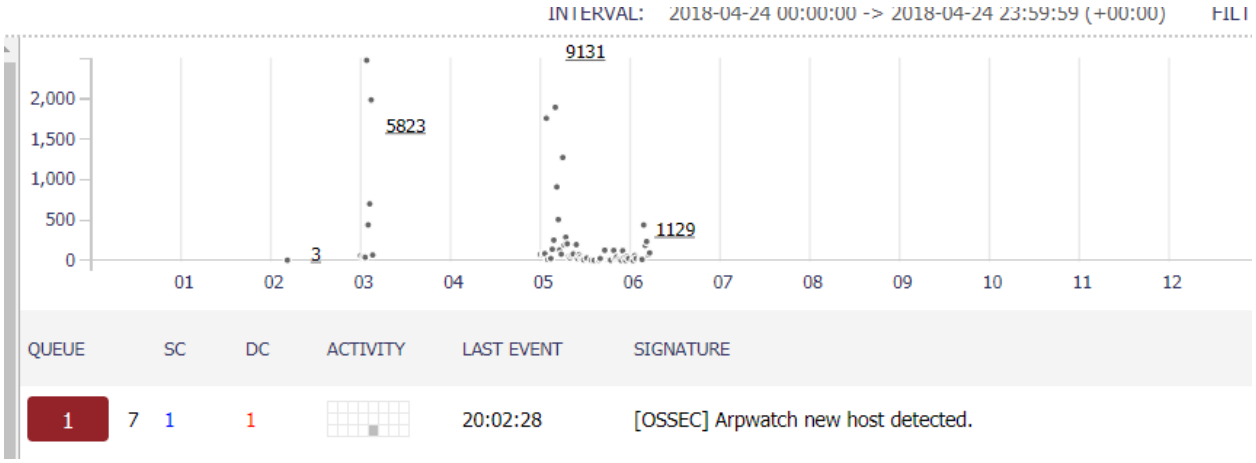
Monitoring for Unauthorized assets:

- Rogue/Unauthorized Asset discovery can be implemented using **Arpwatch** and Ossec. To configure this, install the "arpwatch" package on the Security Onion server. Arpwatch package is available in all Linux distributions. Upon installation start the arpwatch service and configure it to listen to the network interfaces using the `arpwatch -i <interface>` command.

  For instance: `arpwatch -i eth1` where eth1 is monitoring port.
- The Security Onion server already has an inbuilt decoder and a rules file for **arpwatch** located at **/var/ossec/etc./arpwatch_decoder.xml** and **/var/ossec/rules/arpwatch_rules.xml.** A new rule was added to our **local_rules.xml** file as shown below which references this inbuilt decoder and alerts when a new/bogon device is plugged into our network.

```
<rule id="110003" level="7">
  <if_sid>7200</if_sid>
  <match>new|logon</match>
  <description>Arpwatch new host detected. </description>
  <group>new_host,</group>
 </rule>
```

- Once done, restart the OSSEC server upon adding any local rules.
- The below image shows a sample alert in Squert Web Interface, when a new system was physically connected to the network:



Note: This package relies on ARP cache of the local system to detect new devices. It is possible for an intruder to spoof this system's mac-address or poison arp-cache and remain un-noticed.

Lessons Learned:

- The full packet capture feature in Security Onion can fill up the hard disk space quickly depending on the amount of network traffic in your environment. Ensure to plan and allocate substantial amount of storage for the server along with configuring the necessary data retention options in securityonion.conf file. Trimming your pcaps can allow you to store pcap for longer periods of time. For an example, please see https://www.netresec.com/?page=Blog&month=2017-12&post=Don%27t-Delete-PCAP-Files---Trim-Them

4.7.5 Highlighted Performance Impacts

No performance measurement experiments were performed for the use of Security Onion due to its installation location and how it was used (i.e., the software performed passive analysis of network traffic external to the manufacturing system).

4.7.6 Link to Entire Performance Measurement Data Set

N/A

4.8 Cisco AnyConnect VPN

4.8.1 Technical Solution Overview

The AnyConnect Secure Mobility Client is a modular endpoint software product by Cisco. It not only provides VPN access through Secure Sockets Layer (SSL) and IPsec IKEv2 but also offers enhanced security through various built-in modules. These modules provide services such as compliance through the VPN with ASA or through wired, wireless, and VPN with Cisco Identity Services Engine (ISE), web security alongside Cisco Cloud Web Security, network visibility into endpoint flows within Stealth watch, or off-network roaming protection with Cisco Umbrella. AnyConnect clients are available across a broad set of platforms, including Windows, macOS, Linux, iOS, Android, Windows Phone/Mobile, BlackBerry, and ChromeOS.[18]

Points to consider

- Provides additional security in the form of Web Security and DNS-Based security.
- OS Platform independent: The VPN clients are supported on Windows, Mac and Linux.
- Administrators can control which networks or resources for endpoints to connect. It provides an IEEE 802.1X supplicant that can be provisioned as part of authentication, authorization, and accounting (AAA) capabilities along with some unique encryption technologies such as MACsec IEEE 802.1AE.
- Cisco Proprietary Product. This replaces the earlier free product called AnyConnect VPN client. You must either have a Cisco Adaptive Security appliance(ASA) Firewall or Cisco Firepower Services Appliance and an active AnyConnect Secure Mobility Client license.

4.8.2 Technical Capabilities Provided by Solution

Cisco AnyConnect VPN provides components of the following Technical Capabilities described in Section 6 of Volume 1:

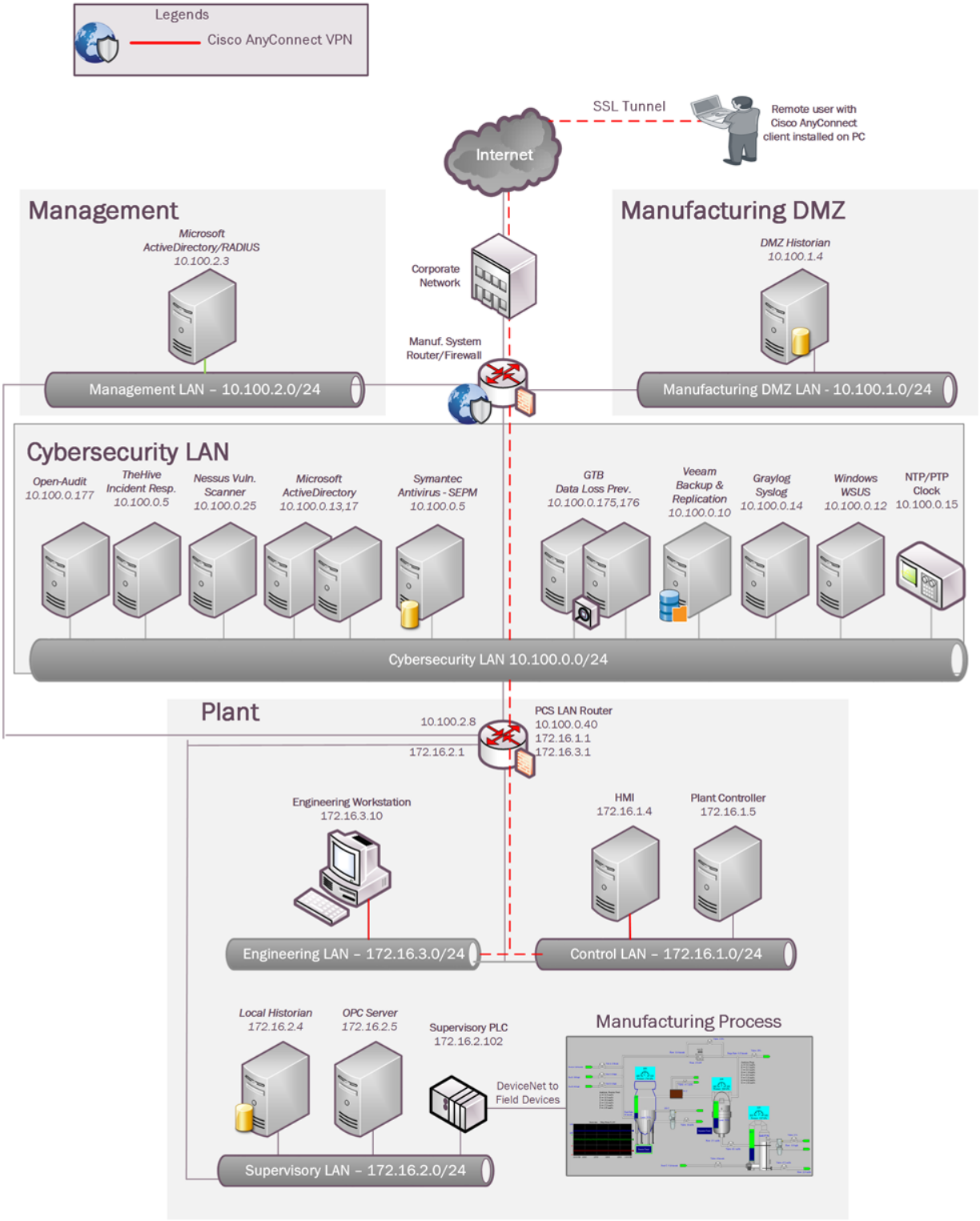
- Secure Remote Access
- Data Replication

4.8.3 Subcategories Addressed by Implementing Solution

PR.MA-2

[18] Cisco AnyConnect VPN https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-secure-mobility-client/at_a_glance_c45-578609.pdf

4.8.4 Architecture Map of Where Solution was Implemented



4.8.5 Installation Instructions and Configurations

Secure Remote Access was implemented for PCS system using the Cisco AnyConnect VPN. The AnyConnect VPN was configured on the top-level firewall - Cisco ASA in the Cybersecurity LAN network.

Overview

The following devices are involved in this setup

Device	Function	OS / Version
Cisco ASA 5512 with Firepower services	Firewall	FTD 6.2.3
AnyConnect VPN	VPN Client software	4.7.01076
A Server in the Management LAN	Active Directory, Radius	Windows 2012 R2

Setup of Radius server

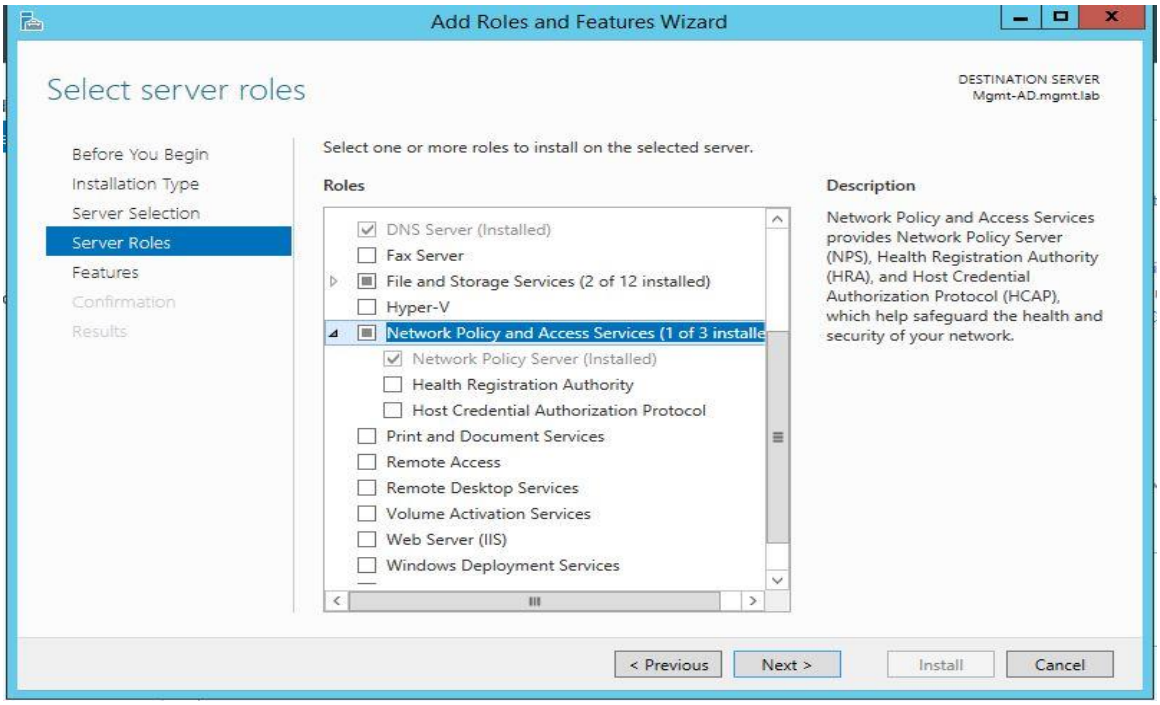
A Windows server was setup in the Management LAN for hosting Active Directory and Radius Authentication services for VPN clients.

Configuration Steps:

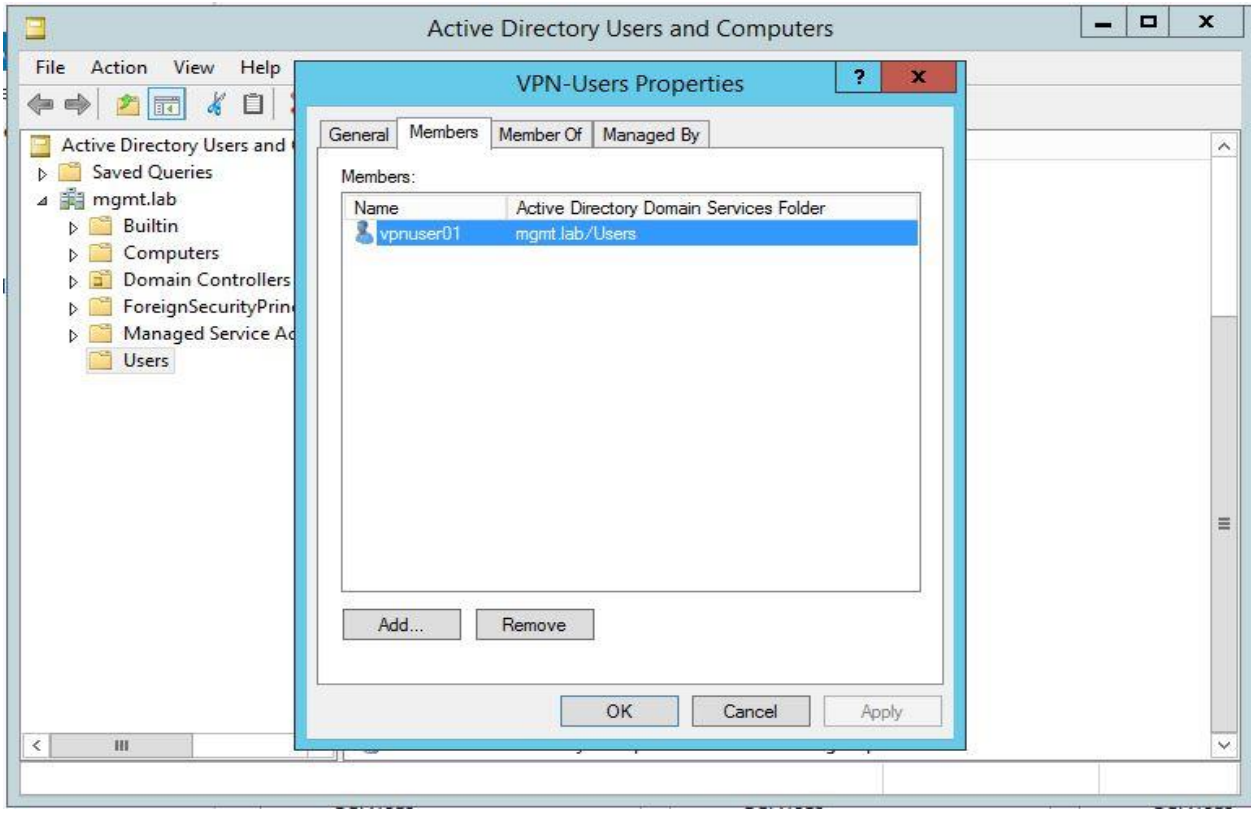
Install the following roles on the server. Different servers can be used to separate out the Roles and for redundancy.

- Active Directory Services
- DNS Server
- Network Policy Server

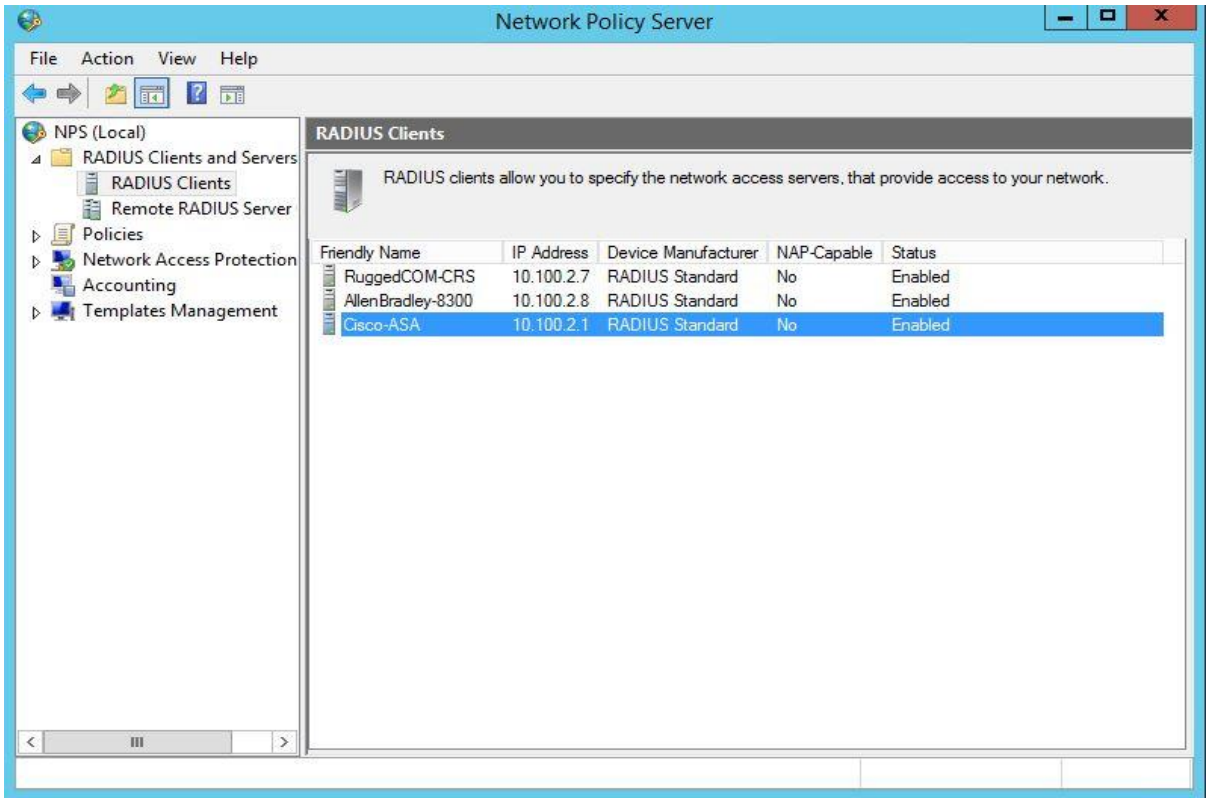
- All the above 3 roles can be installed using Windows Server Manager >> Add Roles and Features wizard. Below image shows the role to be installed for Network Policy server



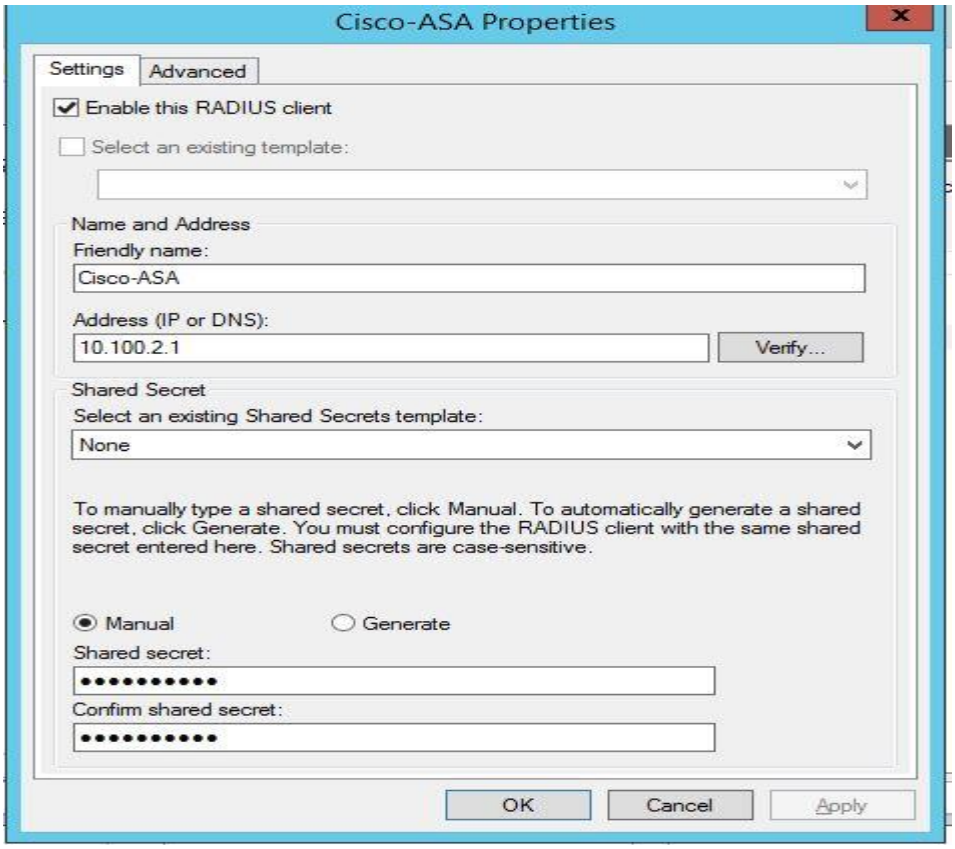
- Create a security group in Active Directory for VPN users and add those users to this group requiring VPN Access. A group called **VPN-users** was created in our AD server and a user **vpnuser01** was added to this group.



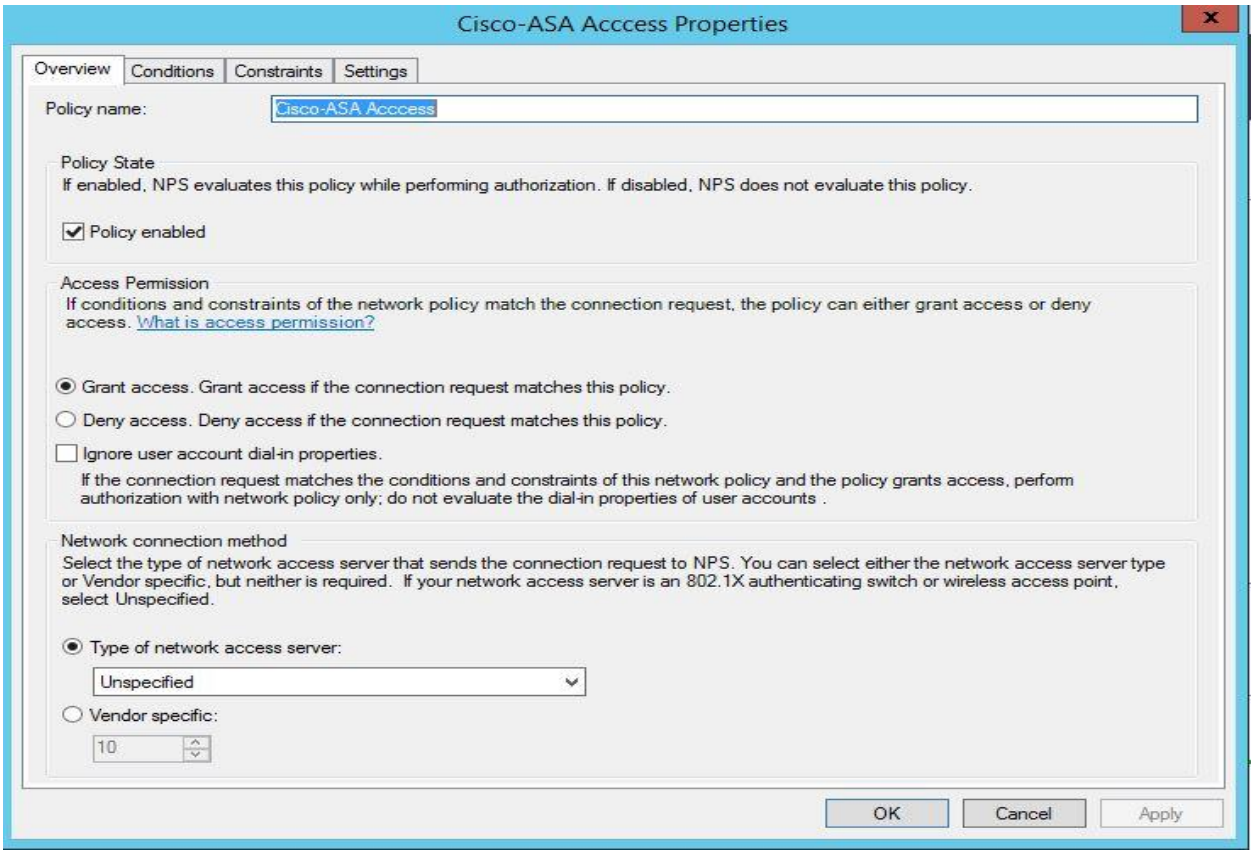
- Open up the "**Network Policy Server**" console, click on **Radius Clients** and create a client for your firewall device. Below image shows a Radius client created for our Cisco-ASA firewall.



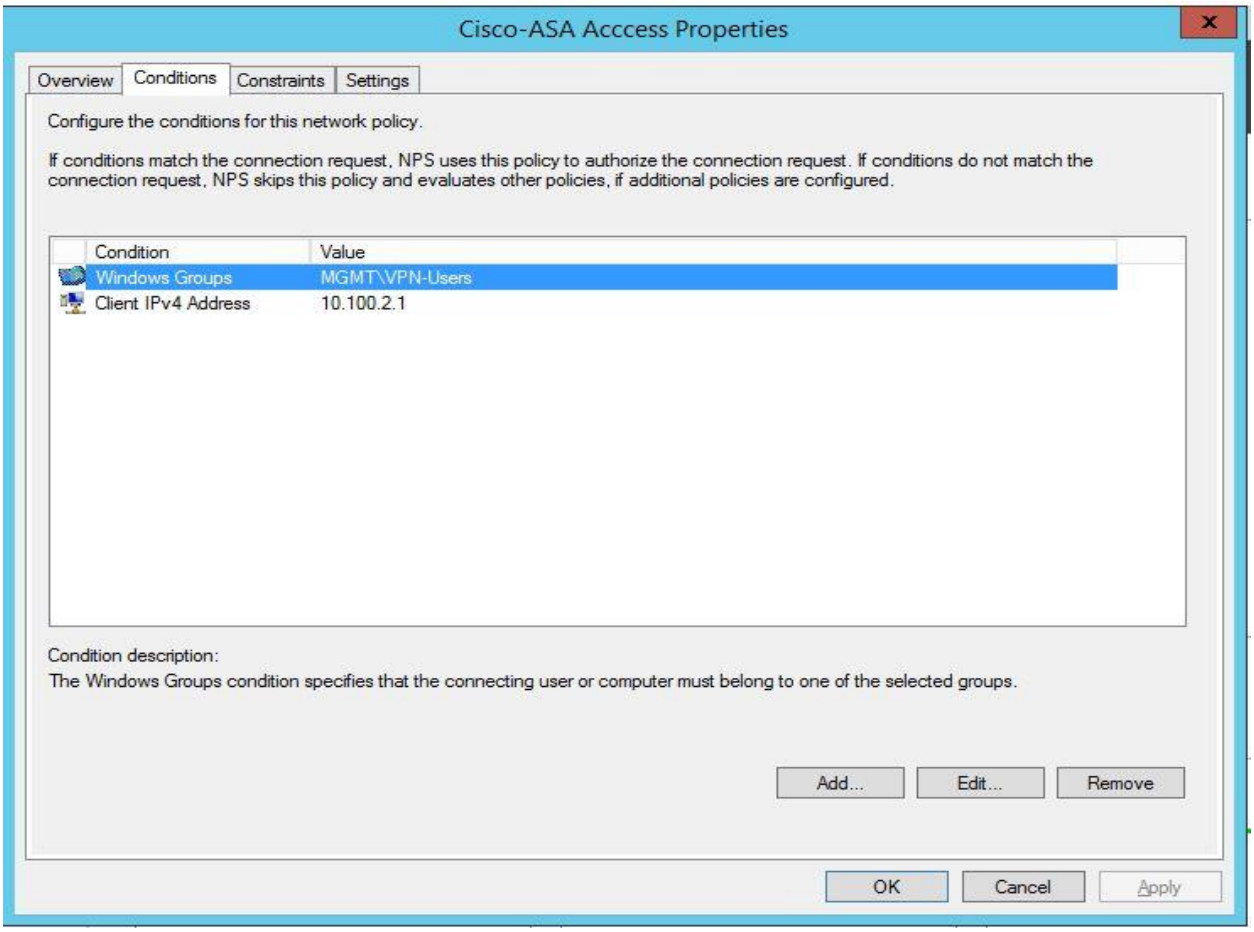
- While creating the Client, enter the IP address of the Interface on the ASA. This is typically the Default Gateway of the subnet where the AD/Radius server is in. Enter a strong password for Shared secret. This secret will later be used during the setup of a AAA group on the Firewall.
  Hit **OK** when done.


Cisco-ASA Properties
Settings
Advanced
Enable this RADIUS client
Select an existing template:
Name and Address
Friendly name:
Cisco-ASA
Address (IP or DNS):
10.100.2.1
Verify...
Shared Secret
Select an existing Shared Secrets template:
None
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
Manual
Generate
Shared secret:
Confirm shared secret:
OK
Cancel
Apply

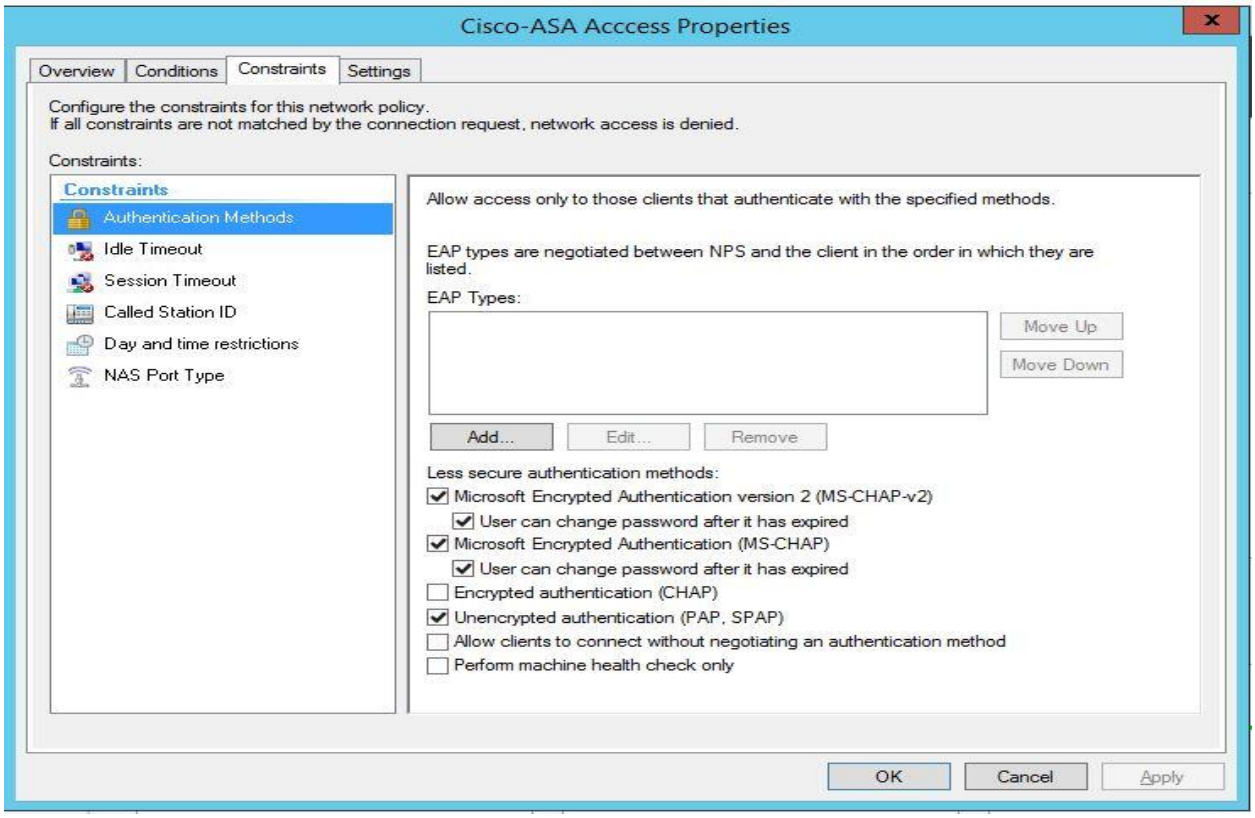
- Under **Policies** >> Click on **Network Policies**. Create a Network Policy here corresponding to the Radius client setup earlier. Below image shows network policy created for the Cisco-ASA client. Ensure the policy is enabled.



- Under **Conditions** tab, click **ADD** to add the following two conditions. More conditions can be added as per your requirement.
  - **VPN-Users** security group created earlier.
  - **Client IPv4 Address:** IP address of the Radius client created earlier.

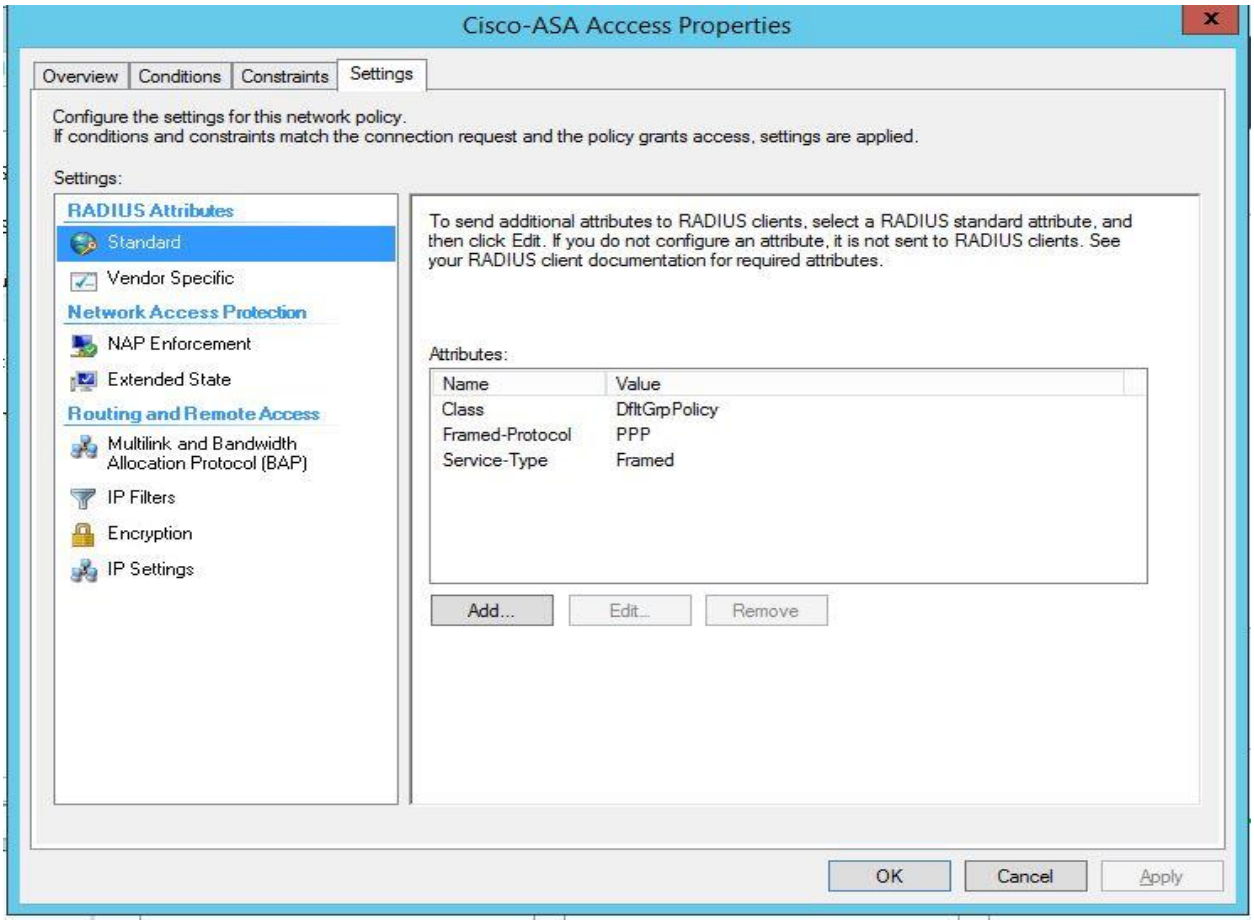


- Under **Authentication Methods**, select the methods shown below. This is as per Cisco documentation.[19]



[19] Cisco ASA VPN User Authentication: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/117641-config-asa-00.html

- Under **Settings >> Radius Attributes >> Standard** set the following attributes
  - Framed Protocol= **PPP**
  - Service-Type=**Framed**
  - Class = <**Name of group policy**>. This policy is configured in the Firewall for VPN



VPN Setup on Cisco-ASA firewall

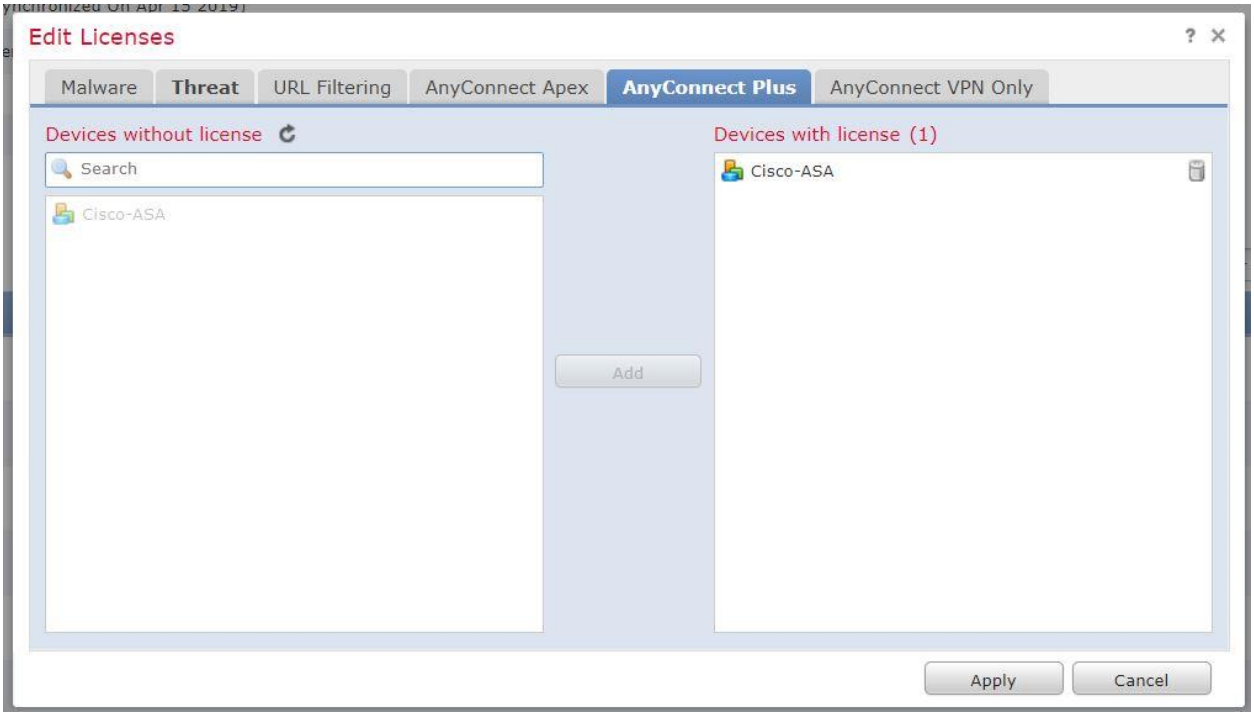
Below are the high-level steps for configuring Remote Access VPN in the FMC (Firepower Management Console)

- Go to **Licenses** >> **Smart Licenses** >> Verify if either **AnyConnect Plus** or **AnyConnect VPN** license has been enabled (if not already).

To enable license (assuming an AnyConnect license has been procured and tied to your Cisco smart account), Click **Edit Licenses** >> Select the corresponding firewall device from the left side window "**Devices without license**" and move it to the right side under "**Devices with license**". Hit **Apply**.

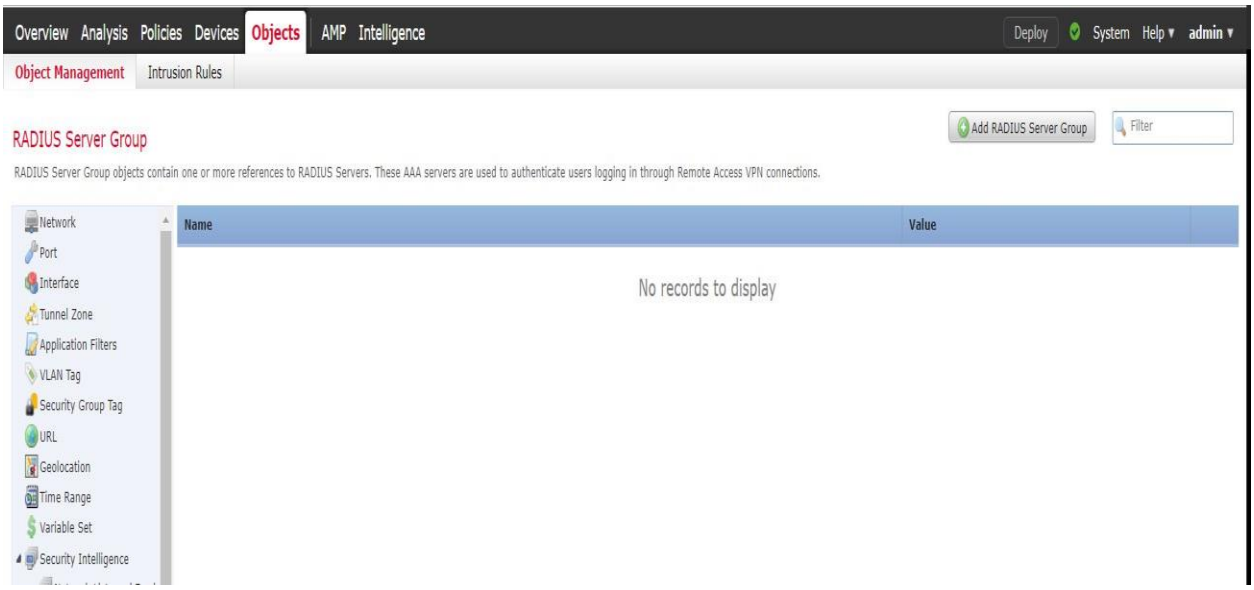
3627

3628



3629

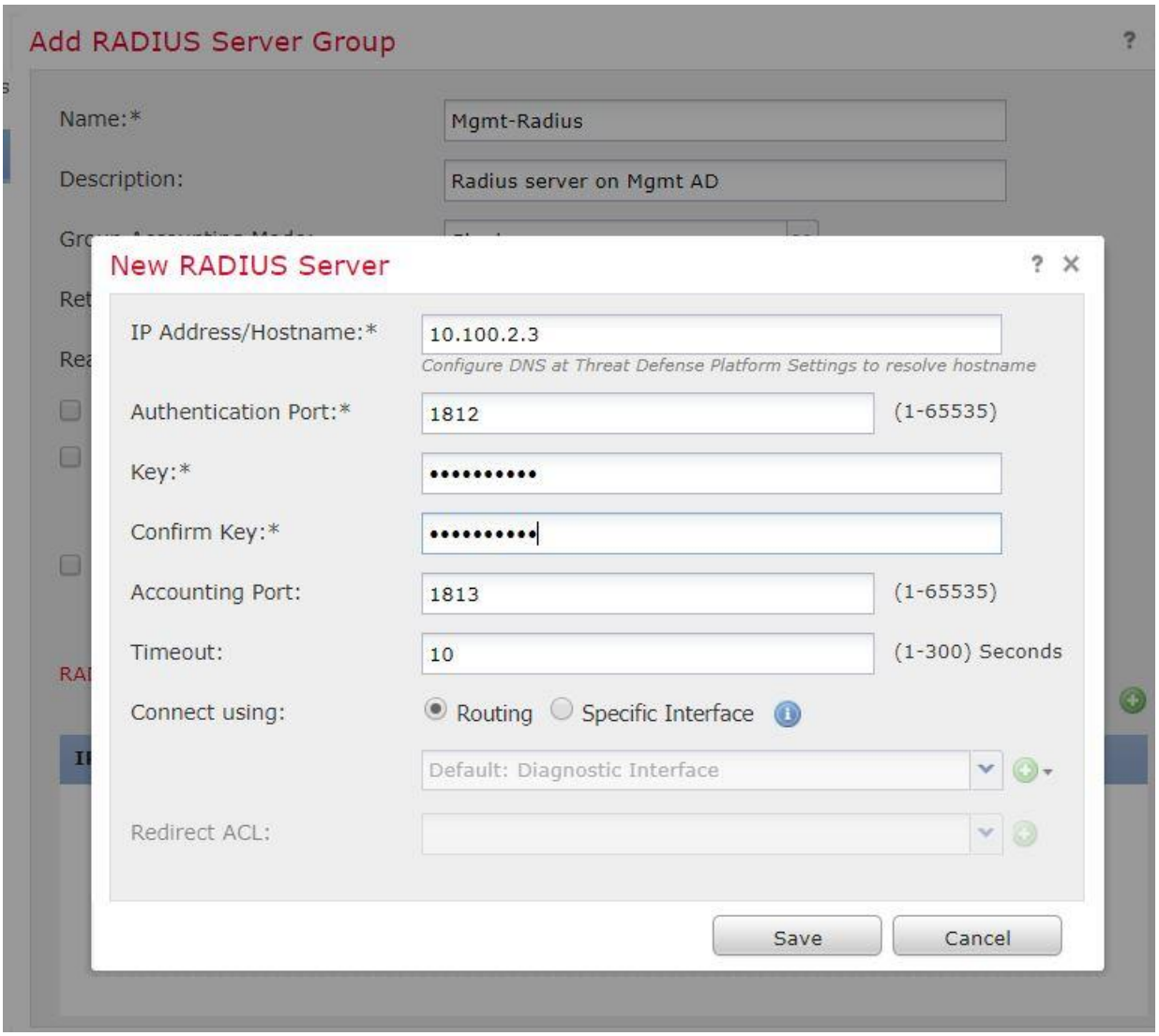
3630 • Go to **Objects menu** >> **Object Management** >> **Radius Server Group** >> **Add Radius**
3631 **Server Group** (if not already configured)



3632

3633

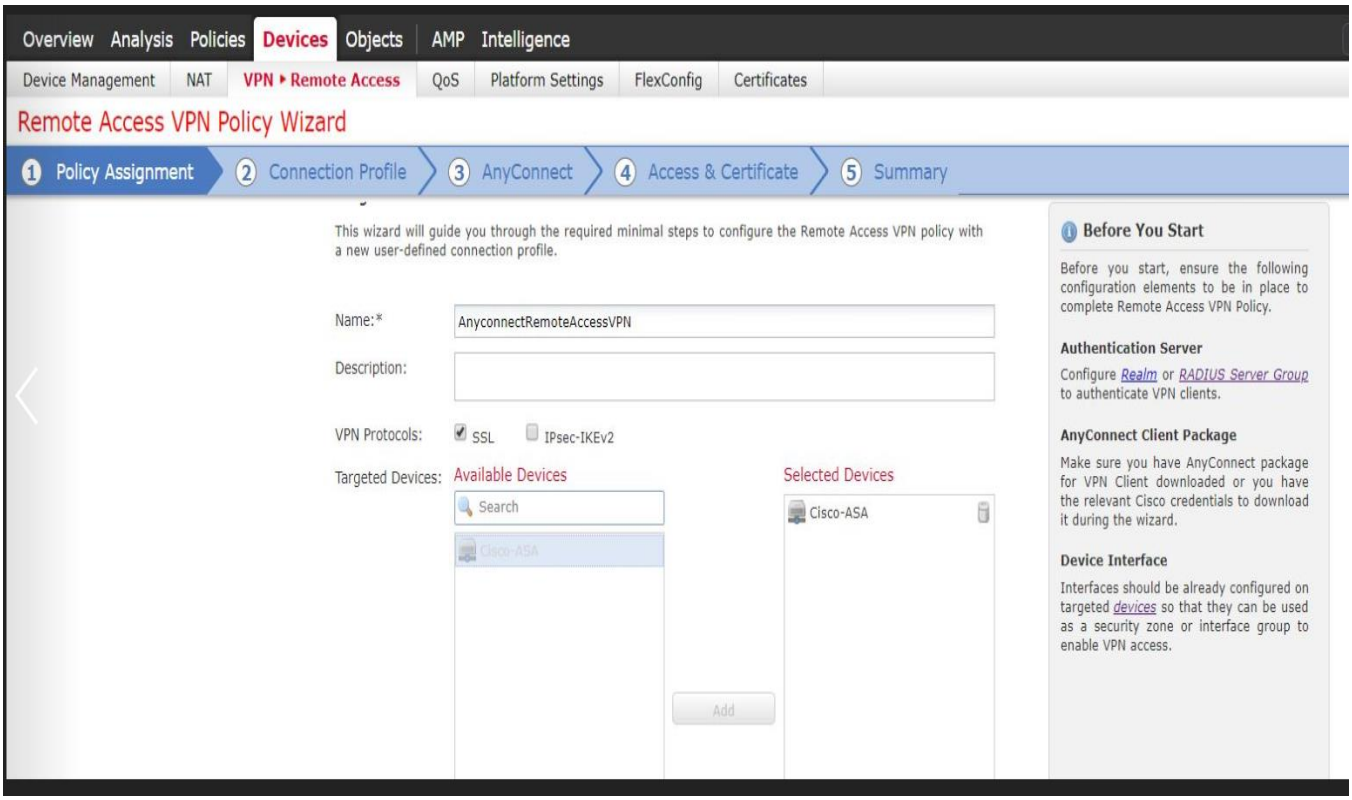
- Under **Add Radius Server Group** >> Enter a Name and Description >> Under **Radius Servers** in the bottom menu >> Click on + to add one.
- Under **New Radius Server** wizard >> Enter the IP address of the Radius Server. Shared Secret. Hit Save.



- Next, go to **Devices** menu >> **VPN** >> **Remote Access** >> Wizard >> **Add a new Configuration.**

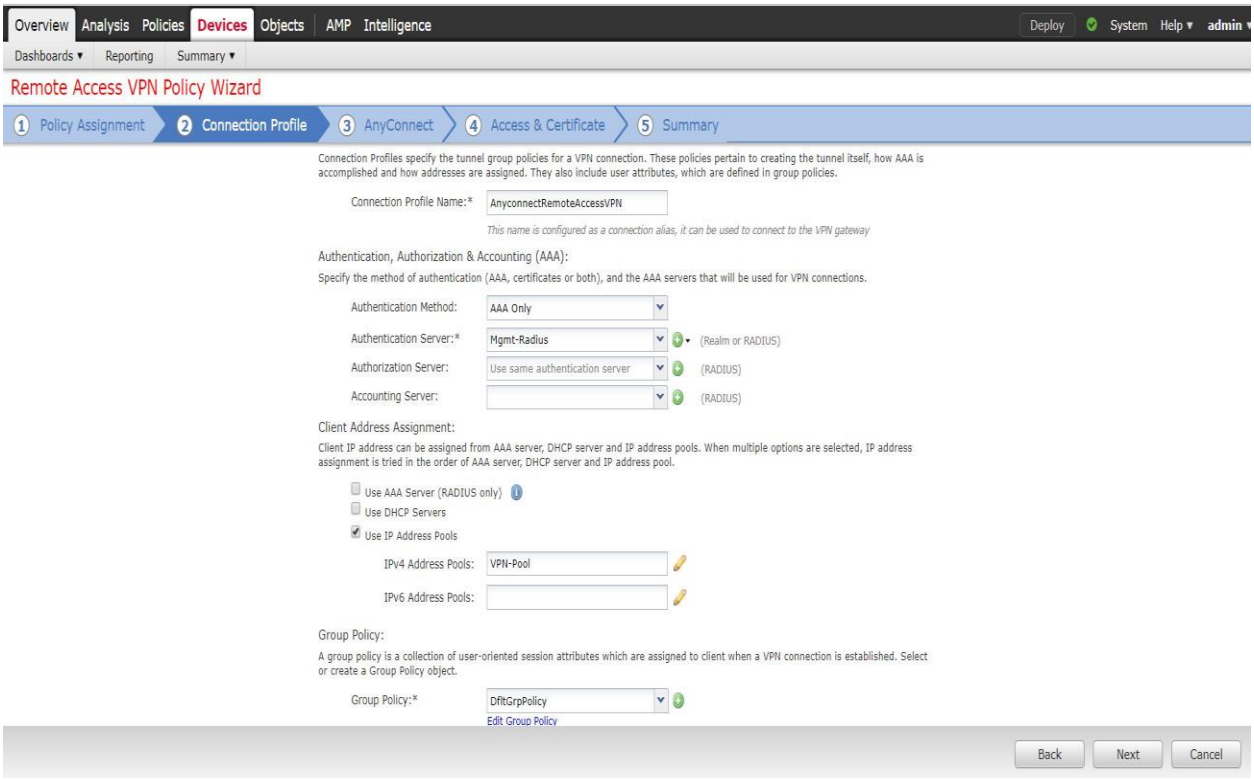
Step 1: Policy Assignment

- Define a **Name, Description**.
- Select a protocol (SSL, IPSec-IKEv2). It is possible to select both.
- Move the appropriate firewall device under "**Available Devices**" (left-side) to "**Selected Devices**" right-side window



3651 Step 2: Connection Profile

3652 • Choose Authentication Method – For instance AAA.

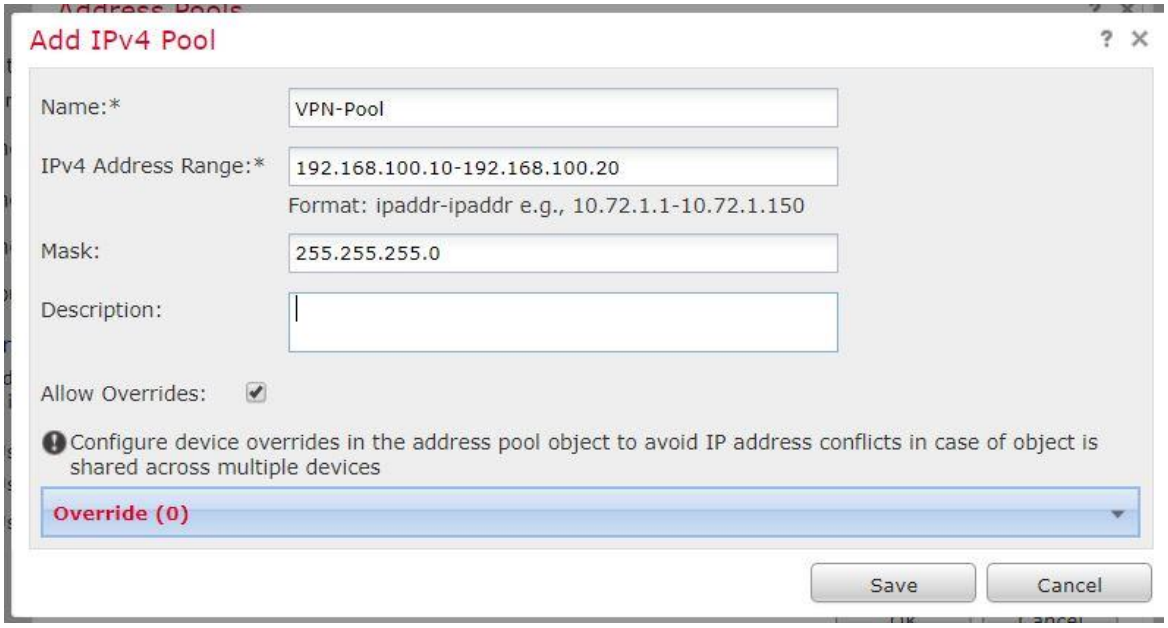


3653

3654

3655

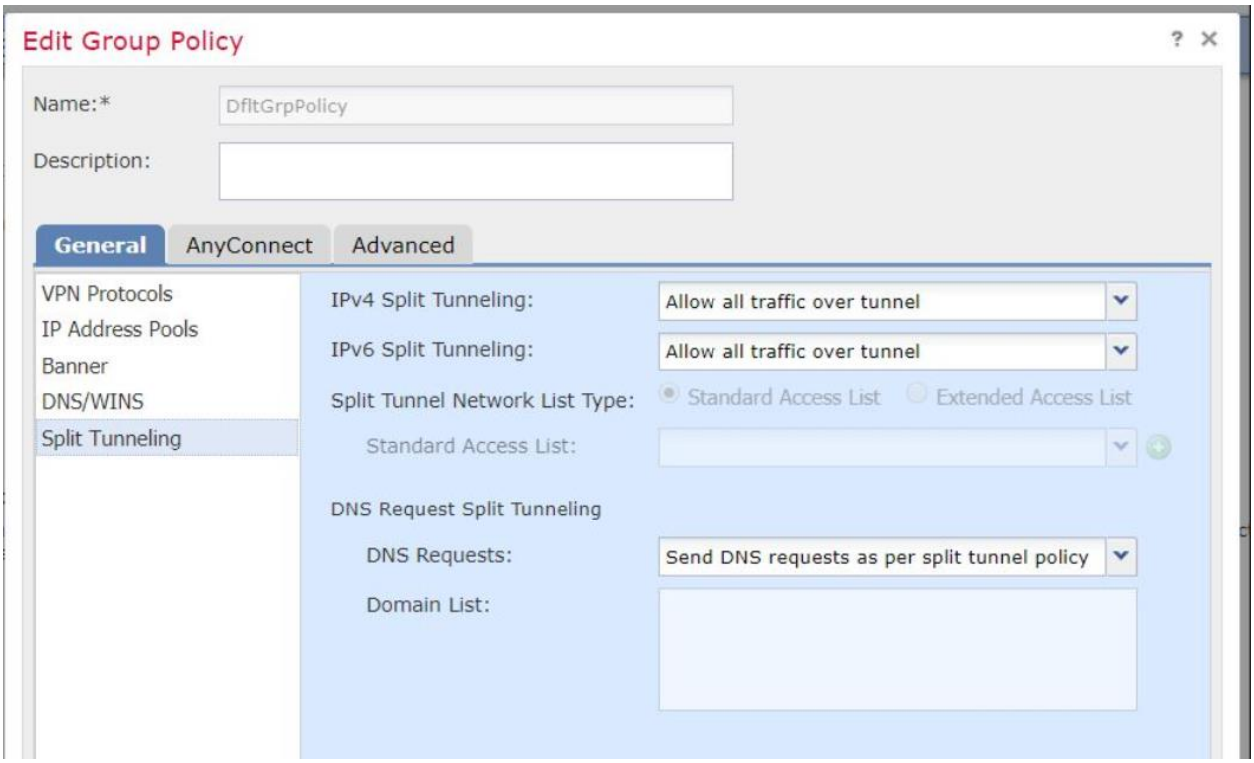
- Under **Authentication Server,** select the Radius Server configured earlier under.
- Select "**Use IP Address Pool**", click to Create a New IPv4 Address Pool. Below image our **VPN-Pool**



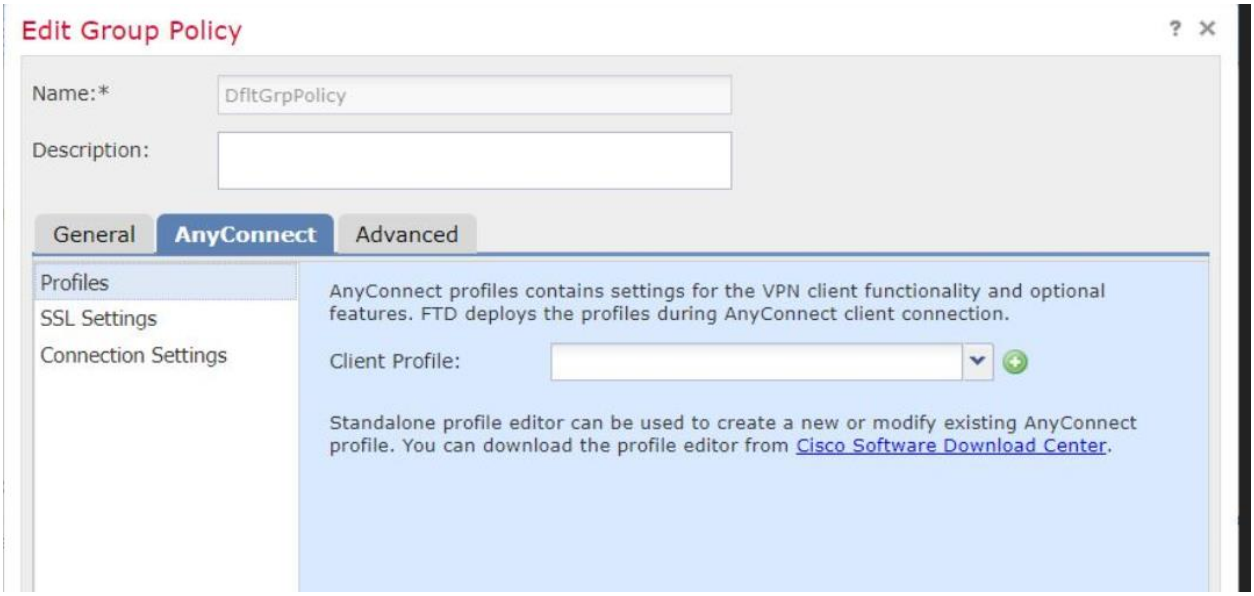
Under **Group Policy** >> **Edit the Default Group Policy** or Create a new one as per your requirement. This is the policy name to be referenced on the Radius server setup on Windows.

The following changes were put in our Default Group Policy

- Under **General** >> VPN Protocols >> **SSL**
- Under **General**>> **Banner** >> Enter a custom welcome message
- Under **General** >> Split Tunneling >> Allow all traffic over tunnel (Split tunnel was disabled)

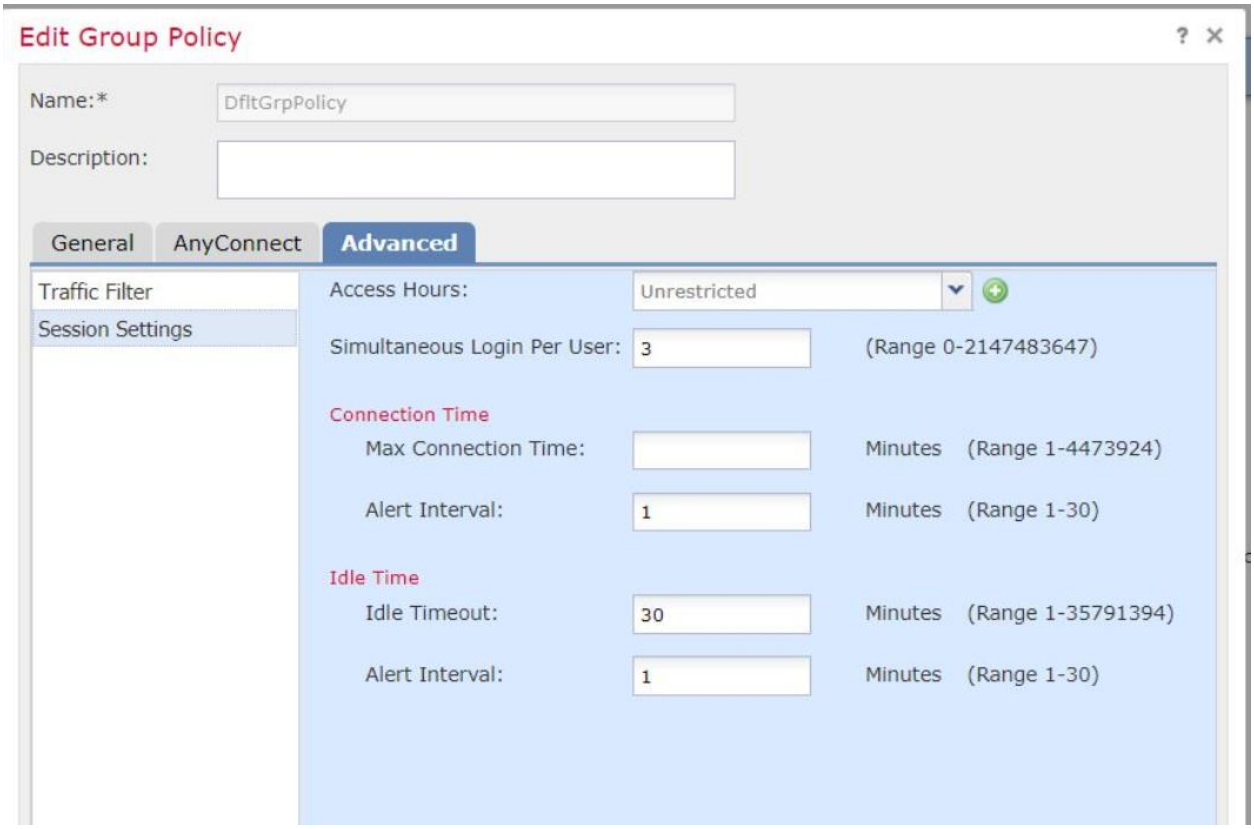


3676 - Under AnyConnect, Create a new Client Profile (if not already)



3677

3678 Under **Advanced** >> **Session Settings** >> Idle Session Timeout was set to 30 minutes

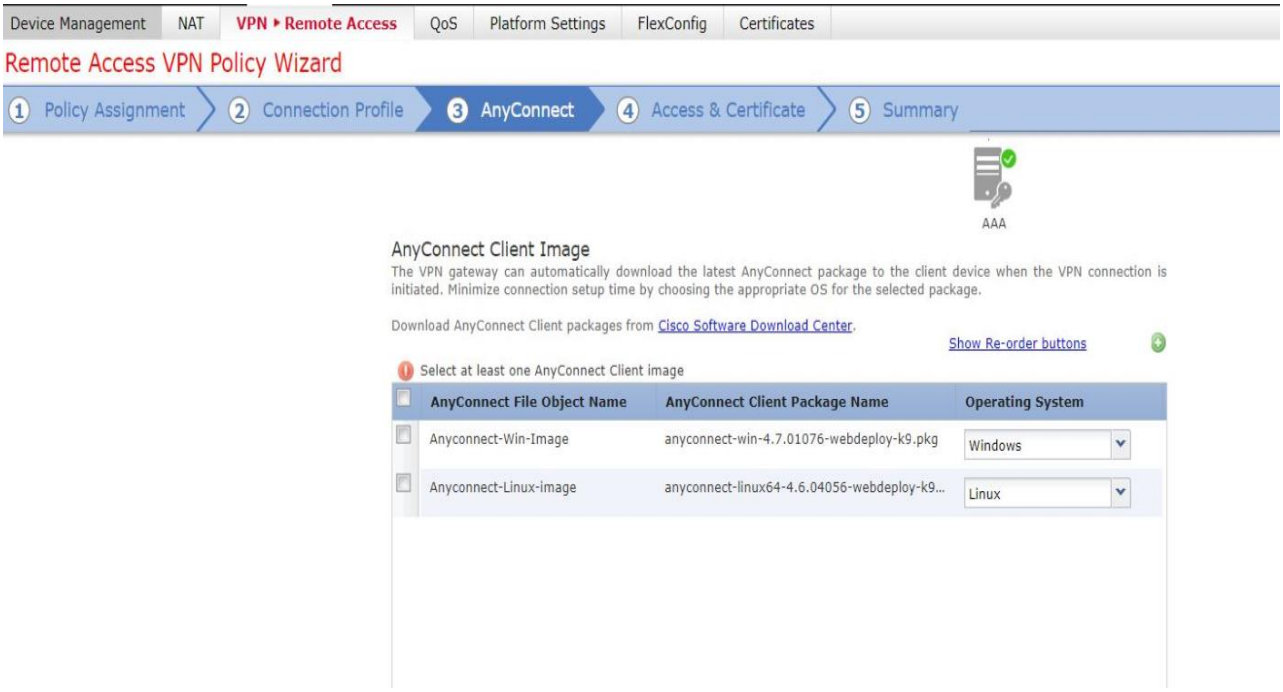


3679

3680

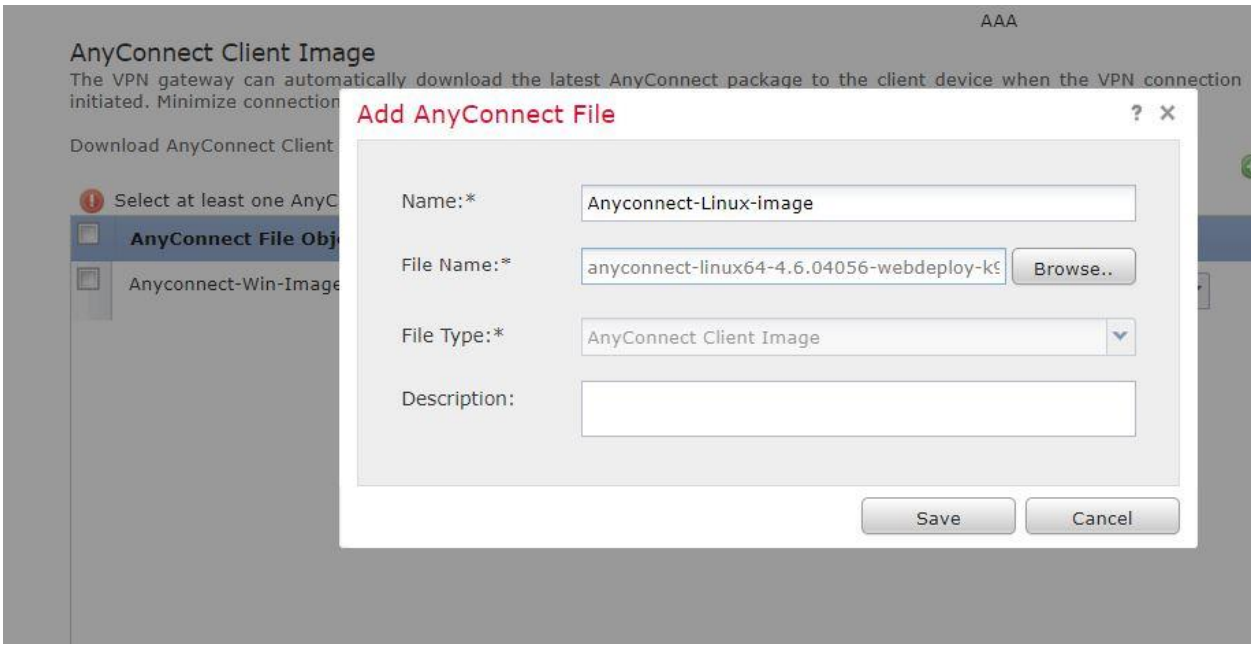
3681 Step 3: AnyConnect:

3682 • Select the AnyConnect Image for OS Supported (Windows, Linux, MacOS)



3683

3684 • The Image files can be added manually by clicking on + icon.

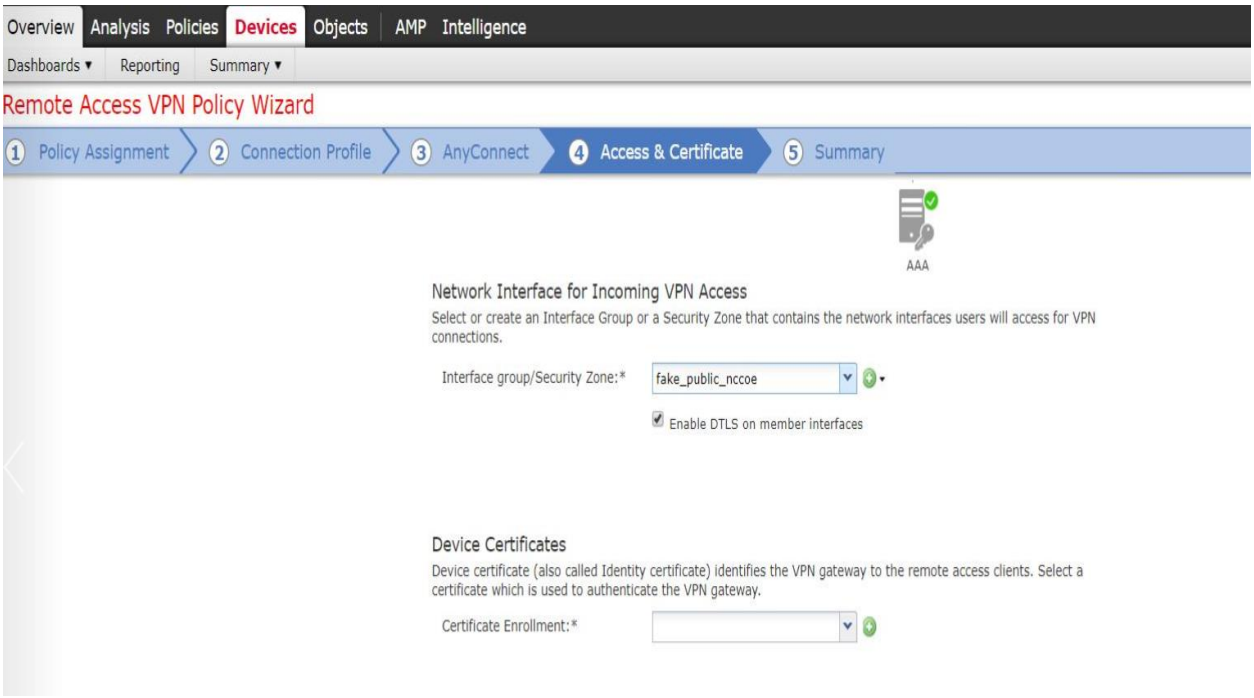


3685

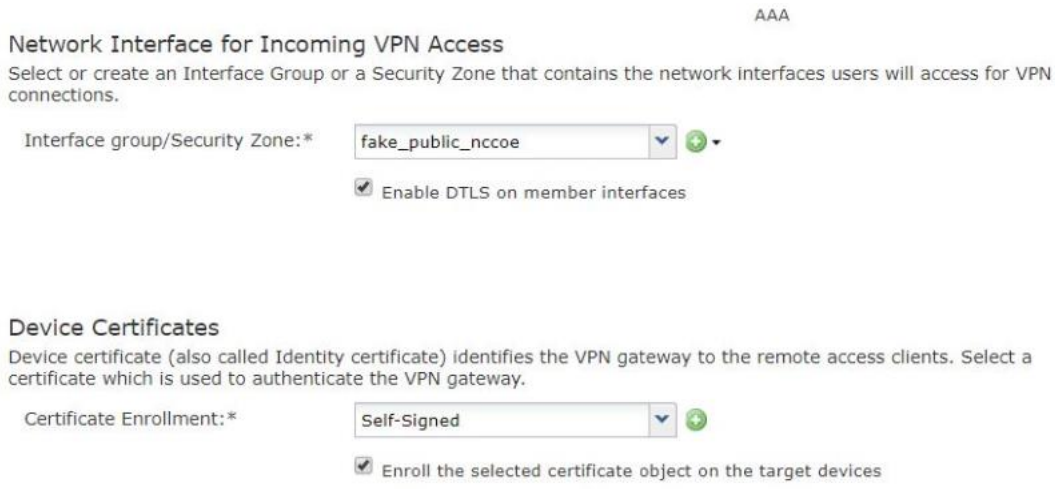
3686

Step 4: Access and Certificate:

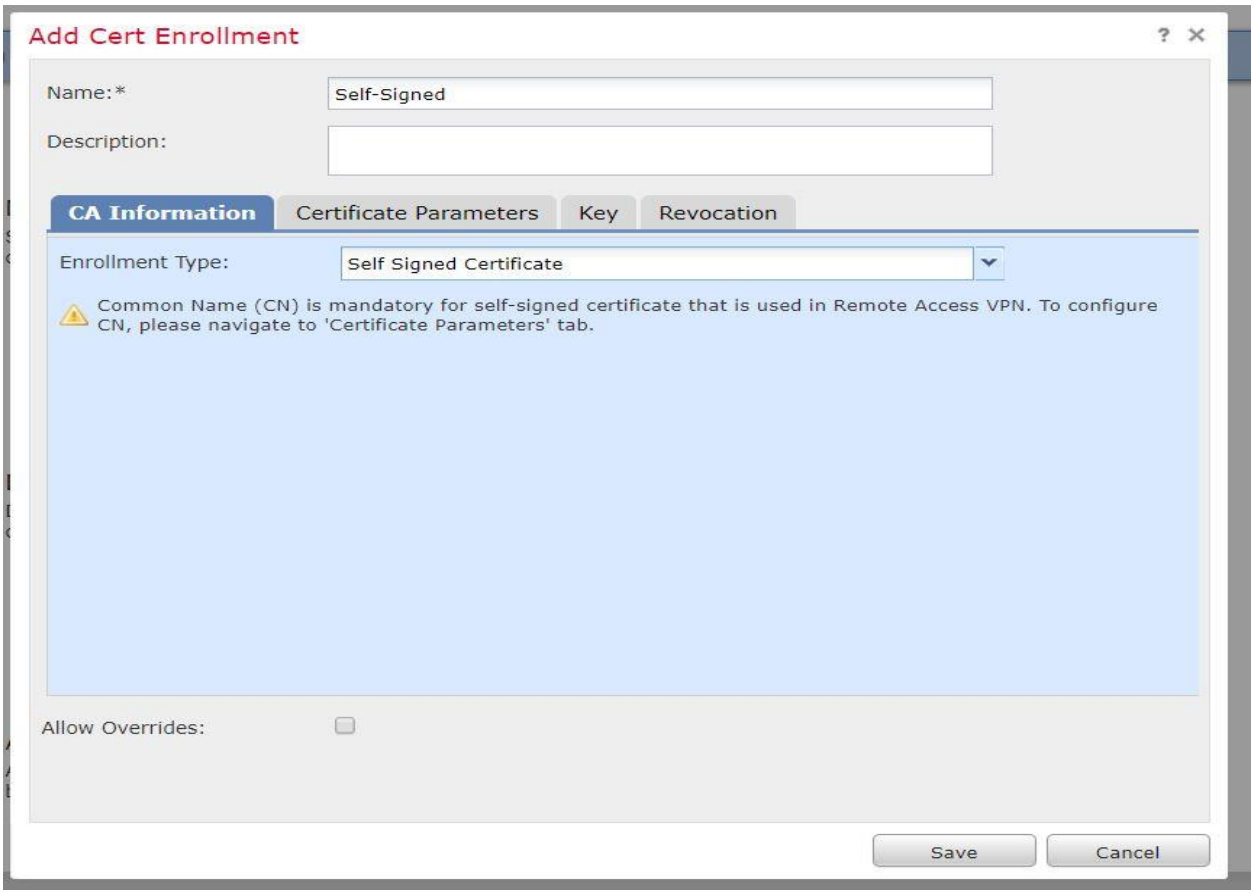
- **Interface group/Security Zone**: Select your **outside** interface



- **Device Certificates:** Select a Name and Certificate can be imported manually or Click + to create a Self-signed Certificate. A self-signed certificate was used in our environment.



3695

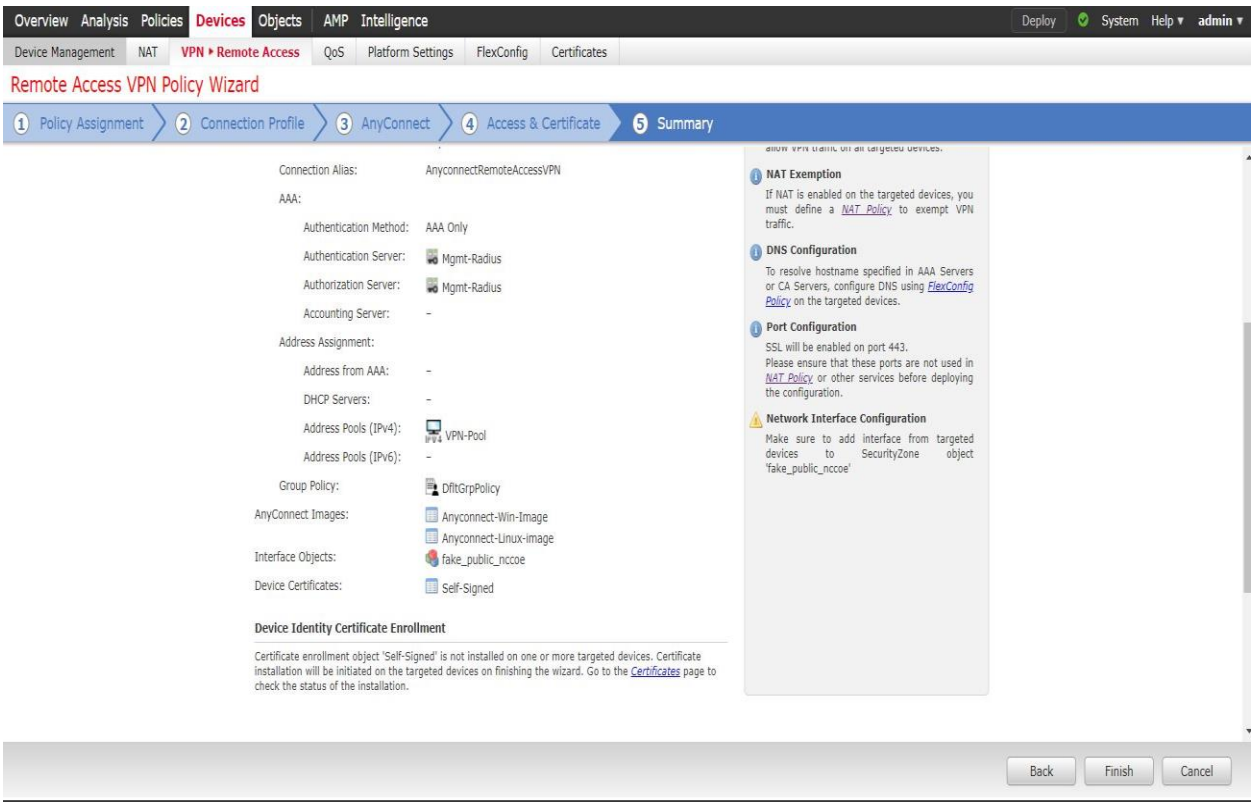


3696

3697

3698 Step 5: Summary:

3699 • Review the **Summary**. If all OK, click **Finish** to apply the changes.



3700

3701 Further Configuration Requirements:

3702 Once the Wizard is completed, the following configuration requirements need to be done for RA
3703 VPN to work on all device targets:

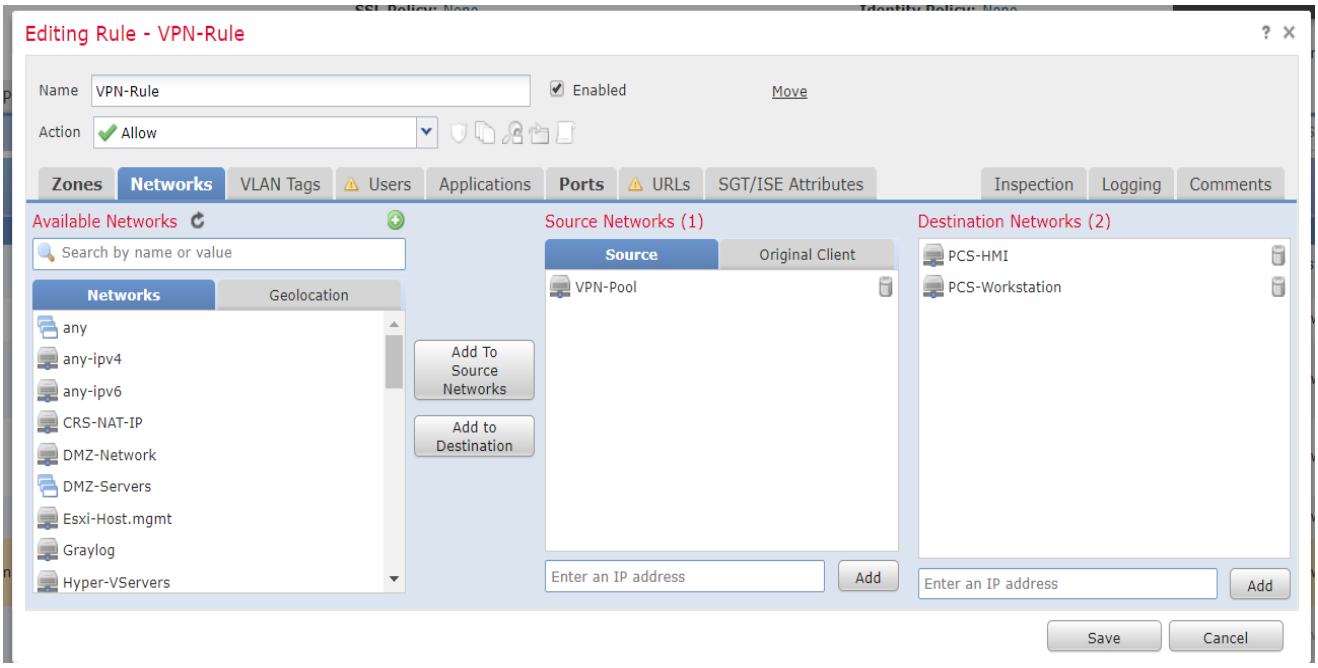
3704 **Access Control Policy:** An ACL rule must be defined to allow VPN traffic on to whichever
3705 network segments you wish to permit.

3706

3707 The image below shows an ACL configured to allow VPN traffic from outside to only a couple
3708 of internal servers in the Process Control system over Remote Desktop Port 3389.

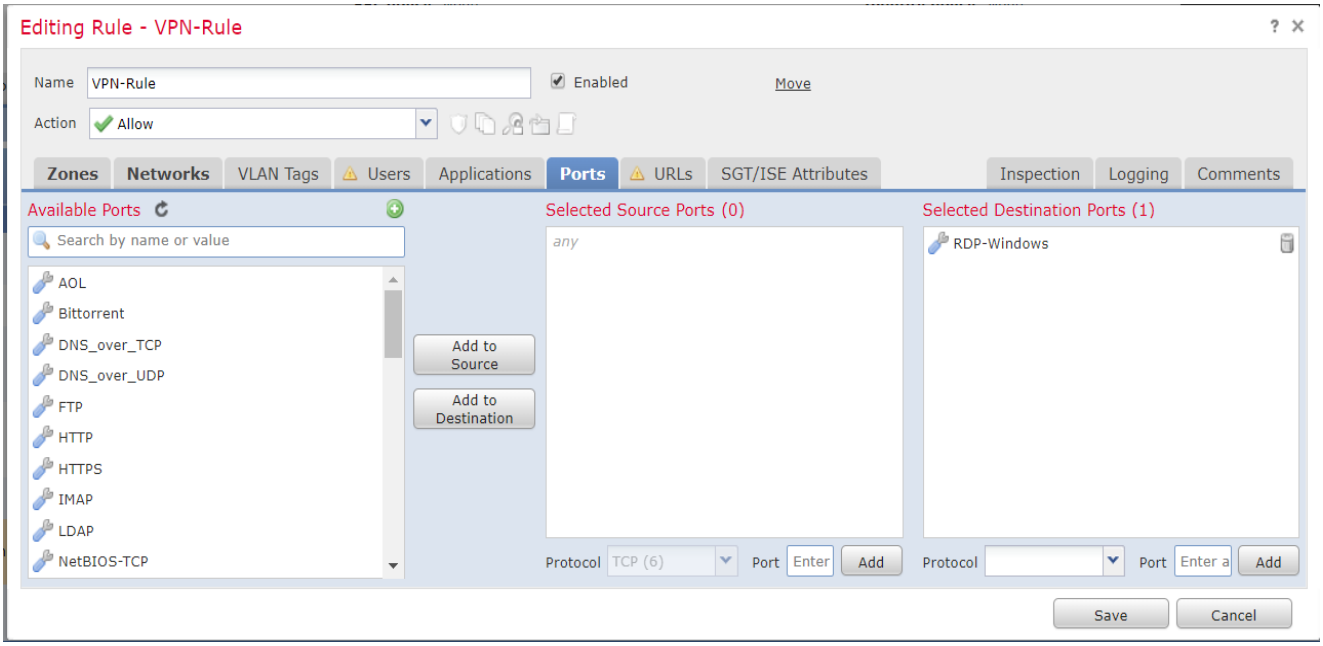
	Source	Destination	Selection
Zones	Outside	Inside	
Networks	VPN_Pool (Network)	HMI Server (Host) Workstation (Host)	
Ports	Any	3389 TCP	
Action			Allow
Inspection			Enabled. Balanced connectivity over Security.

3709



3710

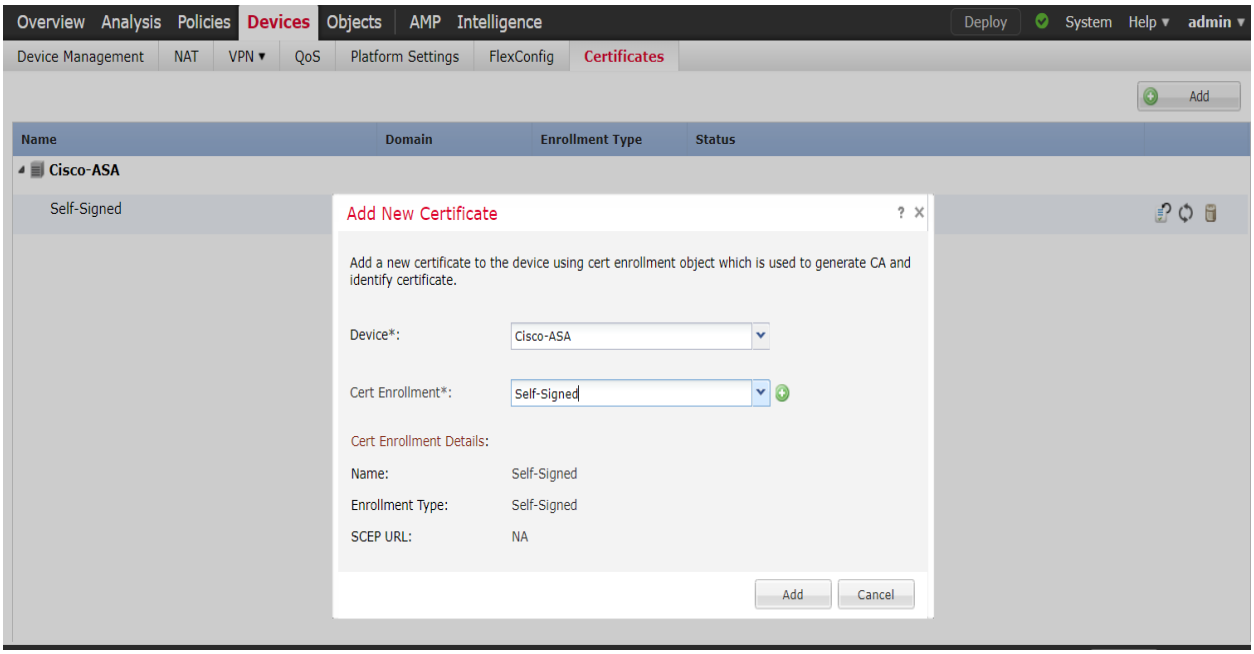
3711



3712

3713

3714 **Device Certificate:** Associate the certificate created earlier with the Firewall device.



3715

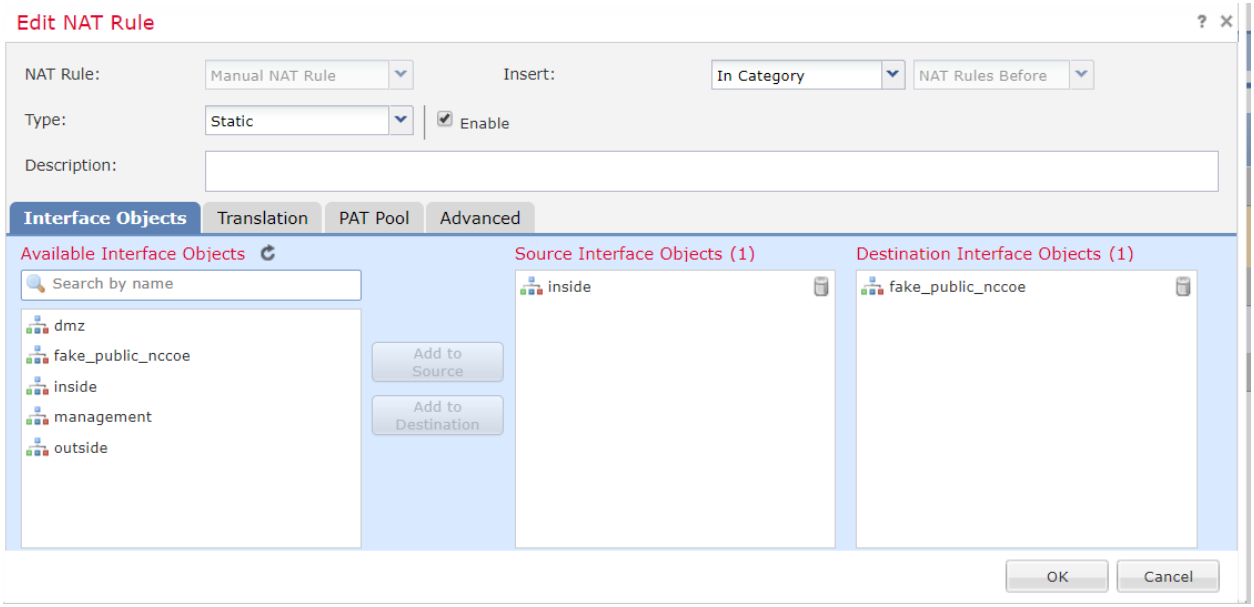
3716

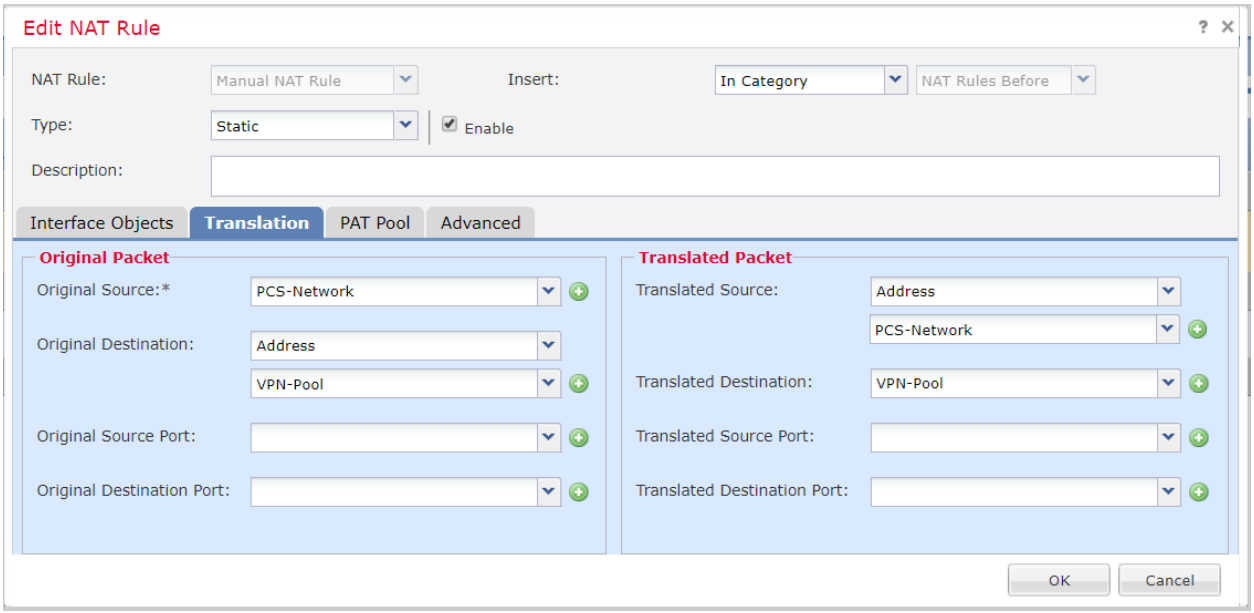
3717

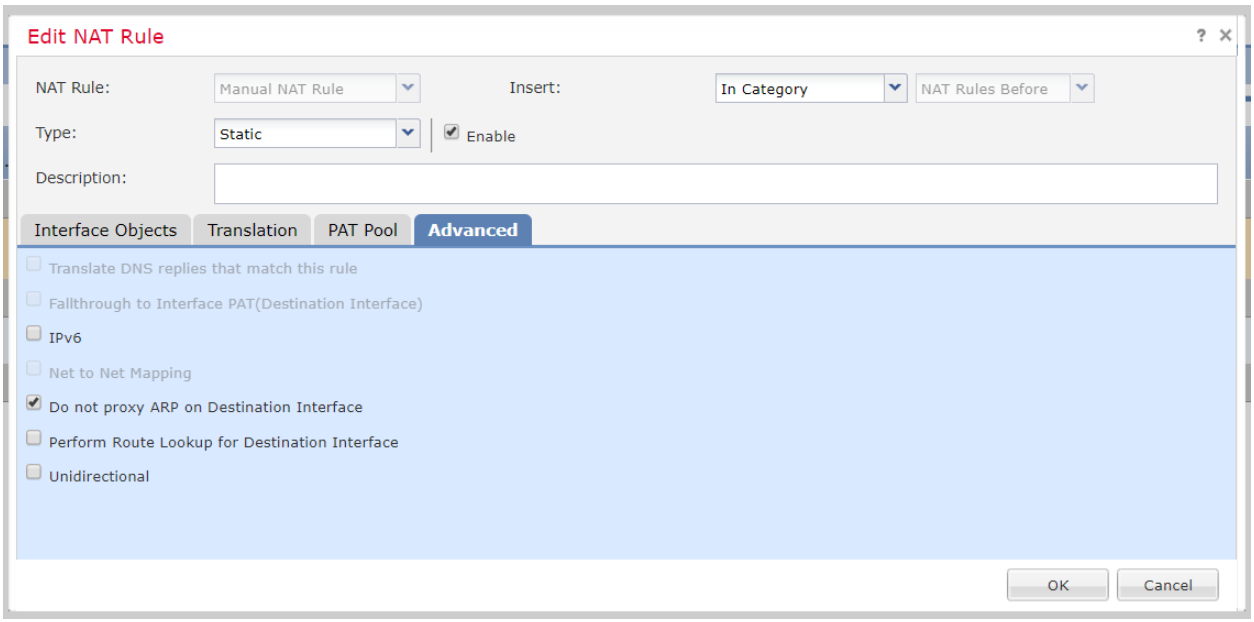
Create a NAT Exemption rule: If NAT is enabled on the firewall, you must define a NAT rule to exempt VPN traffic.

Go to **Devices** Menu >> **NAT** >> **Select <NAT Policy>** >> **Add Rule.**

Below images show a NAT Rule created to exempt VPN Traffic



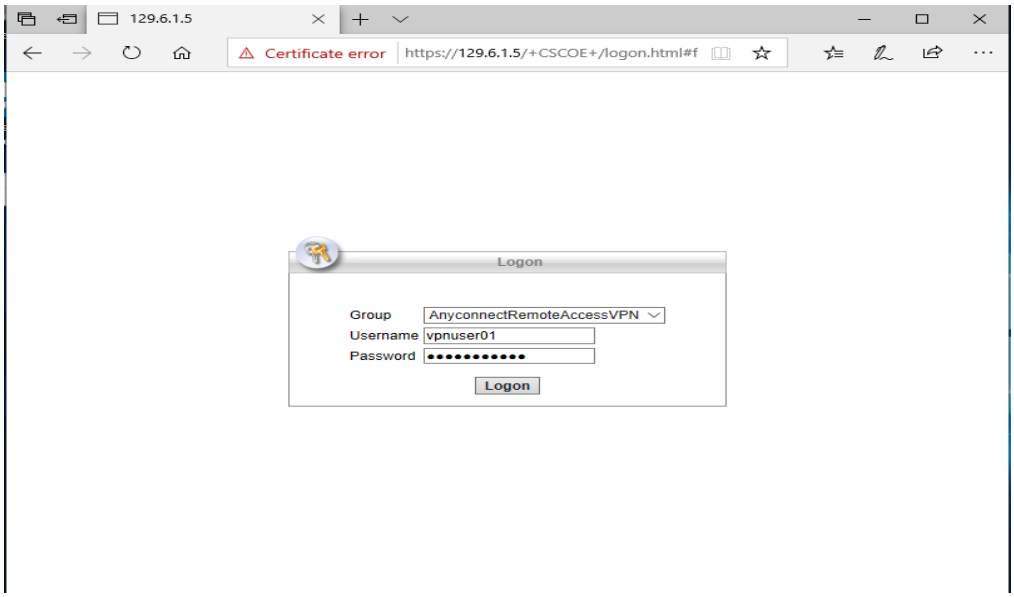




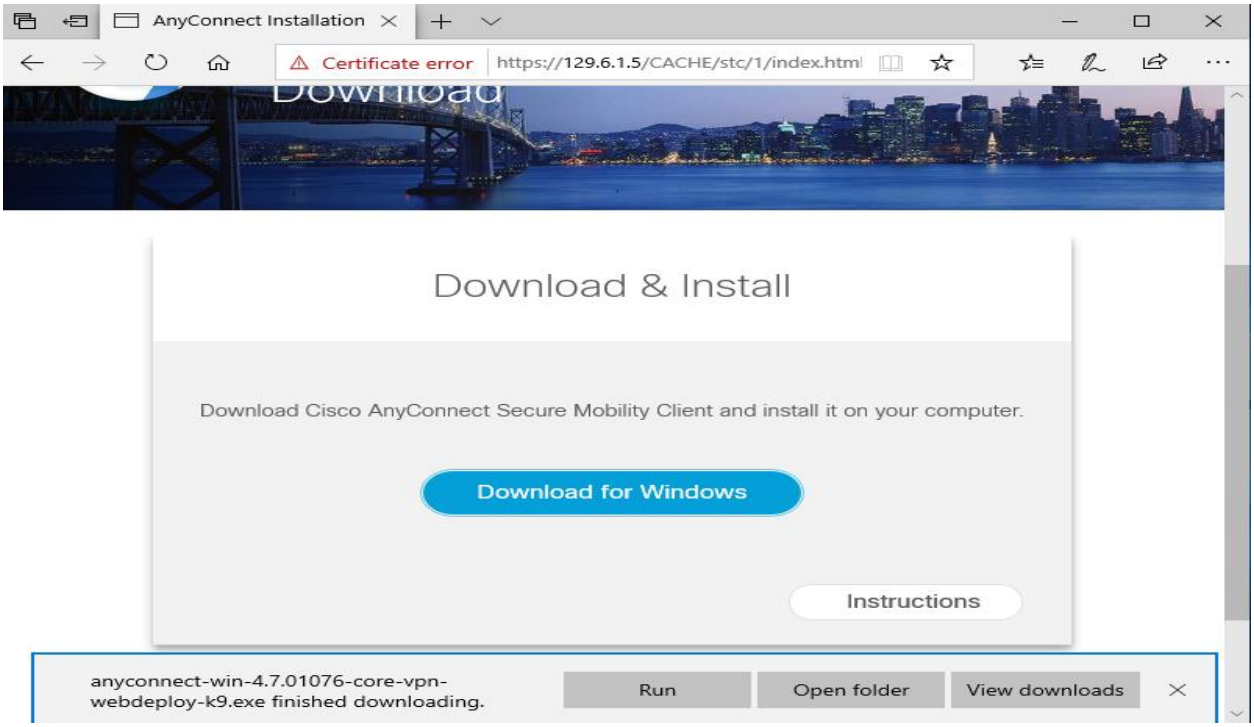
Client Connection:

Clients can use a web browser to connect to the Outside interface of the device. Once they login, the AnyConnect image is automatically downloaded or updated. After that, clients can connect using the AnyConnect software installed on their device, which already has the AnyConnect XML profile with all the parameters for the RA VPN connection.

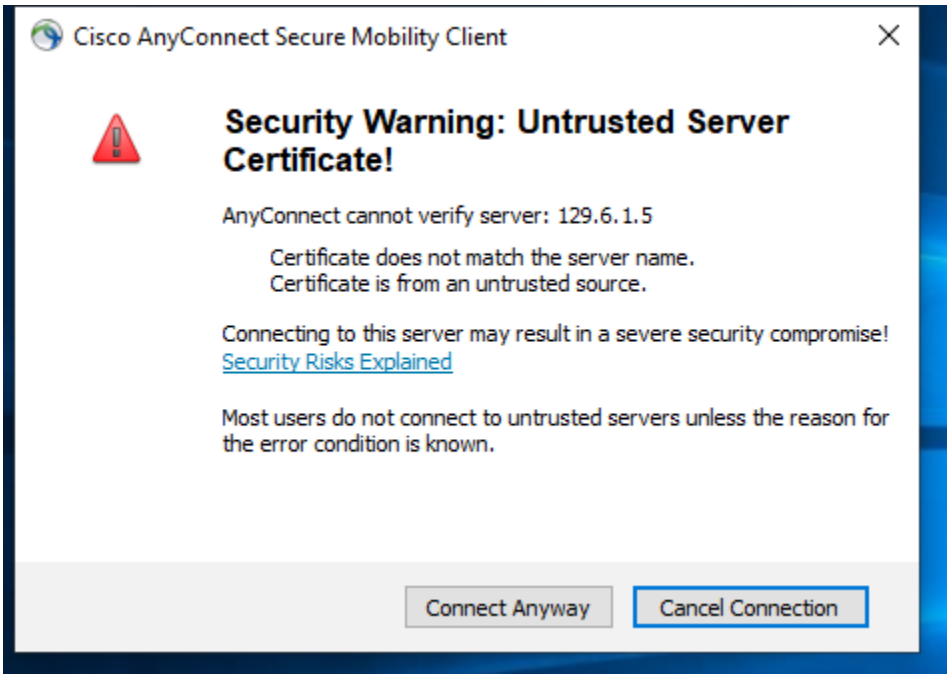
- Accessing the outside interface should give a similar page as shown below. Enter the Active Directory user credentials created earlier to Logon.



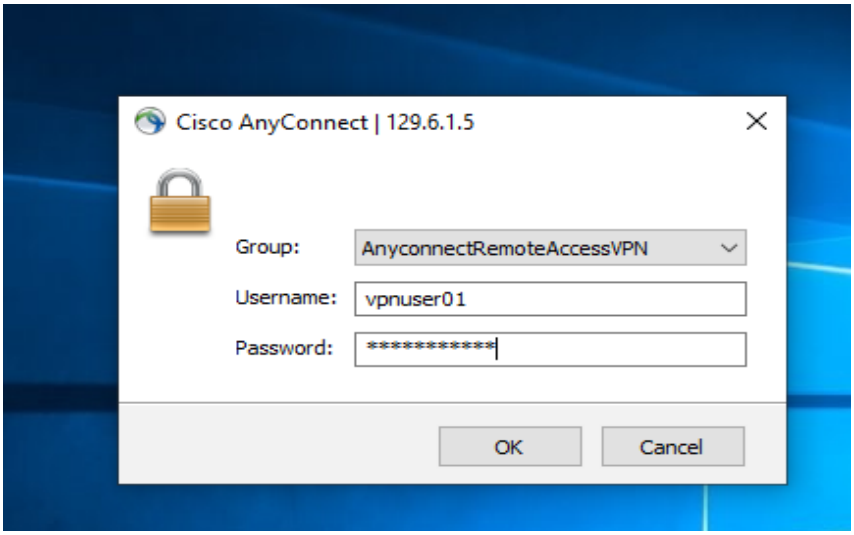
- Download the Client software and Install it.



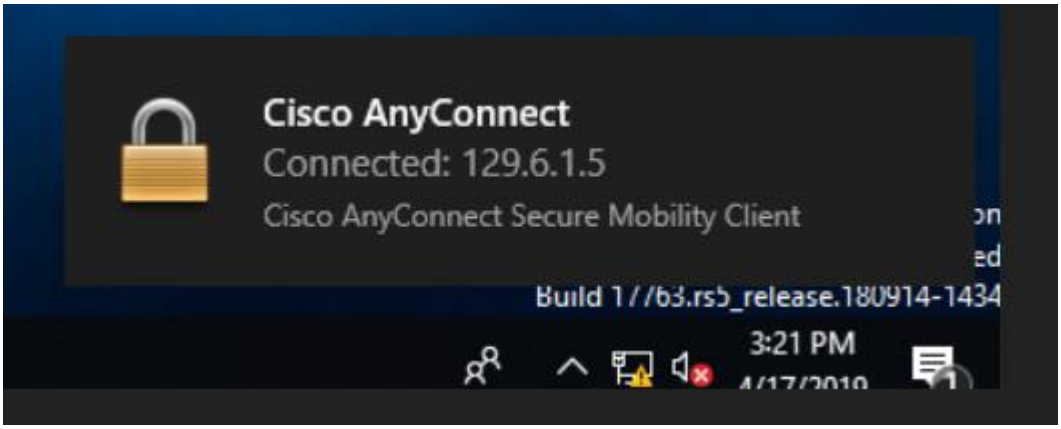
- If using a self-signed certificate as in our case, you will be presented with this warning. Hit **Connect Anyway**



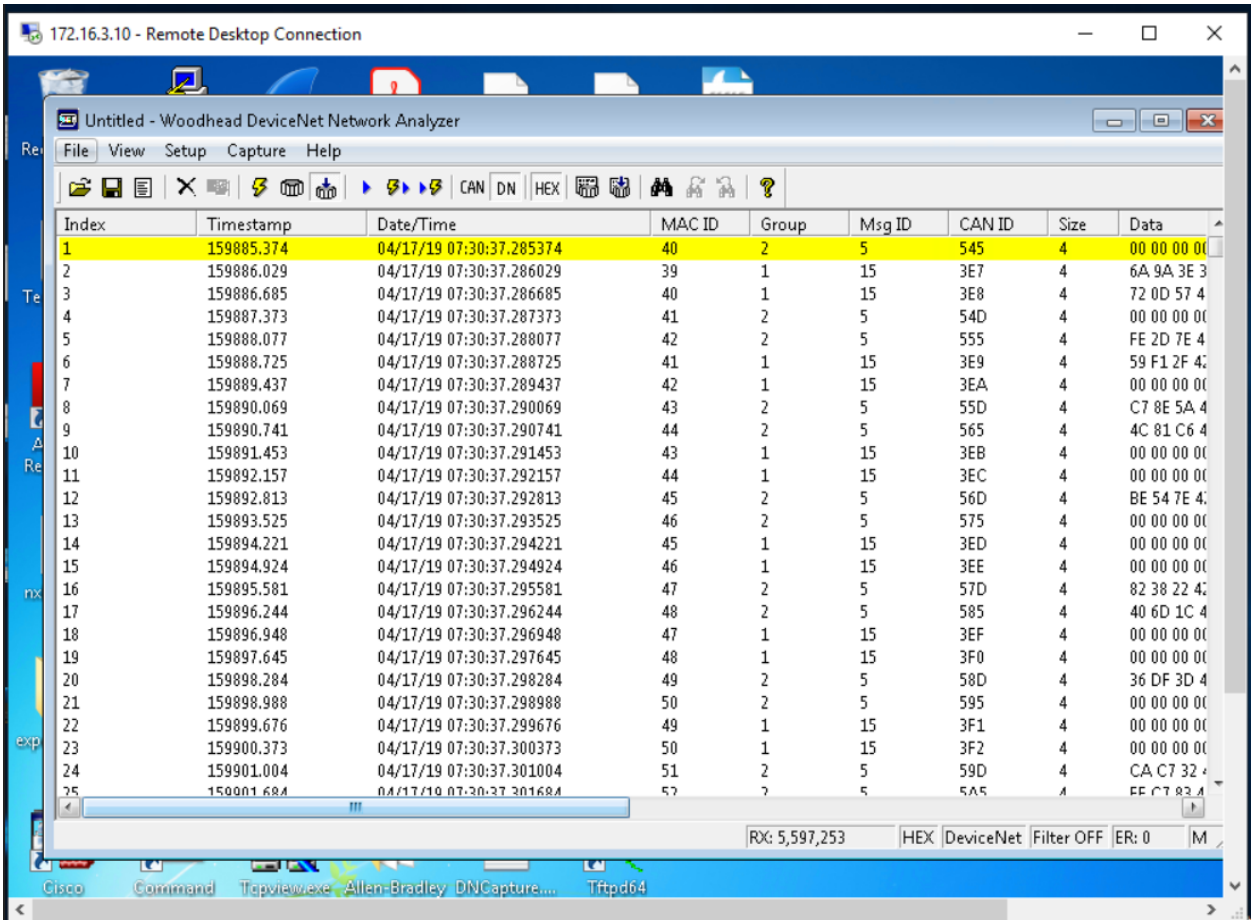
- Enter the AD user credentials



- When connected, a pop-up message appears showing the Client as Connected.

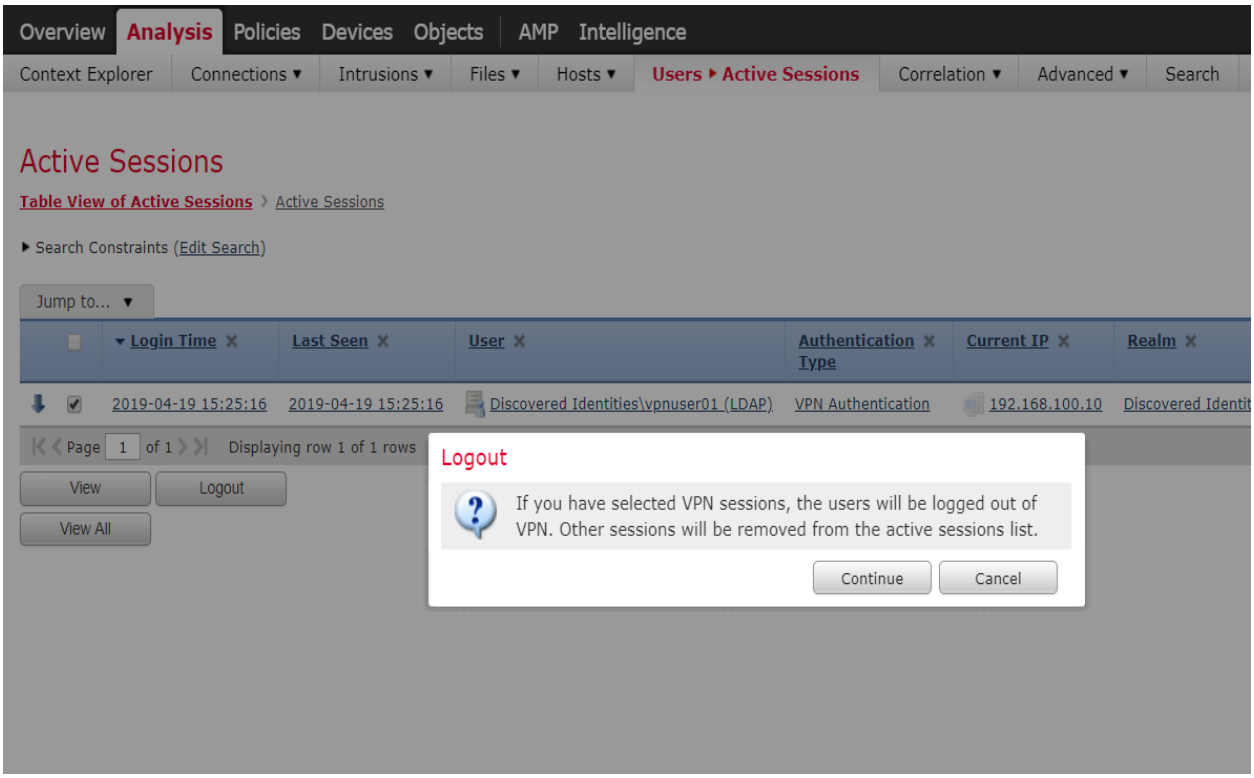


- Upon establishing the connection, the two servers in Process Control System whitelisted earlier in the ACL Rule were accessed using RDP to perform Remote Maintenance.



Session Termination

To terminate a VPN Session, log on to the Cisco FMC Web interface, go to **Analysis** >> **Users** >> **Active Sessions**. Select the **session** and click **Logout**



References:

[1] Cisco AnyConnect VPN
https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-secure-mobility-client/at_a_glance_c45-578609.pdf

[2] Cisco ASA VPN User Authentication:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/117641-config-asa-00.html

4.8.6 Highlighted Performance Impacts

The following performance measurement experiment was performed for the Cisco AnyConnect VPN tool while the manufacturing system was operational:

Experiment PL012.1- VPN connection from testbed LAN
In this experiment, a remote user was accessing the HMI from a remote computer through the VPN connection. A remote computer was first connected to the testbed LAN through the VPN, then used the Remote Desktop to connect to the HMI computer to access the HMI screen.

Although there was slightly increased network traffic between the testbed LAN and the PCS system due the Remote desktop session, there was no significant performance impact observed in the PCS system. The packet round trip time between the HMI and OPC remained mostly constant with and without the VPN connection.

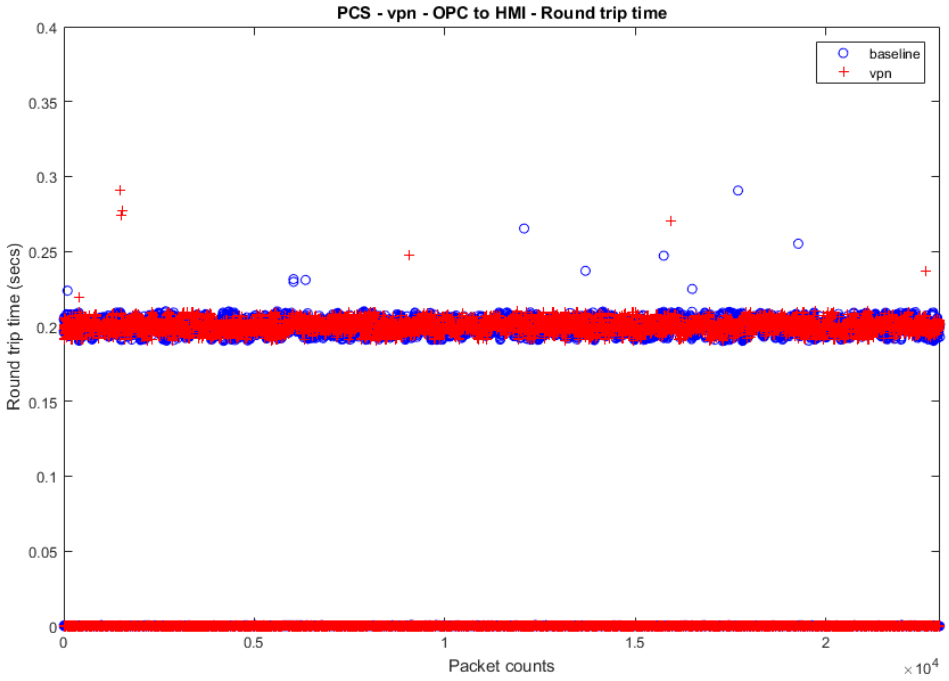


Figure 4-12 Plot of packet round trip time from OPC to HMI computer during the use of VPN connection from a remote computer

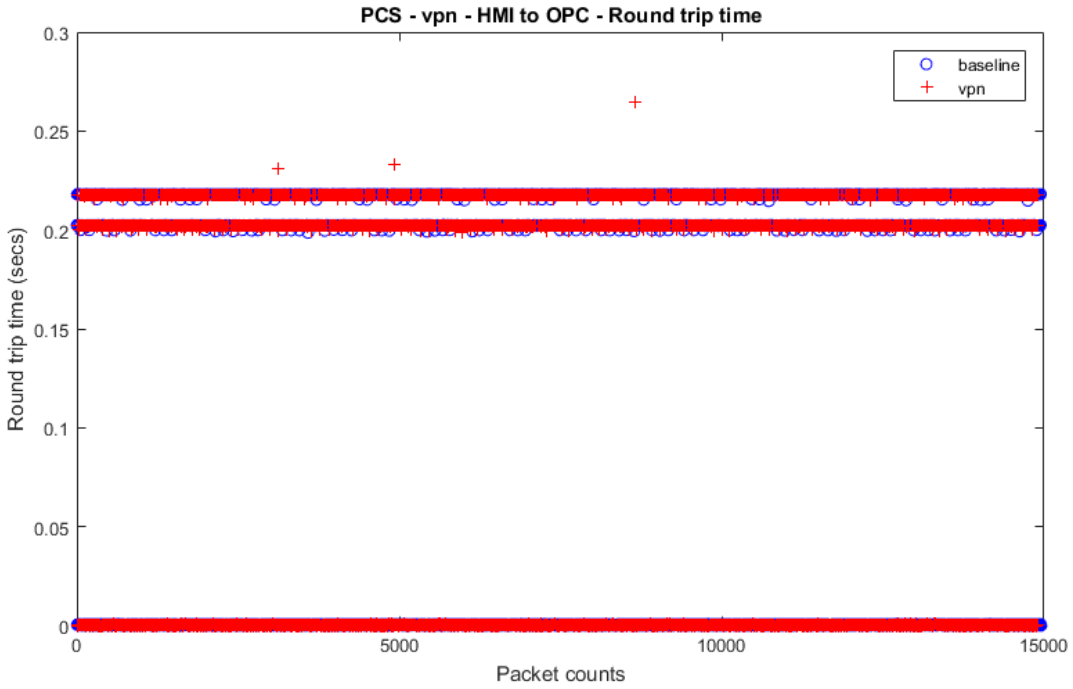
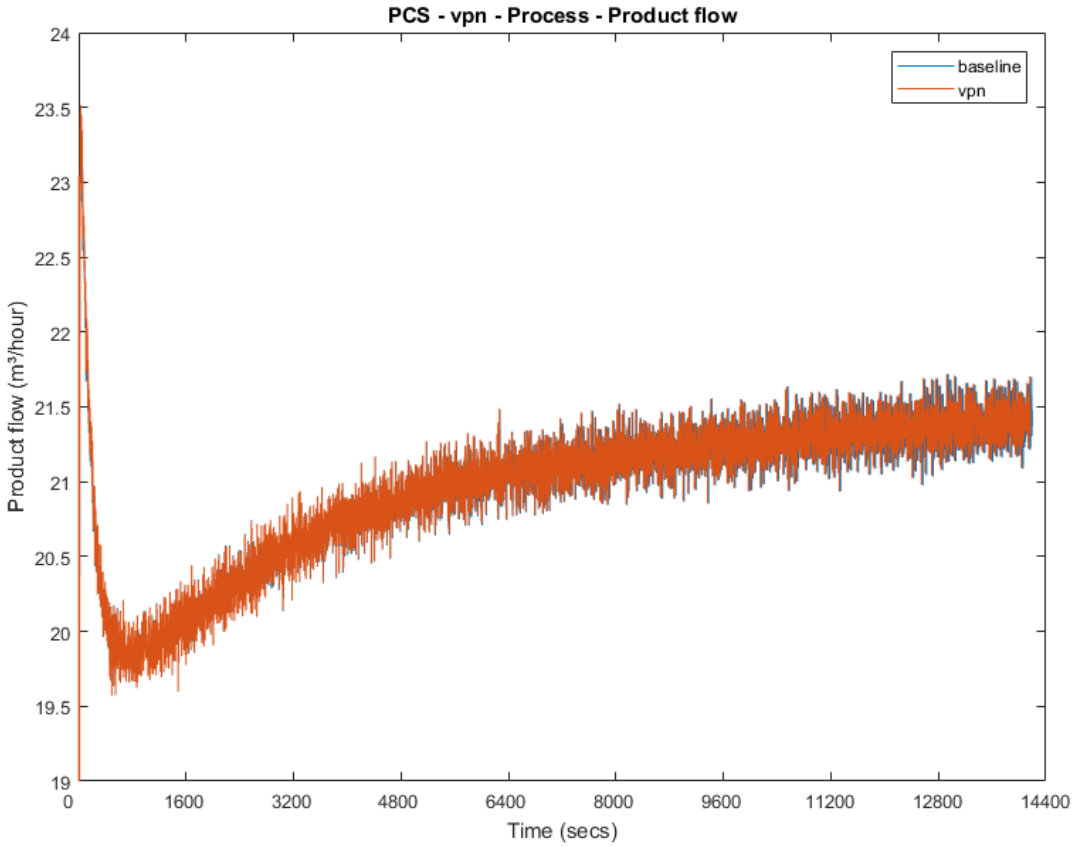


Figure 4-13 Plot of packet round trip time from HMI to OPC computer during the use of VPN connection from a remote computer

The manufacturing process also remained stable without any significant performance impact observed. The reactor pressure and product flow rate remained constant with and without the VPN connection.



3796

3797 **Figure 4-14 Manufacturing process product flow rate during the use of VPN connection from a remote**
3798 **computer**

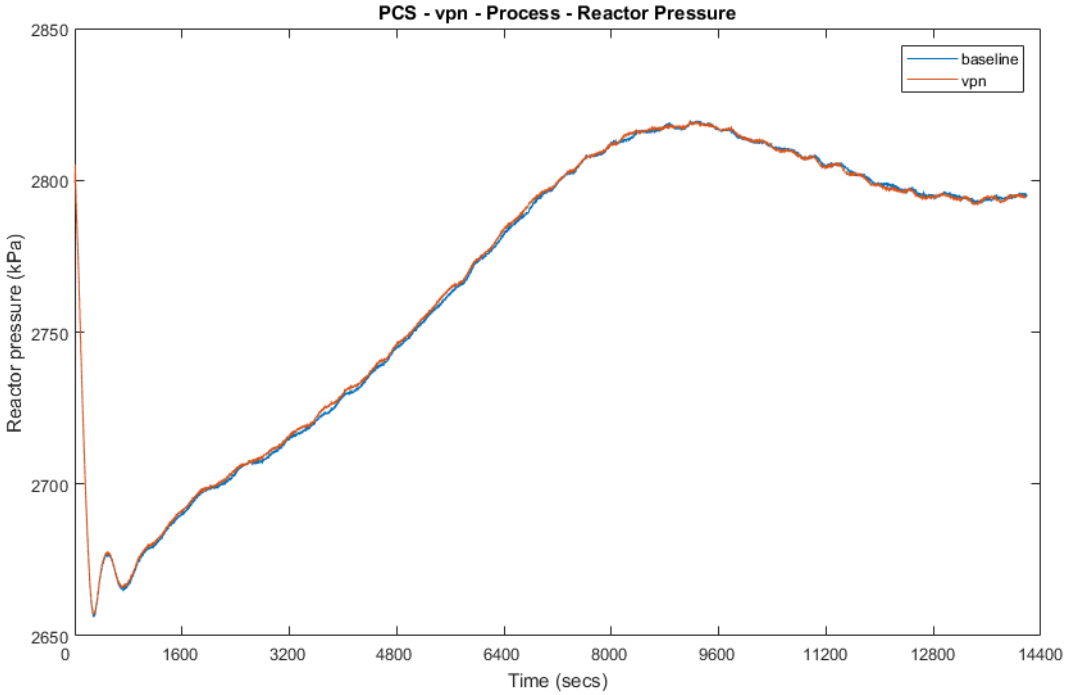


Figure 4-15 Manufacturing process reactor pressure during the use of VPN connection from a remote computer

4.8.7 Link to Entire Performance Measurement Data Set

Cisco VPN KPI data

Cisco VPN measurement data

4.9 Microsoft Active Directory

4.9.1 Technical Solution Overview

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. A directory is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators. For example, AD DS stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information. A server running Active Directory Domain Services (AD DS) is called a domain controller. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. Active Directory uses Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos and DNS.[20]

Points to consider

- Cost of infrastructure can get high.
- Requires expertise to setup and maintain. Setup involves detailed planning.
- It is prone to being hacked.

4.9.2 Technical Capabilities Provided by Solution

Microsoft Active Directory provides components of the following Technical Capabilities described in Section 6 of Volume 1:

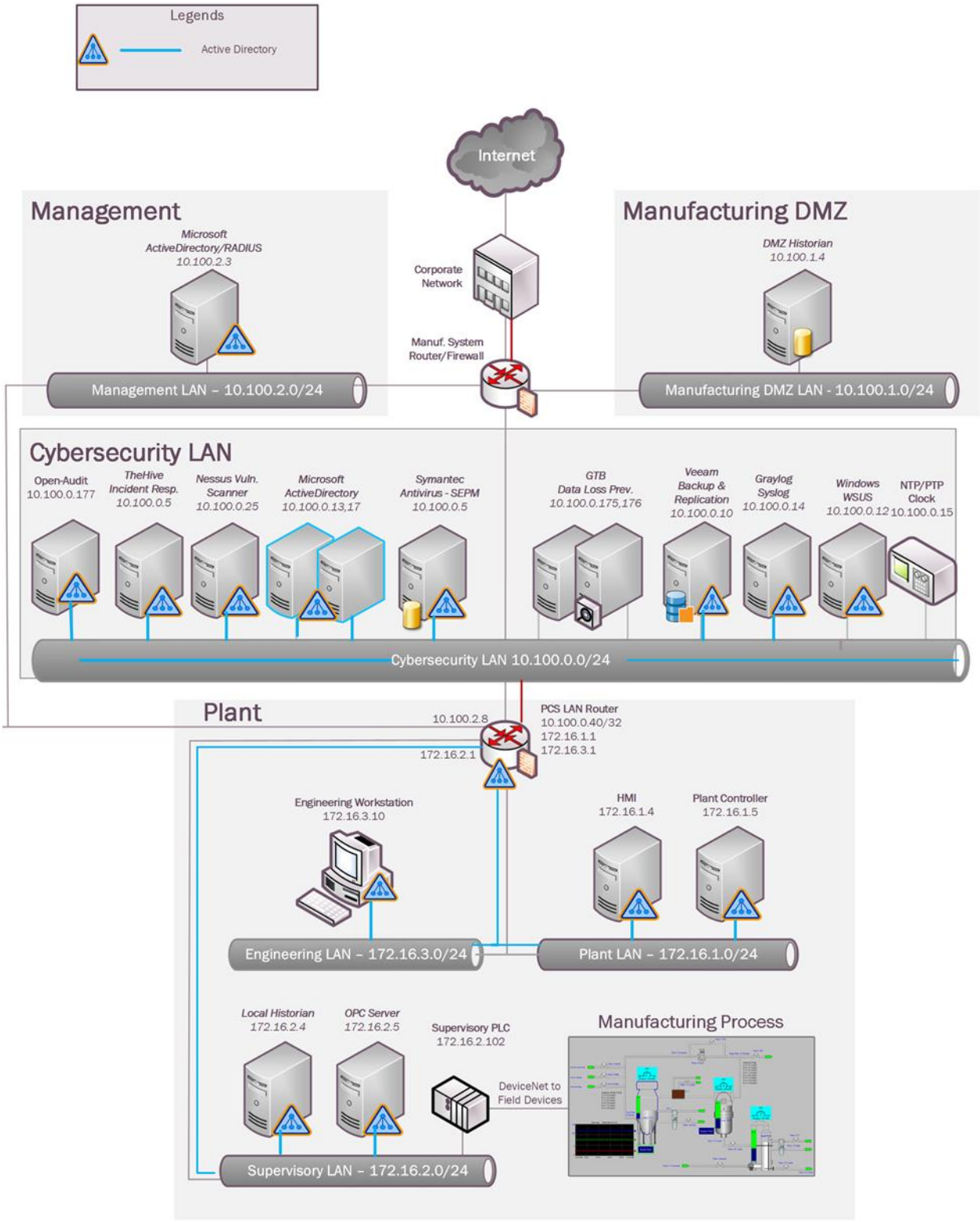
- Credential Management
- Authentication and Authorization

4.9.3 Subcategories Addressed by Implementing Solution

PR.AC-1, PR.MA-1, PR.MA-2, PR-PT-3, PR.PT-4, DE.CM-3

[20] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

4.9.4 Architecture Map of Where Solution was Implemented



4.9.5 Installation Instructions and Configurations

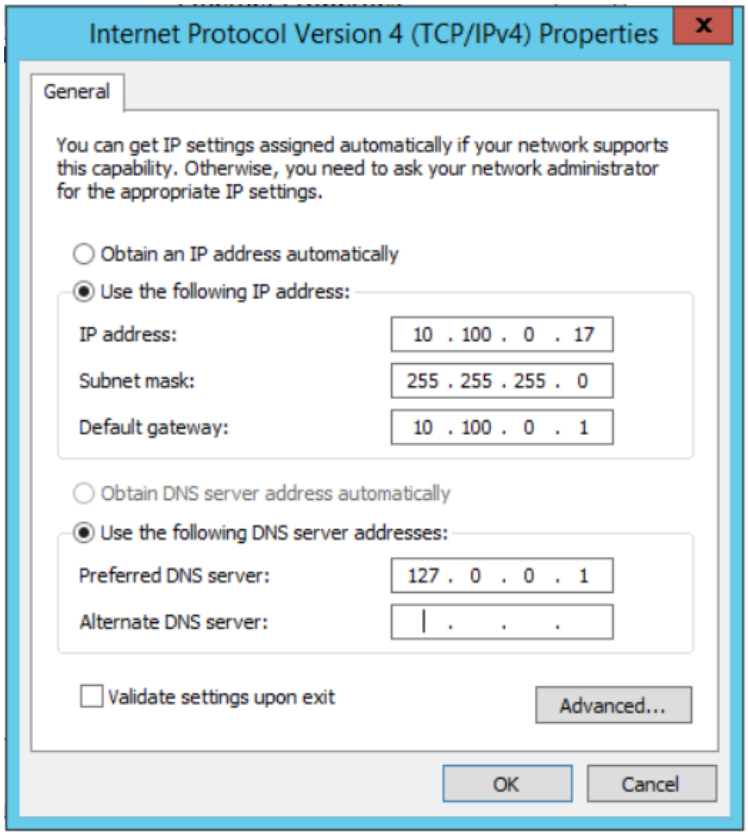
Setup:

Our setup consists of two separate Active Directory domain environments; one for the Cybersecurity -LAN network and other for the Management network. For security reasons, The AD domain in the Cybersecurity LAN network is separate from the domain that's in the Management network. A pair of Domain Controllers (DC) running on Windows 2012 R2 were setup in the Cybersecurity LAN network for authenticating Windows/Linux devices and another separate DC on Windows 2012 R2 was setup in the Management network for authenticating VPN users and network devices such as boundary routers. This DC in the Management network is used in conjunction with a Windows NPS (Radius) server for authenticating the network devices.

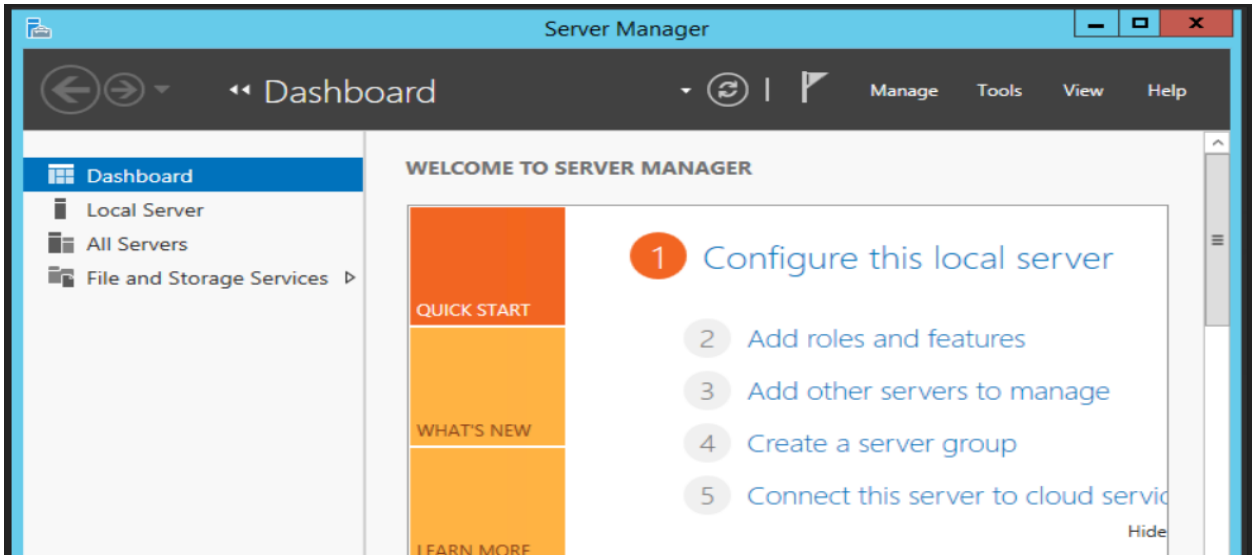
Hostname	IP address	Roles	Domain Name
LAN-AD	10.100.0.17	Active Directory, DNS, Network Policy Server (Radius)	LAN.lab
LAN-AD02	10.100.0.13	Active Directory, DNS, Network Policy Server (Radius)	LAN.lab
Mgmt-**AD**	10.100.2.3	Active Directory, DNS, Network Policy Server (Radius)	Mgmt.lab

Installation:

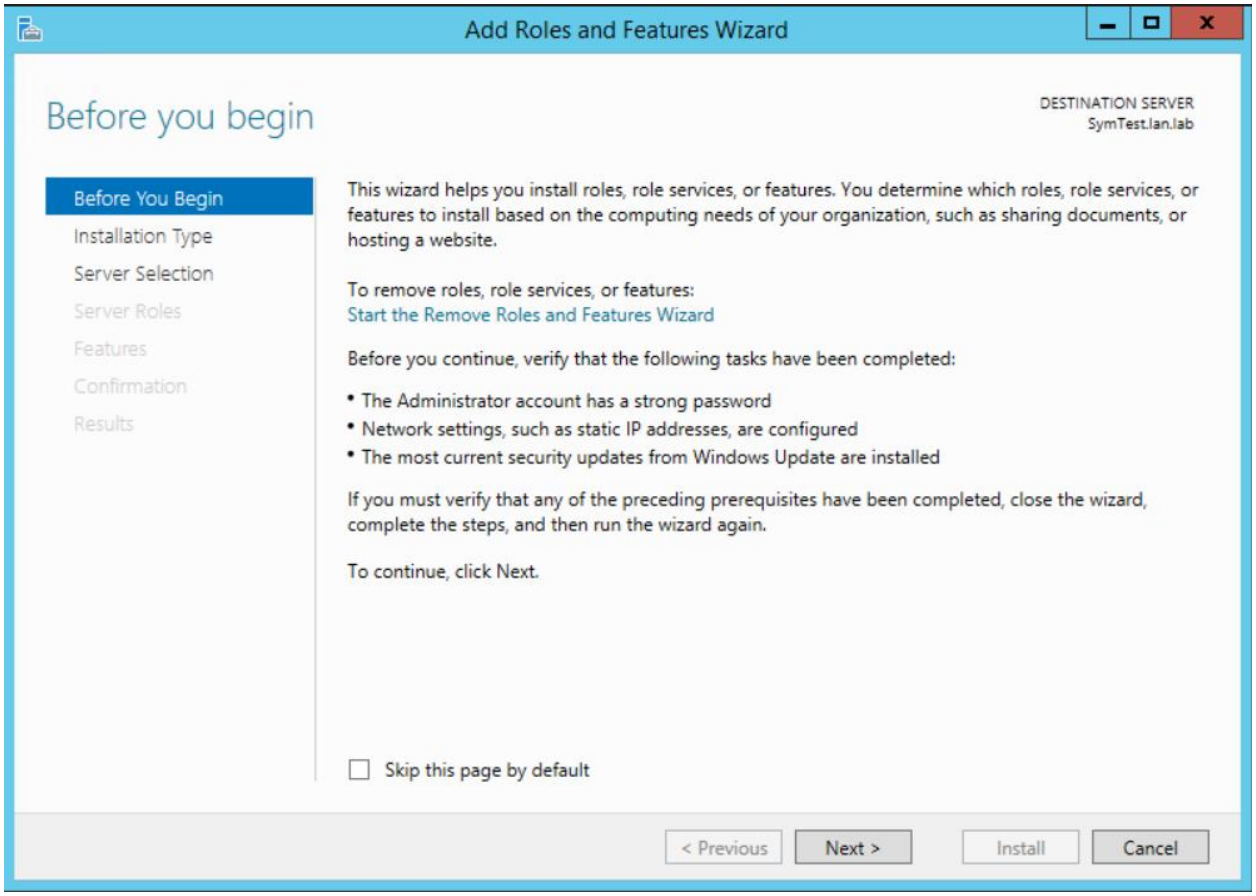
- Below are high level instructions for installing Active Directory services (ADDS) on a Windows 2012 R2 server.
- It is recommended to have 2 servers running AD for redundancy. Ensure the servers are up to date with patches and have meaningful hostnames as per their role. Begin by configuring a static IP address on the network interface of your server. Since the server will also act as DNS server, for DNS server field you can use local host address 127.0.0.1



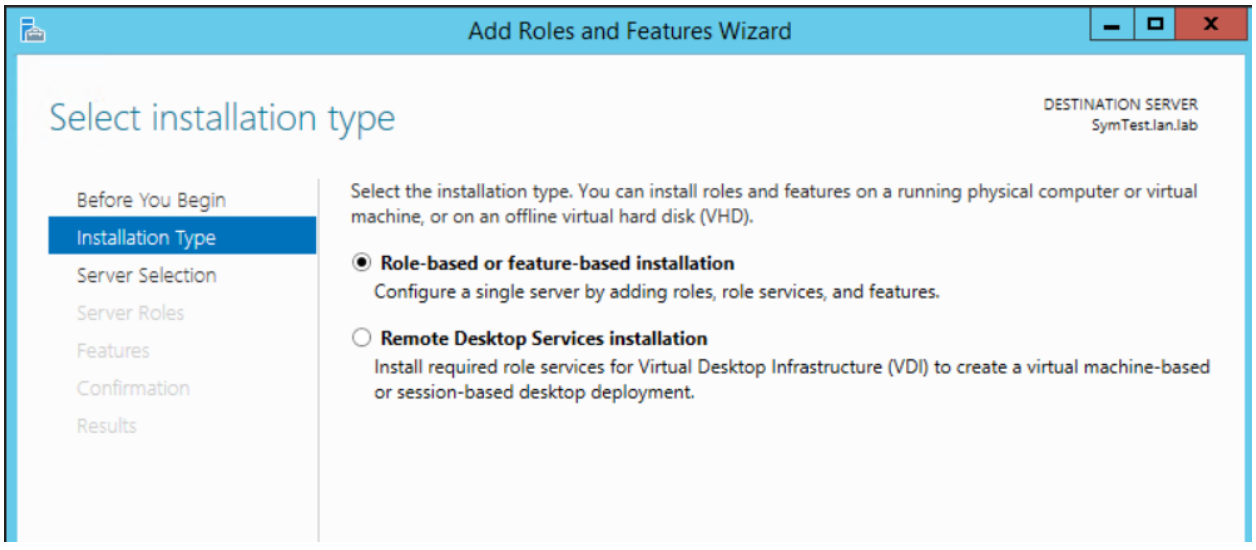
- Launch "Server Manager" and click on "Add Roles and Features"



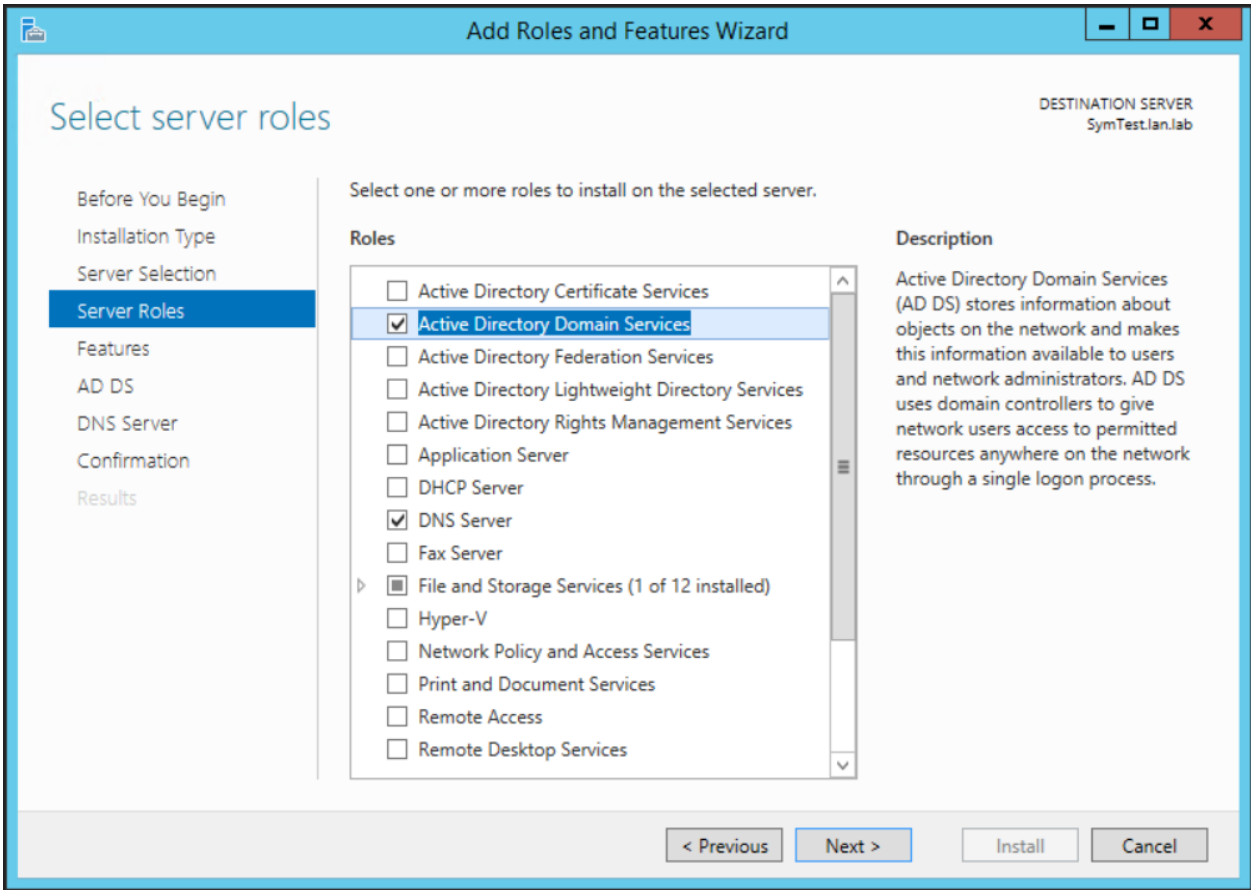
- Click "**Next**" at the first page



- Select "**Role Based or Feature Based Installation**" under Installation Type



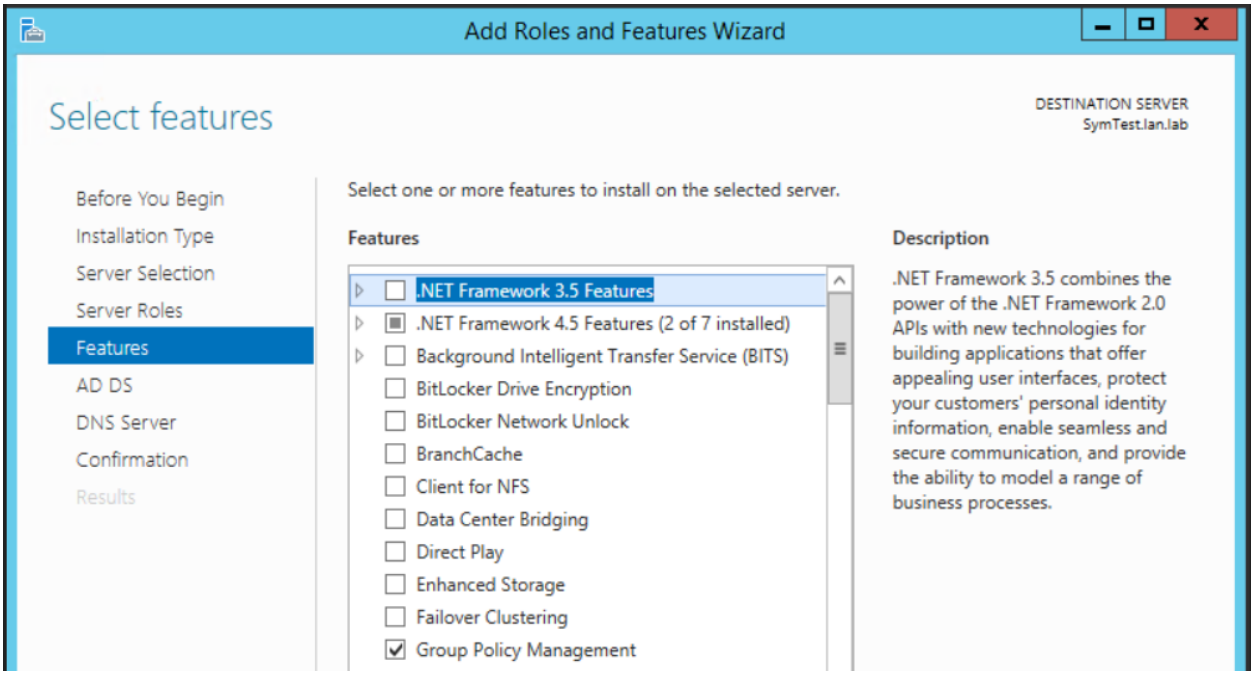
3867 • Select "**Active Directory Domain Services**" and **"DNS Server**" to install. Click Next



3868

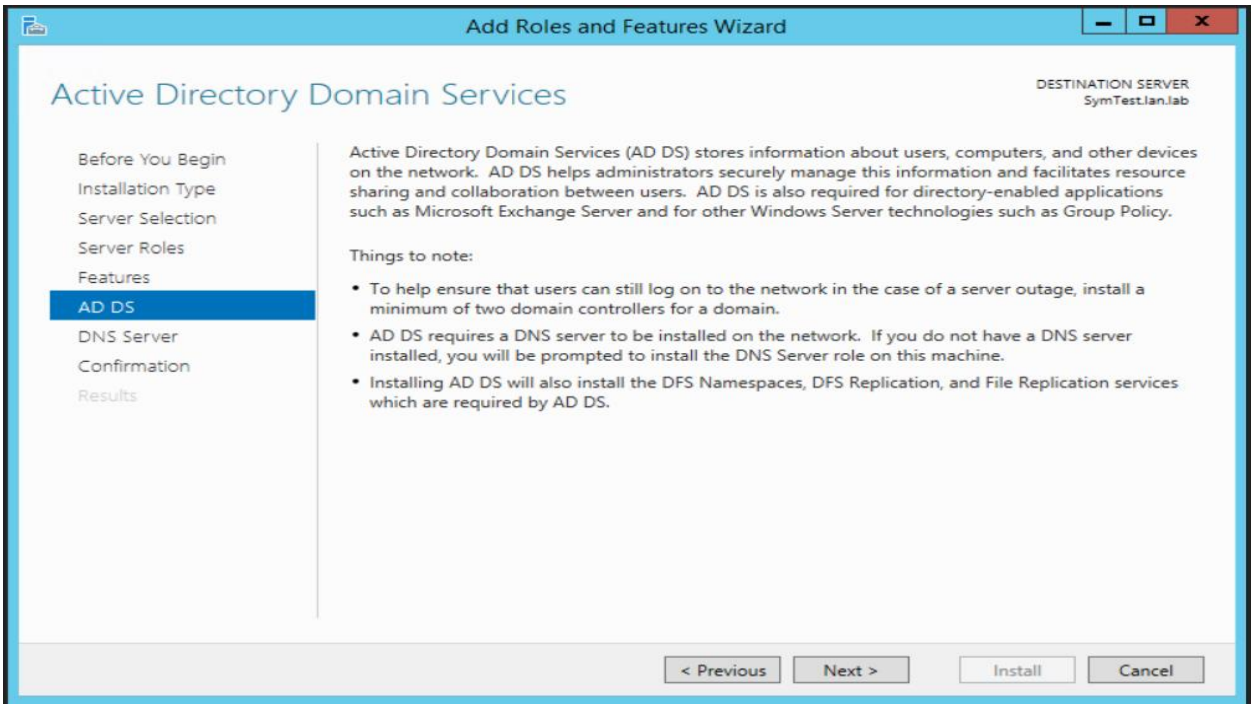
3869

3870 • Under "**Features**", leave the default options selected and click **Next.**



3871

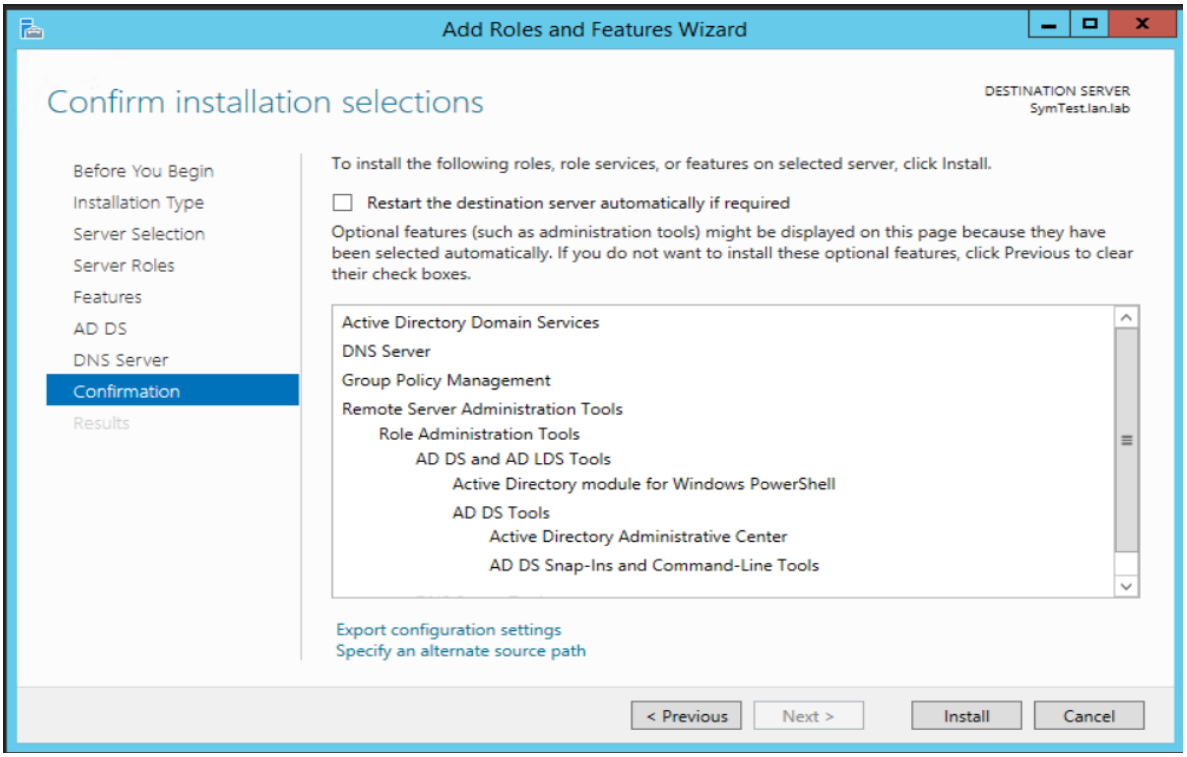
3872 • On the "**AD DS**" page, click **Next**. Likewise, on the "**DNS Server**" page click **Next** as well.



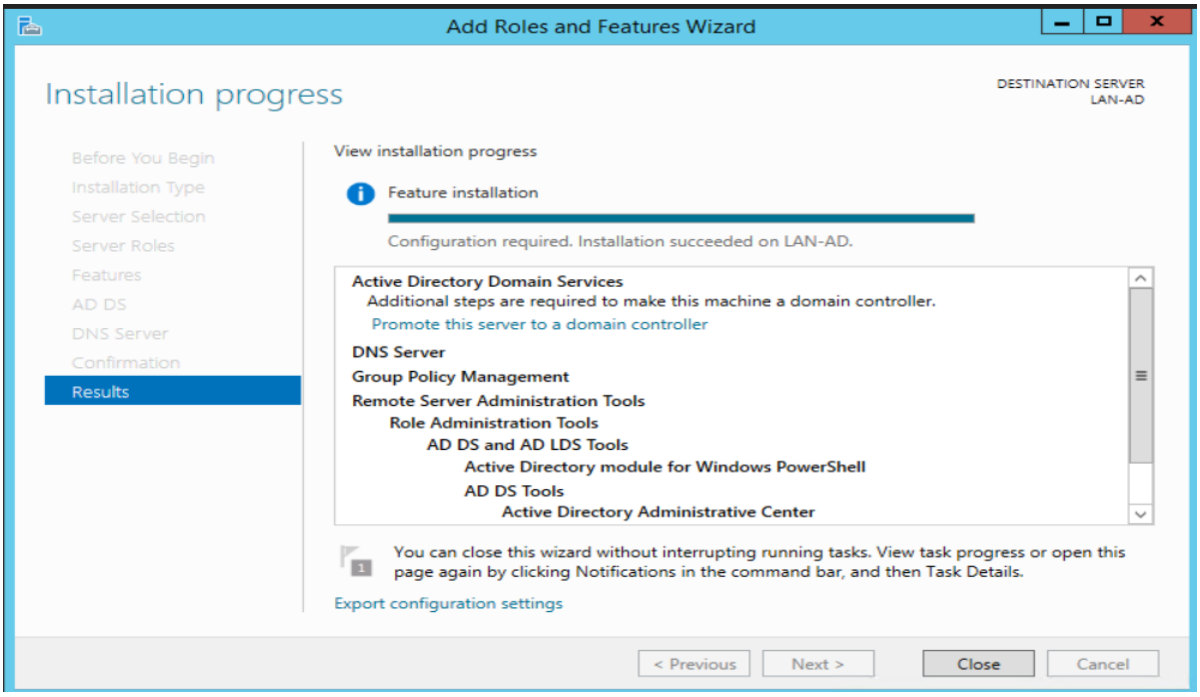
3873

3874

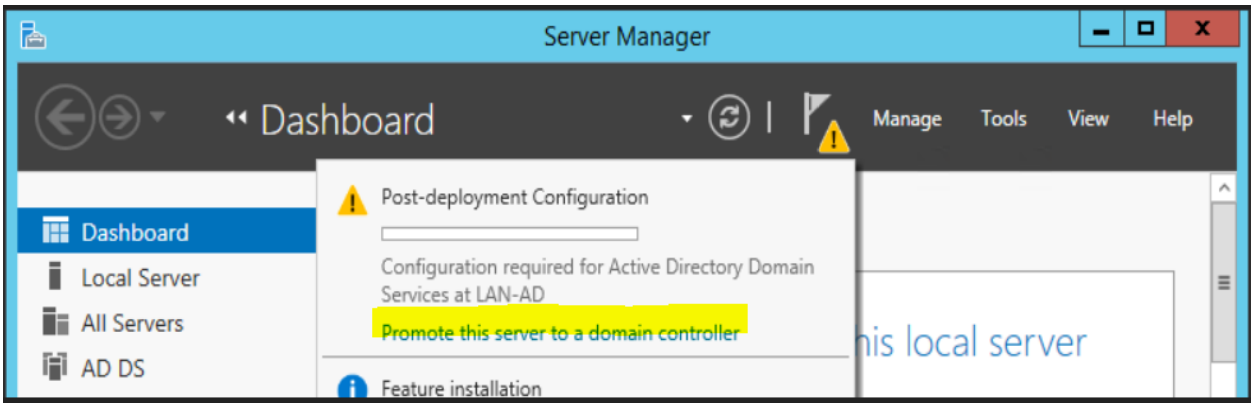
- Verify your settings on the "**Confirmation**" page. Click **Install** to proceed.



- The installation process will run and will show an "Installation succeeded" message upon completion. Hit **Close** button.

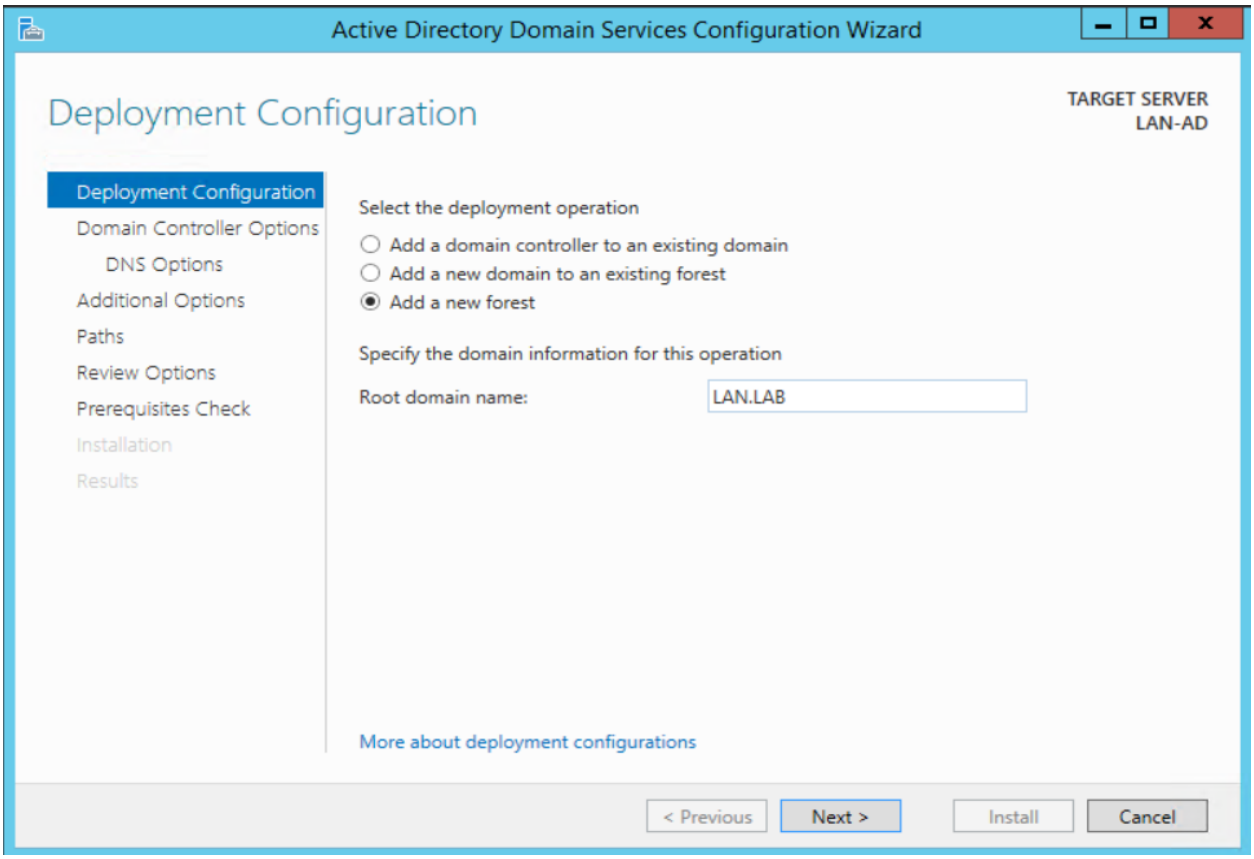


3880 ➢ Launch "**Server Manager**" again and click on "**Promote this server to a domain**
3881 **controller**"



3882

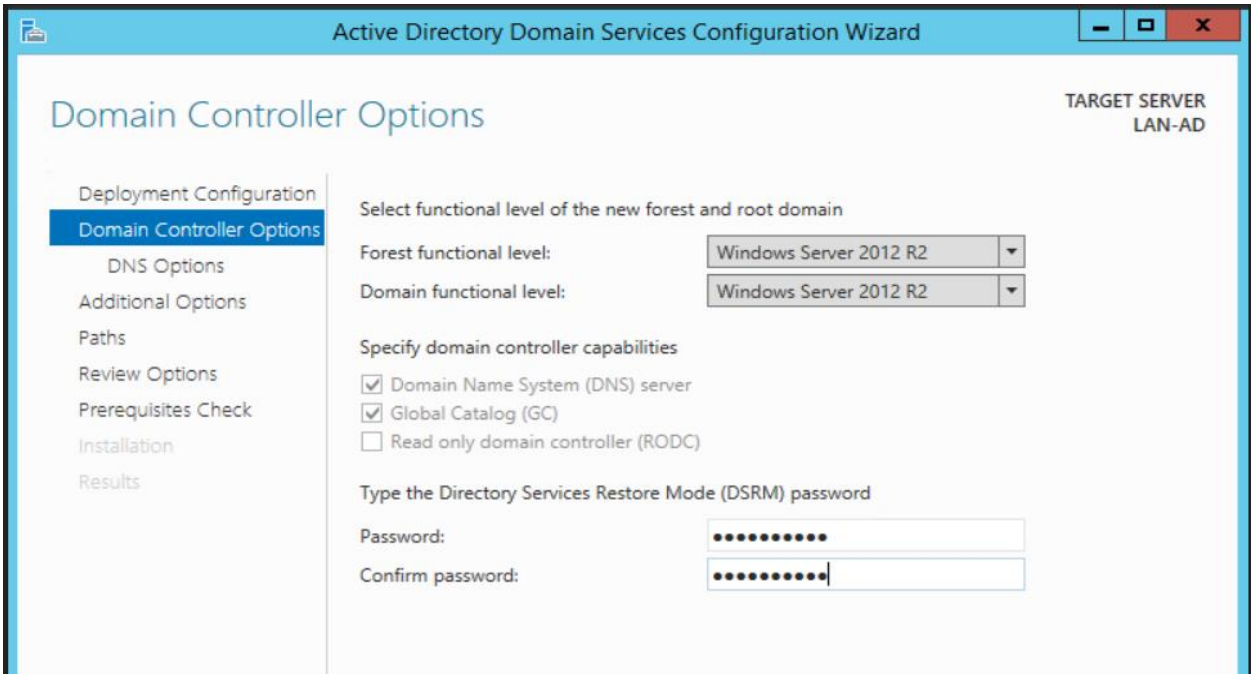
3883 • On the "Deployment Configuration" step, select "**Add a new forest**" as this would be a new
3884 domain controller in a new forest. Mention a Root Domain name as applicable to your
3885 environment.



3886

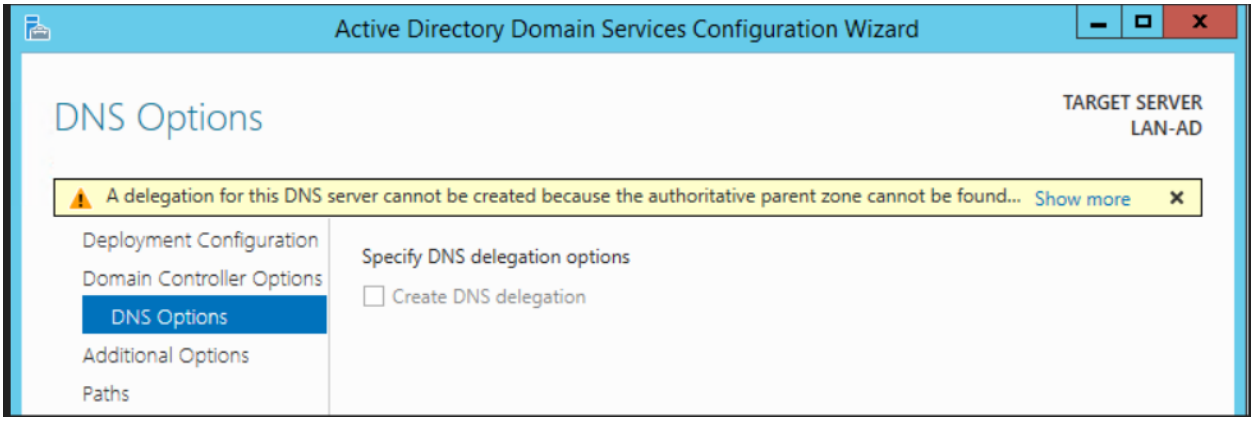
3887

3888 • Set a Directory Services Restore Mode password in the next step. Click **Next**



3889

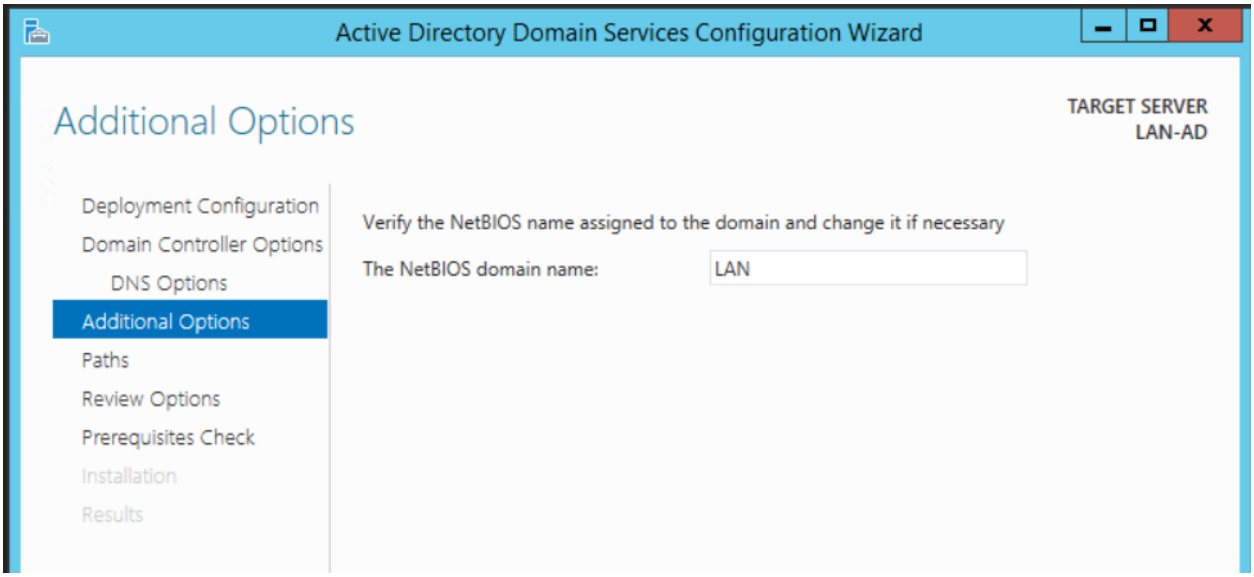
3890 • Under "**DNS Options**" leave the default options selected. Click **Next**



3891

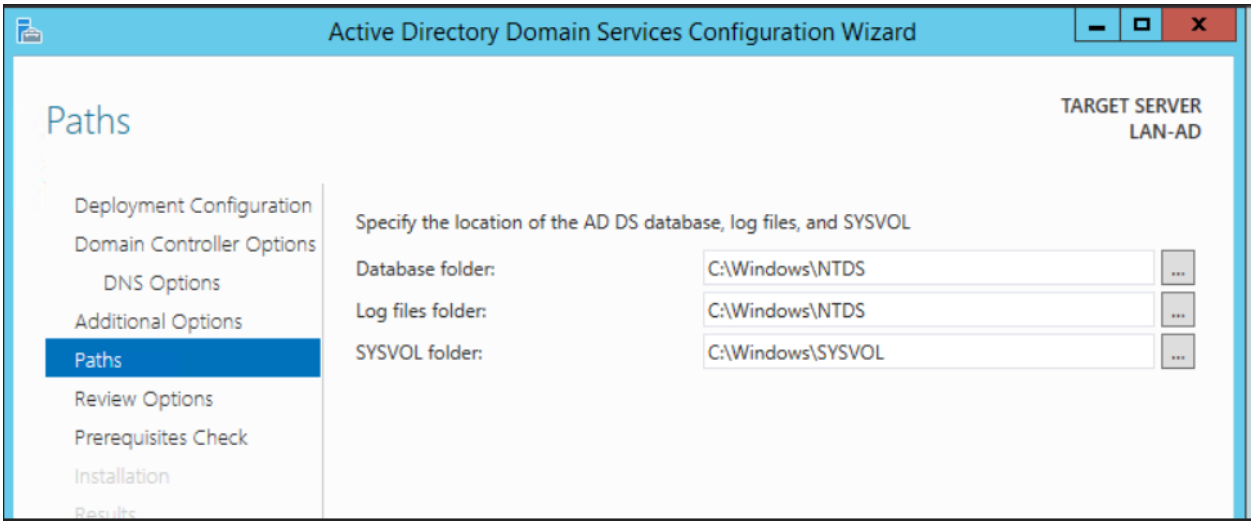
3892

3893 • Under "**Additional Options**", confirm the NETBIOS domain name. Click **Next.**



3894

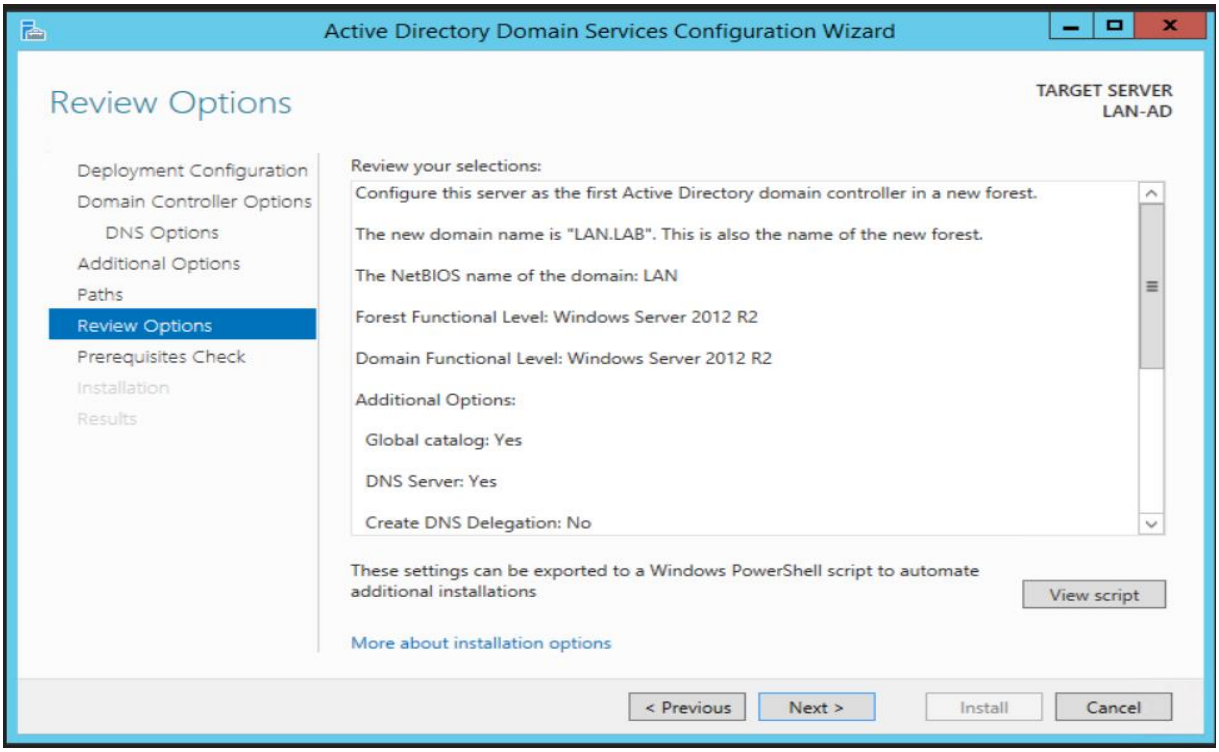
3895 • Under "**Paths**", leave the default folder paths as it is. Click **Next**



3896

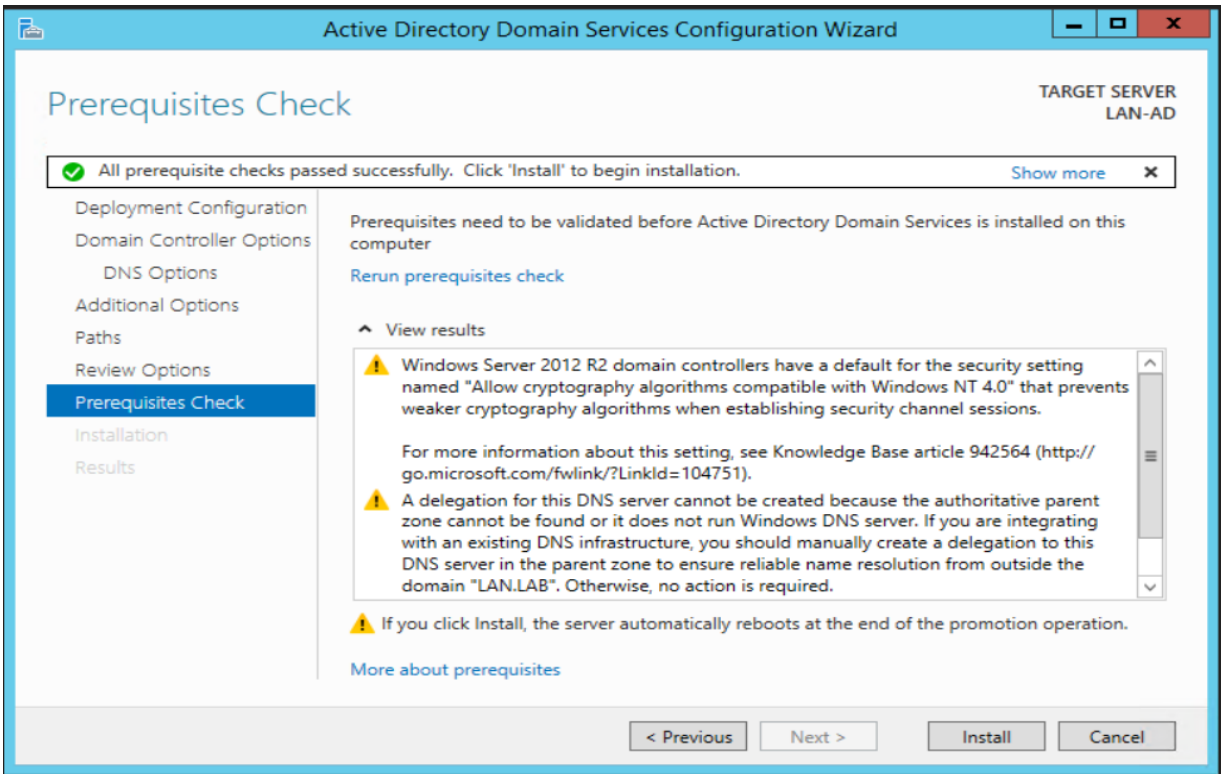
3897

3898 • On the "**Review Options**" page, confirm all the settings and click **Next**.



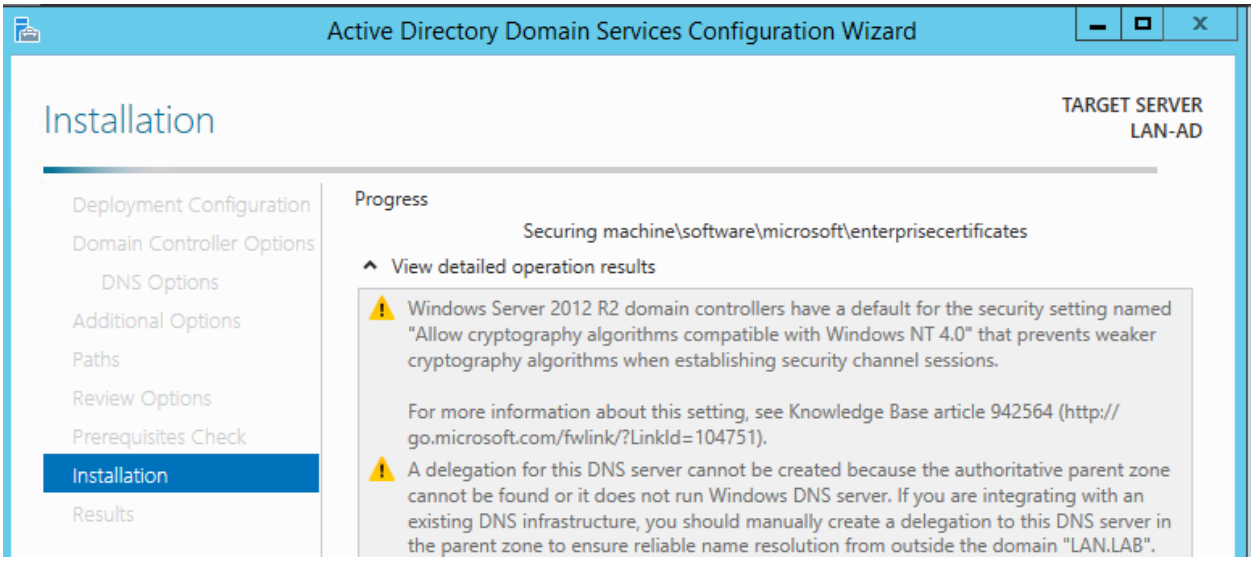
3899

3900 • On the "**Prerequisites Check**", click Install to launch the installation process.

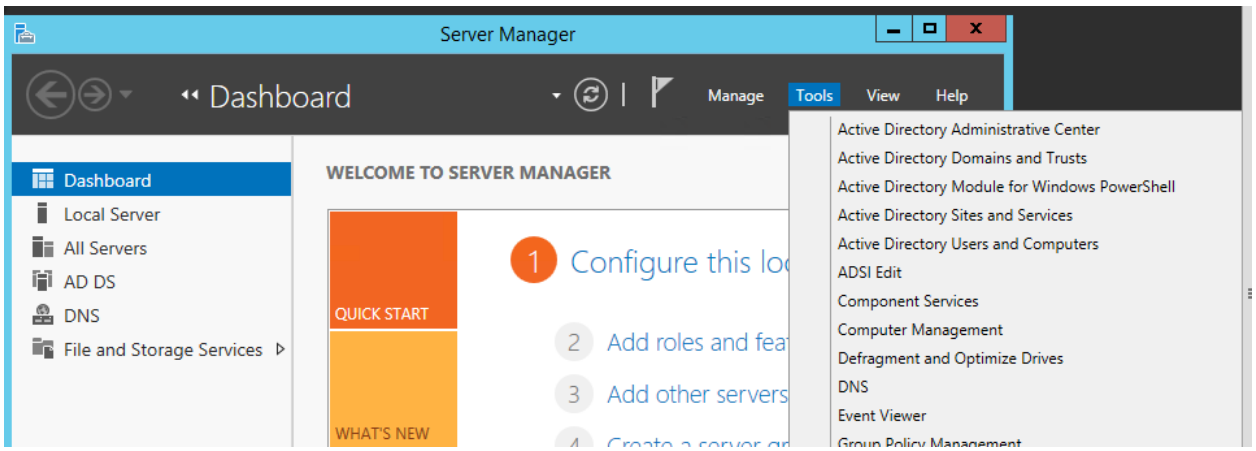


3901

- The installation process will now run displaying the Progress bar. Upon completion, the server should auto reboot.



- Upon reboot, login with domain administrator credentials. Open "Server Manager" and click on "Active Directory Users and Computers" under Tools to manage your AD.



Configurations:

- All windows systems were domain joined to the AD domain in the Cybersecurity LAN network. The initial domain join process is a onetime task and involves a system restart. In addition to authentication piece, the Domain Controllers also have DNS role installed. They also act as internal DNS servers. Any system that is joined to AD, will automatically create a DNS record for itself. For any system that isn't joined to AD such as a switch or a router the DNS record for these would have to be manually created.

- The procedure to integrate or join Windows machines to AD can be found here.

- Once the machines were domain joined, different user accounts with varying levels of privileges were provisioned depending on the role i.e. machine operators, process owners and service accounts. On Windows systems, the accounts used by the process owners were granted administrator privileges on each Windows system by adding them to the local Administrators group while the operator user accounts were only granted "Remote Desktop" rights. The individual user accounts are subjected to a password policy whereas the service accounts are set to not expire.

- On the OPC server, we are running a Matrikon OPC server. The Microsoft Distributed Component Object Model (DCOM) service plays a vital role in integration the OPC server with AD. Having the correct DCOM settings in place when using AD is critical for plant operations. We have followed the steps documented in this Matrikon OPC guide [21] to apply the necessary DCOM settings. Please refer to the section below "**OPC Server DCOM Configuration**" for our settings.

- For using AD authentication against network devices, we leveraged Microsoft Network Policy Services (NPS) to use as a Radius server along with AD DS. Within the Radius server, a connection request policy and a network policy was created for each network device. Please refer to the section below "**Radius Server Setup**"

- A physical network connection was made to the Management port of the Boundary Firewall This port was then assigned a static IP address from the Management subnet on each device so that it could communicate with the above Radius and AD server. Typically, each network device has an option to configure Radius authentication. In addition, we enabled the auditing feature on the DC to track for successful/failed logins. Once the setup is done, you should be able to use AD user accounts to login to your network devices.

OPC Server DCOM Configuration

Pre-requisites:

- All windows systems participating need to be domain joined to the AD server.
- Ensure all systems are getting their time synced from the AD server and verify the time on each server is consistent with the time on the AD (Domain Controller). Time sync is critical.
- Verify TCP port 135 is open between all OPC clients and the OPC server.

Shown below are the changes implemented

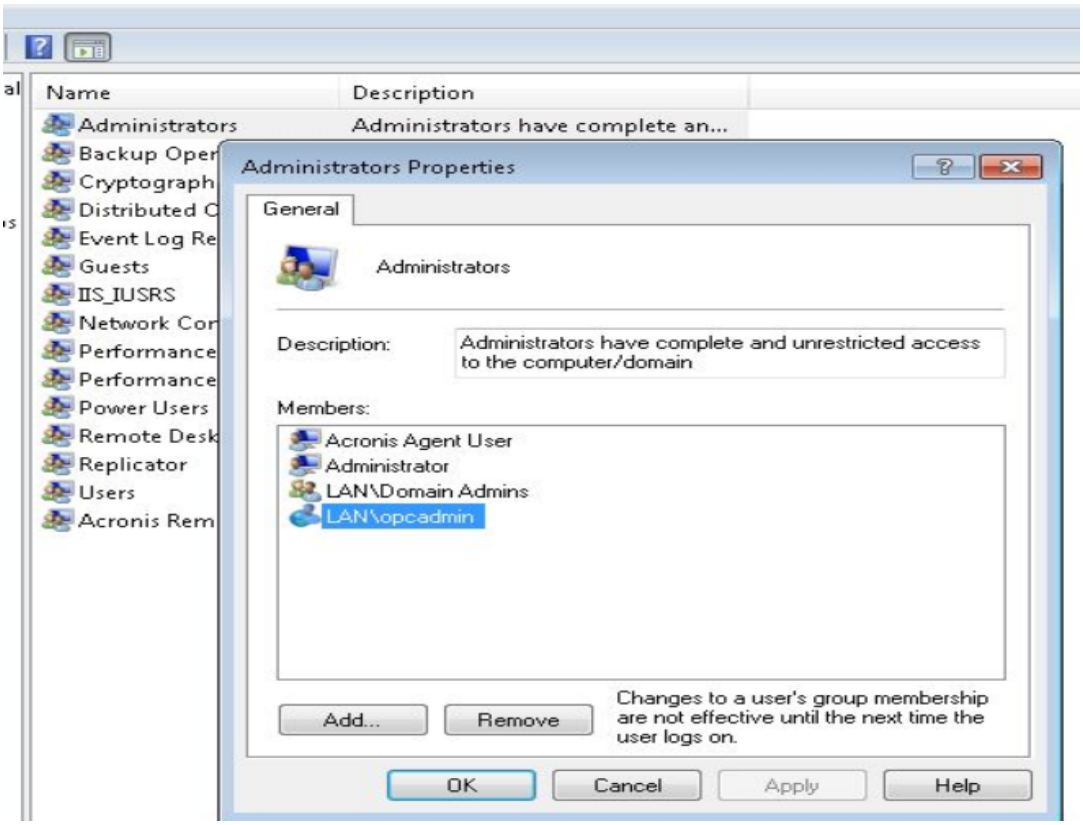
[21] Matrikon OPC DCOM Setup: https://www.matrikonopc.com/downloads/1128/whitepapers/index.aspx

- Created 2 domain users "**opcadmin**" and "**opcuser**" in our AD. The "**opcadmin**" will be the admin user. The other "**opcuser**" will be treated as a non-admin user and is optional to configure. Add the **opcadmin** user to the Local Administrators group on the OPC Server and client.

  Systems taking part in the OPC setup:

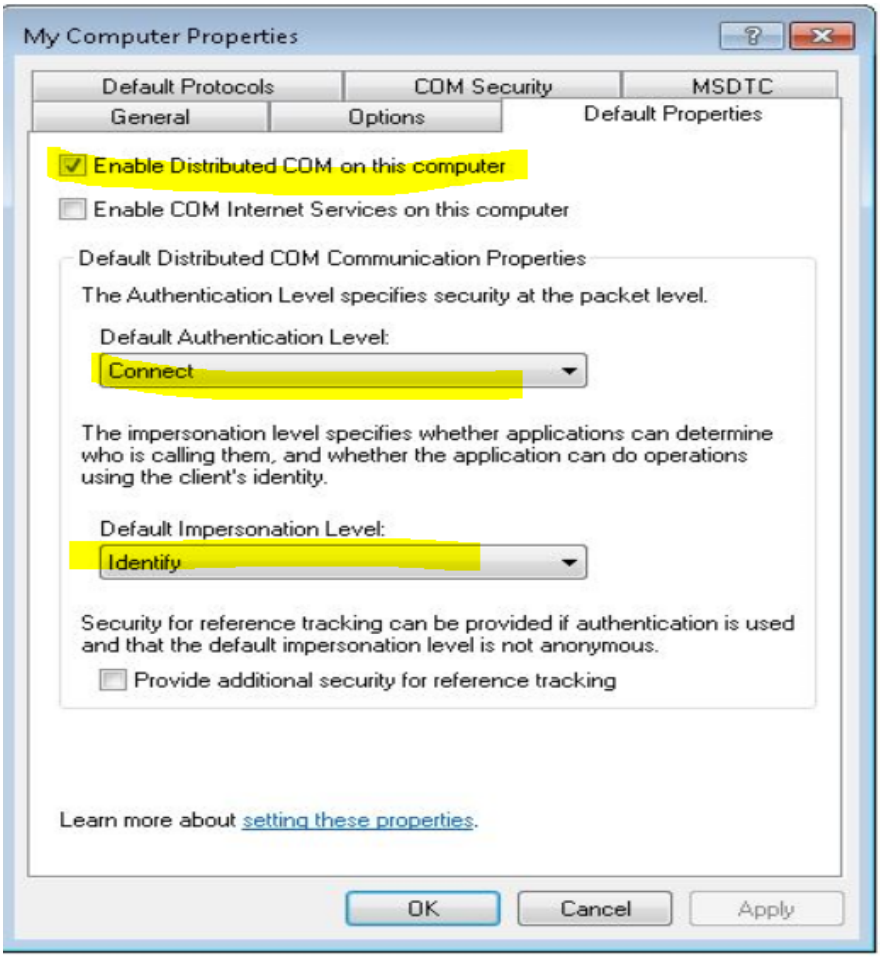
Hostname	IP address	Roles	Administrators
OPC Server	172.16.2.5	OPC_Server	opcadmin
Controller	172.16.1.5	OPC Server + Client	opcadmin, opcuser

  For example: Below is a snap from one of the OPC clients.

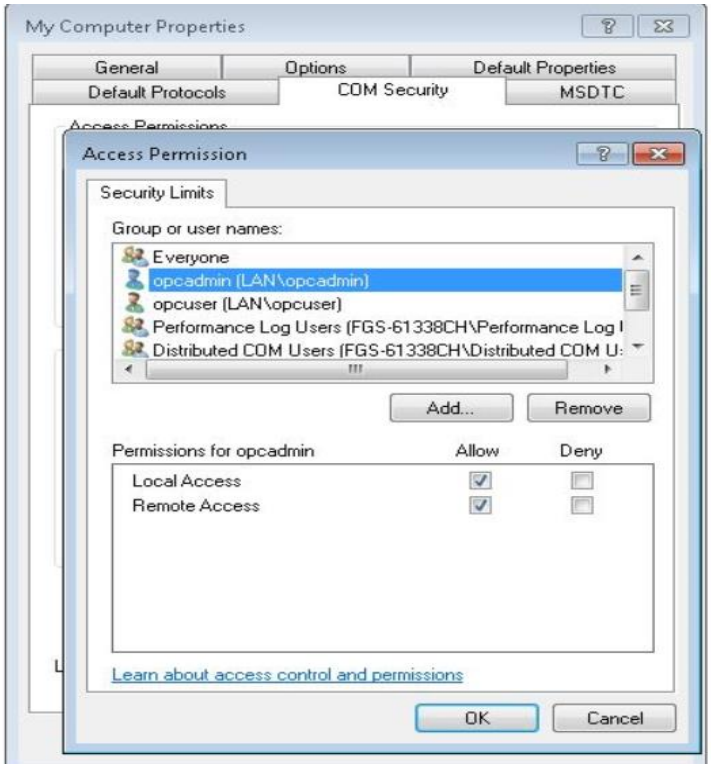


- On the OPC Client, make the following changes to DCOM properties. Launch the "Control Panel >> **Administrative Tools** >> **Component Services** snap-in to open the DCOM console. Alternatively, you can also run "**dcomcnfg**" (without quotes) command from command prompt to launch the DCOM snap-in.

- Expand **Console Root** > **Component Services** > **Computers**, Right-click **My Computer** and then click **Properties**. Ensure the settings are as follows

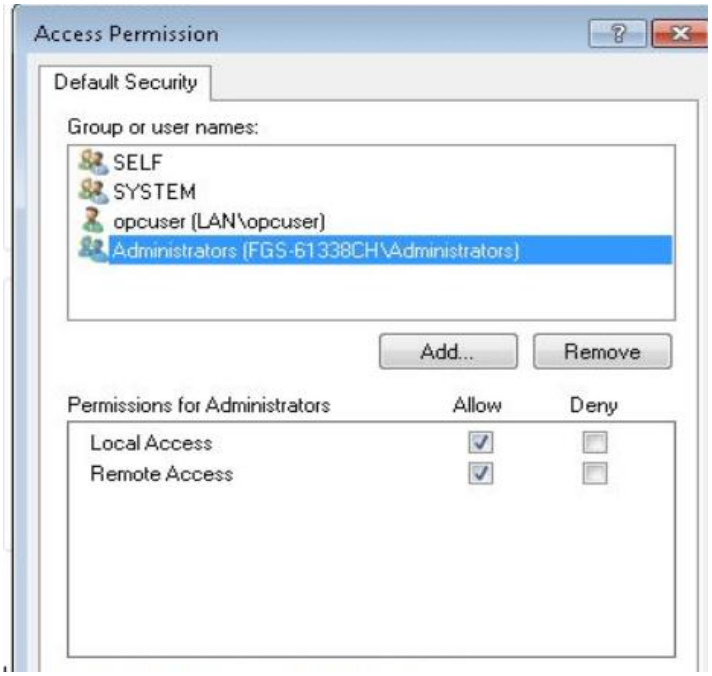


- Click on "**COM Security**" tab. Under "**Access Permissions**" >> "**Edit Limits"** button >> Add the opcadmin user to the list and check on the Allow boxes for both "**Local Access**" and "**Remote Access**" categories. You can add the "**opcuser**" as well if needed and grant it Allow permission for only "**Local Access**".

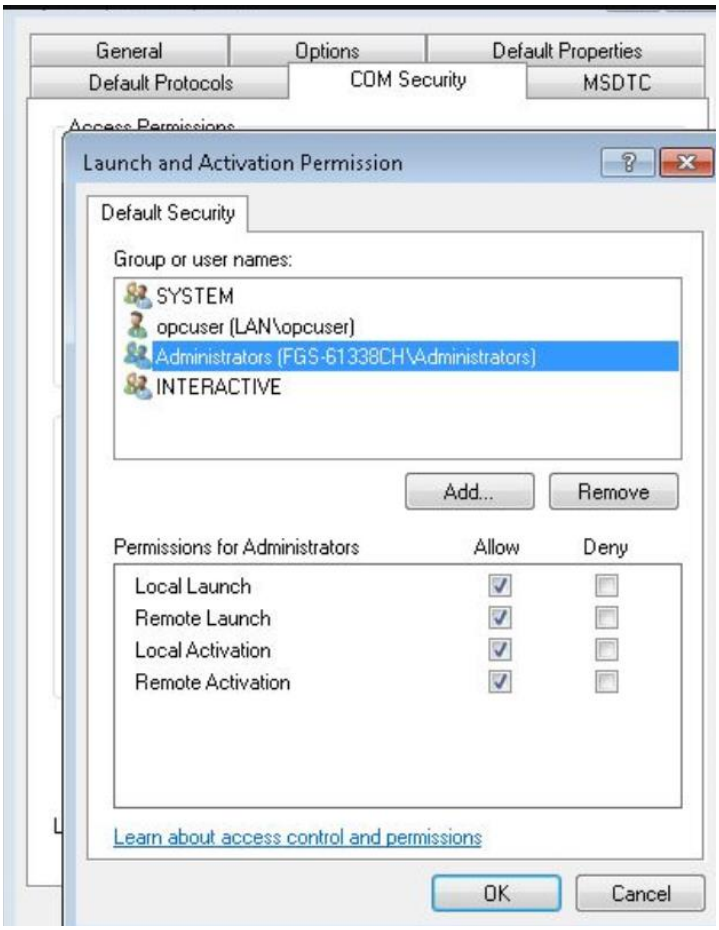


- Under "**Access Permissions**" >> "**Edit Default**" button >> Ensure that "<server-name>\Administrators" group has all the boxes checked. The **opcadmin** user was made part of this Administrators group earlier.

If you are adding the **opcuser**, grant it Allow permissions for "Local Access" only.

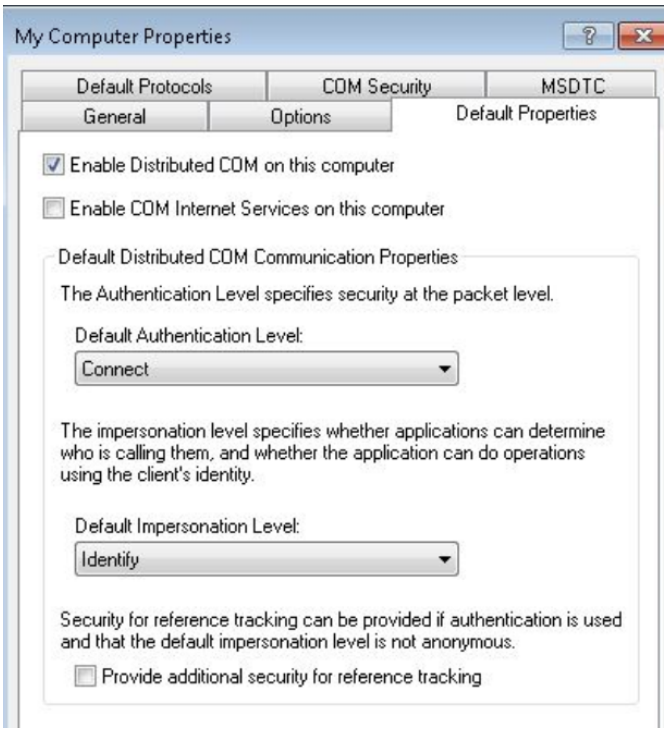


- Under the "**Launch and Activation Permissions**" >> "**Edit Default**" button >> ensure the "**Administrators**" group has **ALLOW** Permissions for all 4 categories. The other "opcuser" should have ALLOW only for "**Local Launch**"

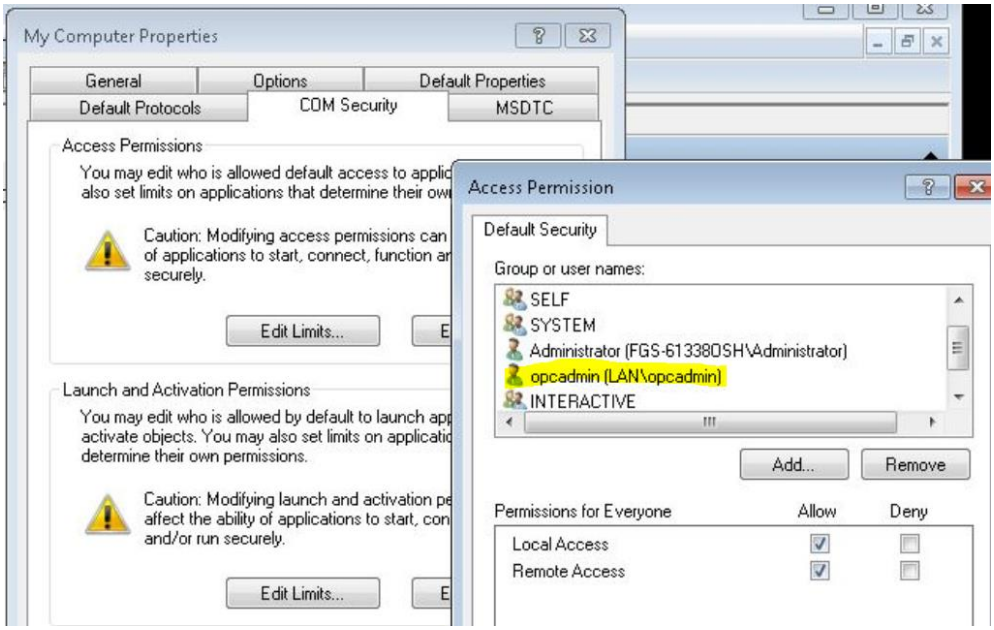


- This completes the OPC client-side configuration. Reboot the system after these changes are made. Repeat the process on each client.
- On each OPC Server machine, make the following changes to DCOM properties. Launch the "**Control Panel** >> **Administrative Tools** >> **Component Services**" snap-in to open the DCOM console.

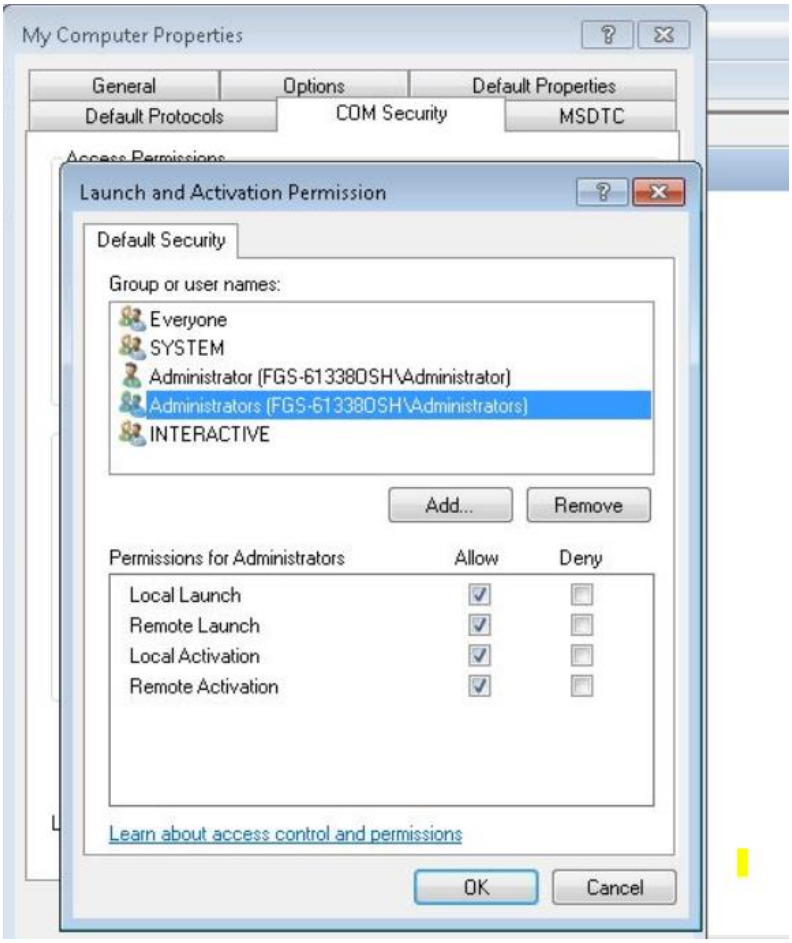
- Expand Console Root > Component Services > Computers, right-click **My Computer** and then click Properties. Ensure the settings are as follows



- Click on the "**COM Security**" tab >> **Access Permissions** >> "**Edit Default**" >> Add the **opcadmin** user and grant it ALLOW permissions for Local Access and Remote Access boxes.



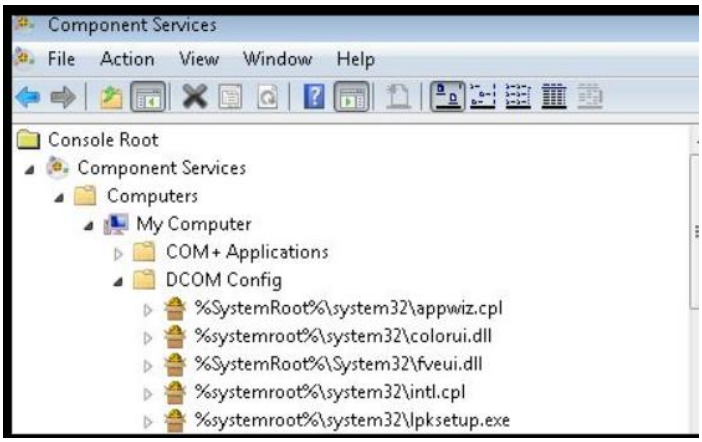
- Similarly, under "**Launch and Activation Permissions**" >> "**Edit Default**" >> Add the "Administrators" group and check on **ALLOW** Boxes for all 4 categories. If adding the other opcuser, it will only have Local Launch permissions.



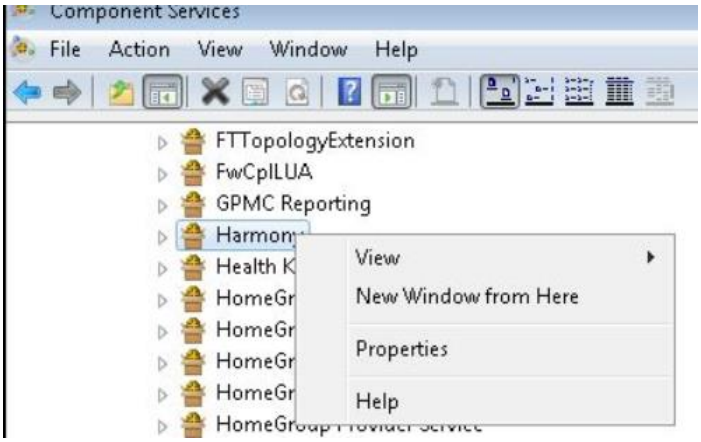
- Note down the names of the opc-server software installed in your environment and make the below shown DCOM changes on each of their application folders. In our case, the list of the s/w is as follows
  - Harmony (Installed on OPC Server)
  - RSLINX (Installed on OPC Server)
  - MATLAB (Installed on the Controller)

- We will start with the main OPC-Server and then move on to the Controller host. Launch the DCOM console and browse to **Console Root > Component Services > Computers > My Computer > DCOM Config**. In the list of applications in the right pane, right-click your OPC server (application folder) and choose PROPERTIES.

4022

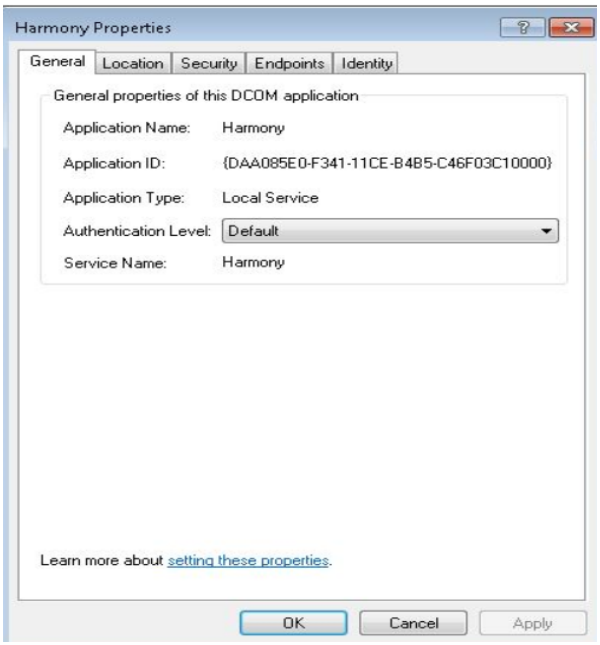


4023
4024

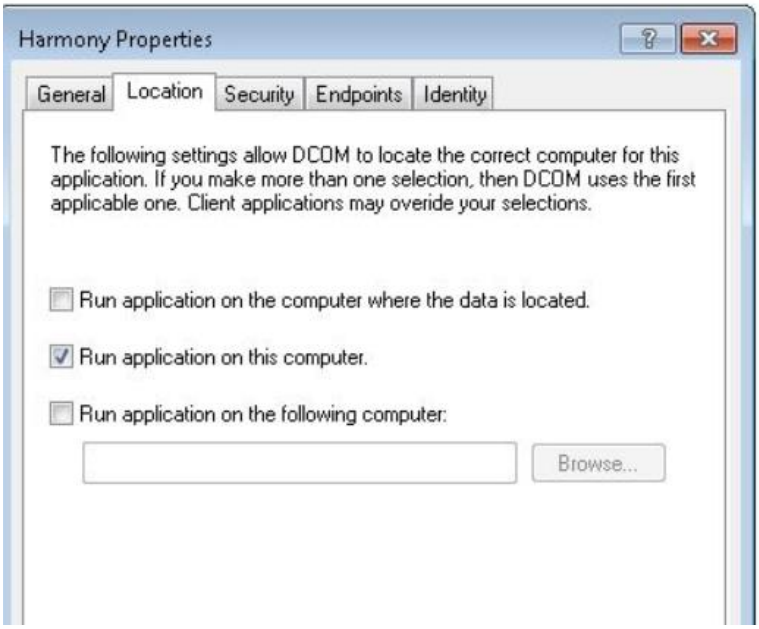


4025
4026

4027 For example, find the "**Harmony**" folder, right click to view its Properties. On the **General** tab,
4028 set **Authentication Level** to **Default**.



- On the Location tab, Select - **Run application on this computer**.



- On the Security tab, typically set permissions as follows:

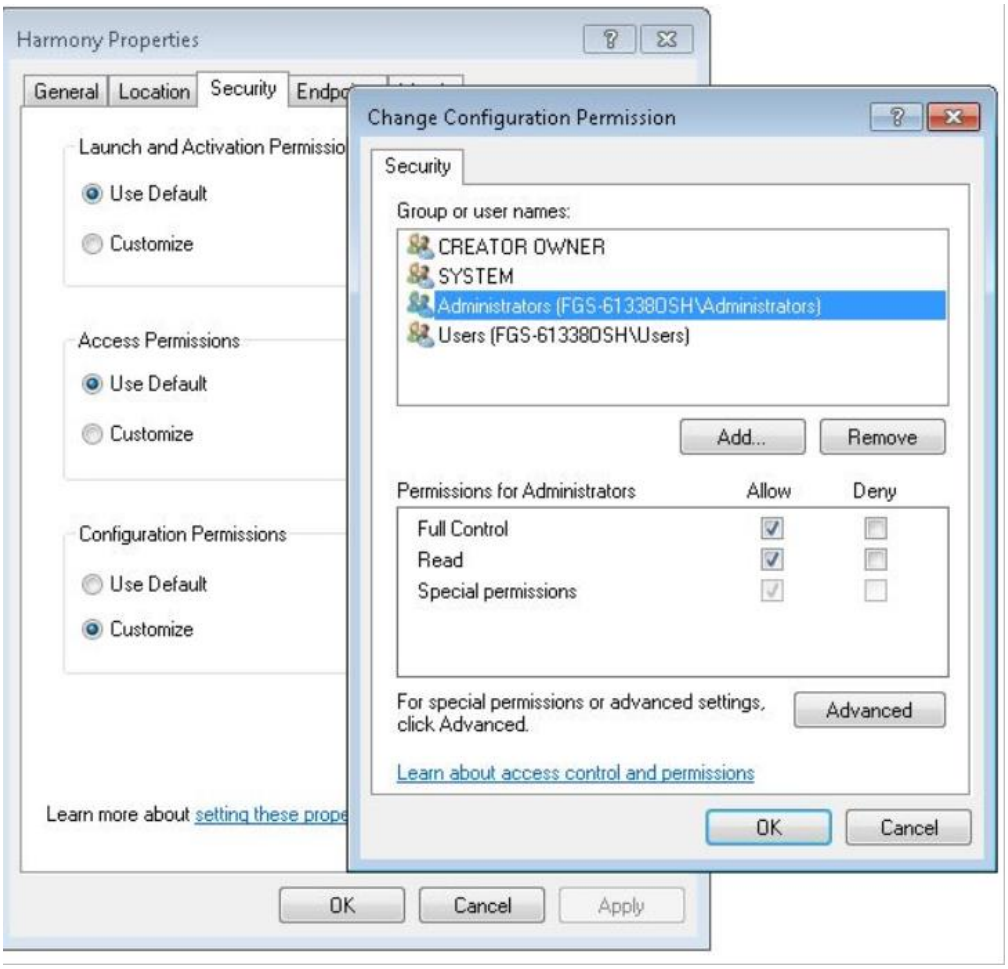
OPC users: (opcuser)

- Launch and Activation Permissions: Use System Defaults

- Access Permissions: Use System
- Configuration Permissions: Allow Read

OPC administrators: (opcadmin)

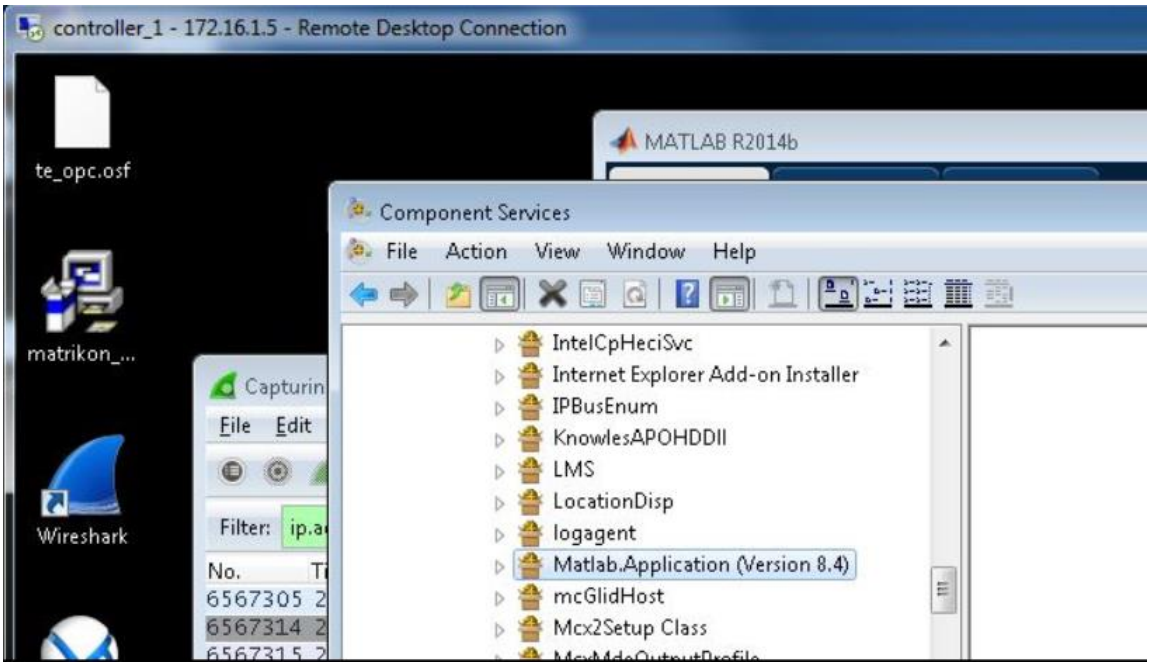
- Launch and Activation Permissions: Use System Defaults
- Access Permissions: Use System Defaults
- Configuration Permissions: Customize Full Control as shown below. (Note opcadmin is a member of Administrators group)

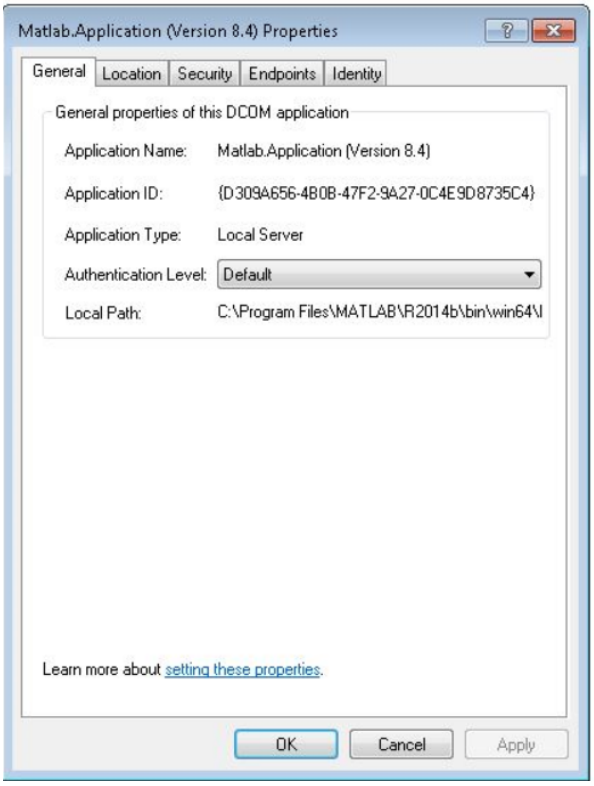


- On the Identity tab, choose the "This user" option and enter the user name and password for the AD user you created. We will select opcadmin as the user in our case. Click OK to save your settings. Reboot system.

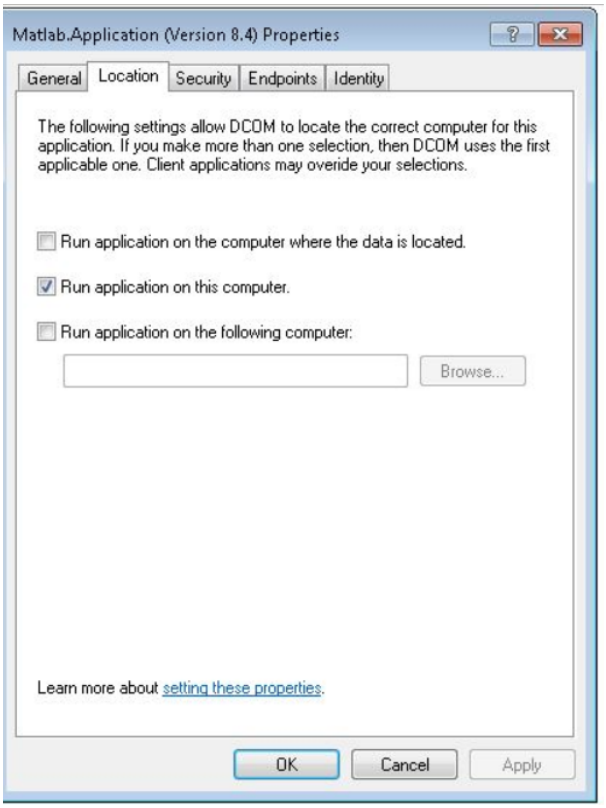
- Repeat the above steps 3.e.1 to 3.e.5 on the "RSLINX" folder (on the OPC Server) and on the MATLAB Application folder (on the Controller Server). Reboot system when done. Some screenshots for the MATLAB folder are shown below.

Note: These settings may not be necessary for the RSLINX folder and depends on the environment.

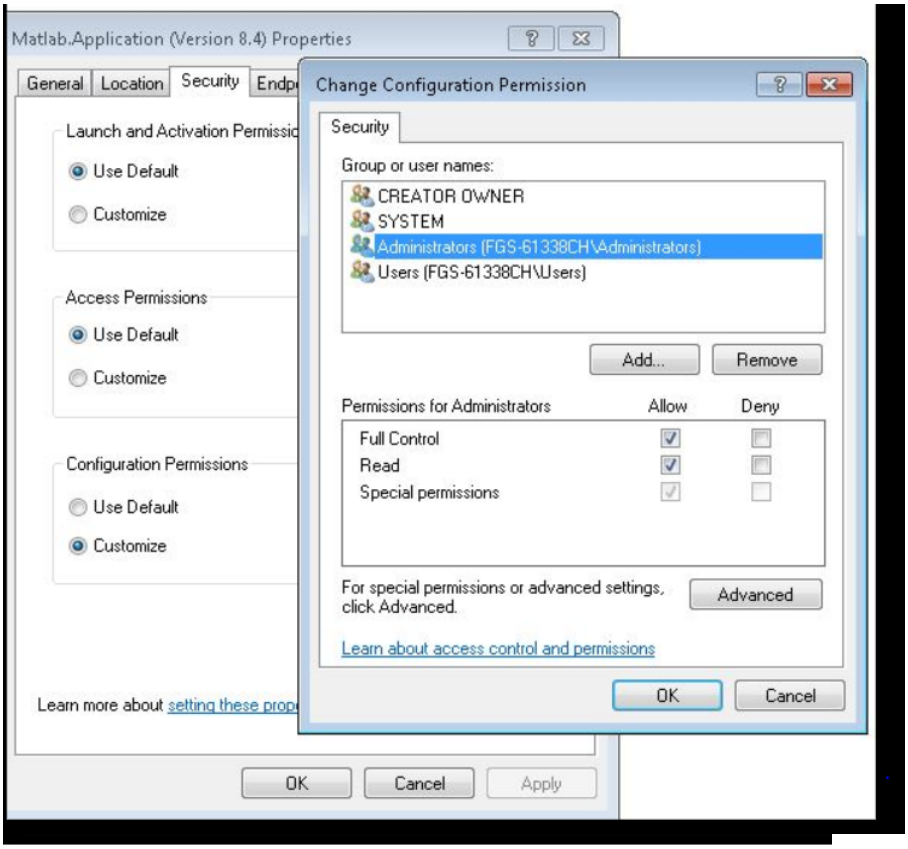




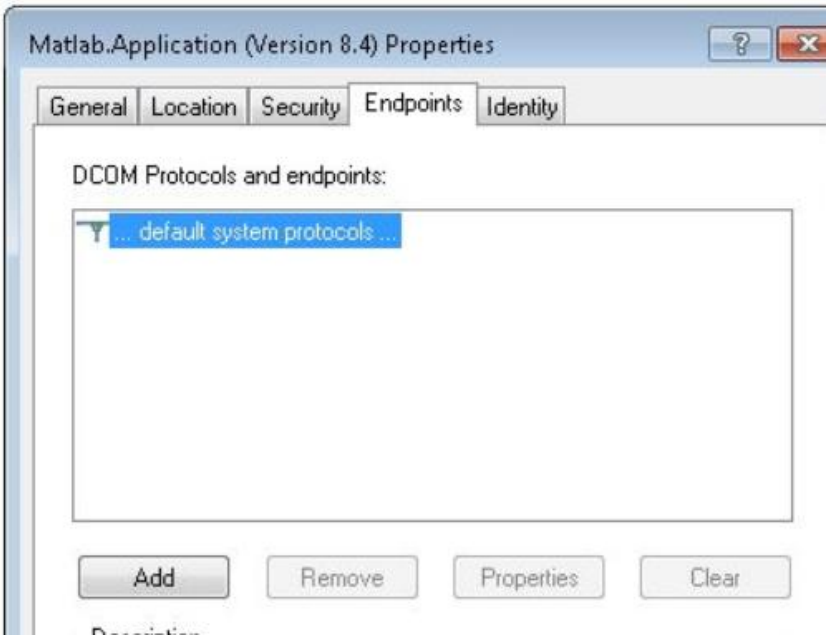
4065
4066



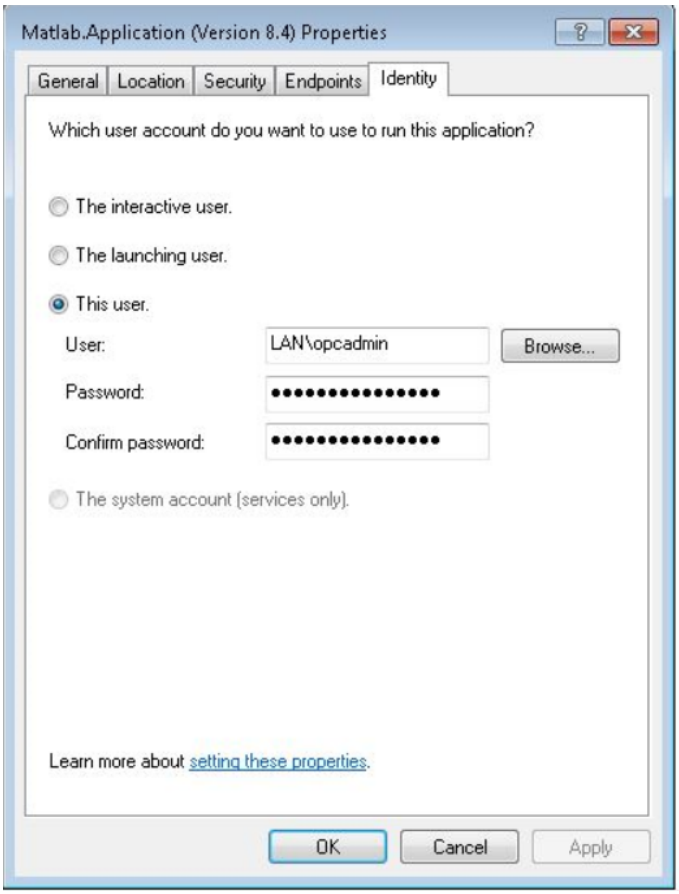
4067
4068



4069



4070
4071
4072
4073
4074
4075



Radius Server Setup

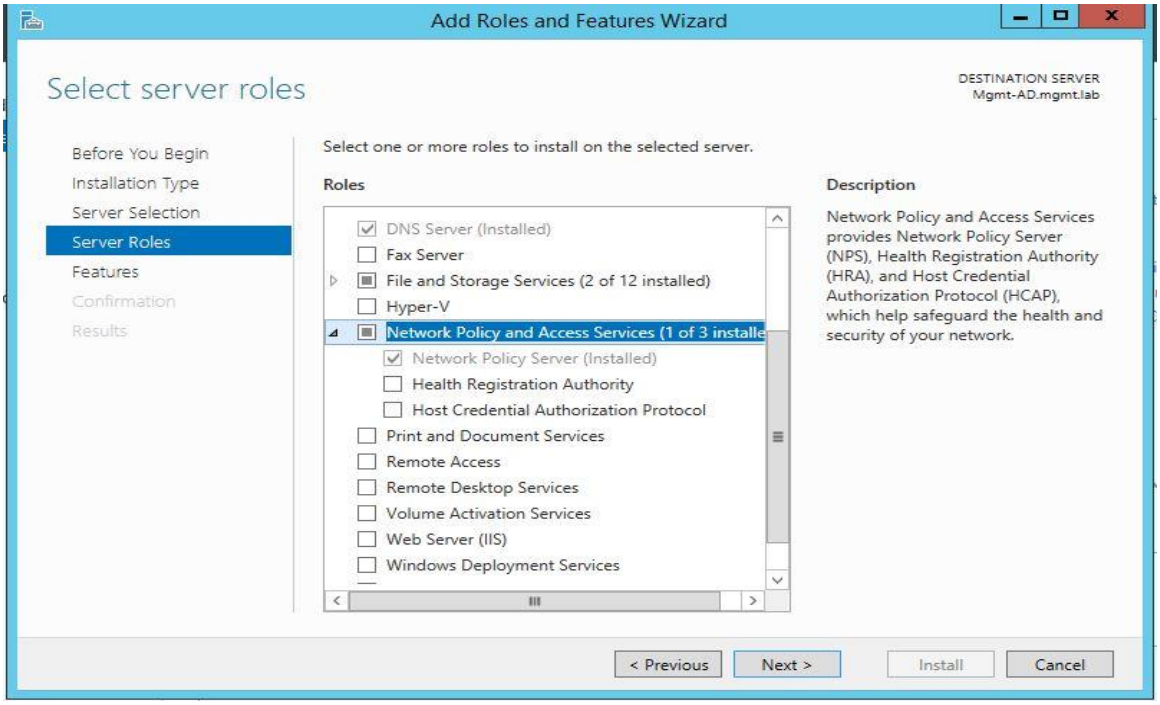
- A Windows 2012 R2 server running Active Directory and Windows Network Policy Server (NPS) was setup in the Management LAN to authenticate the boundary firewall and VPN users. Technically both the roles can be on the same server but its recommended to keep them separate for redundancy.

- High level setups
  - Setup the AD Server
  - Create an AD Domain
  - Setup the Radius Server
  - Join Radius server to the AD Domain
  - Register Radius Server with AD

Details of the AD Server and Domain in Management Network

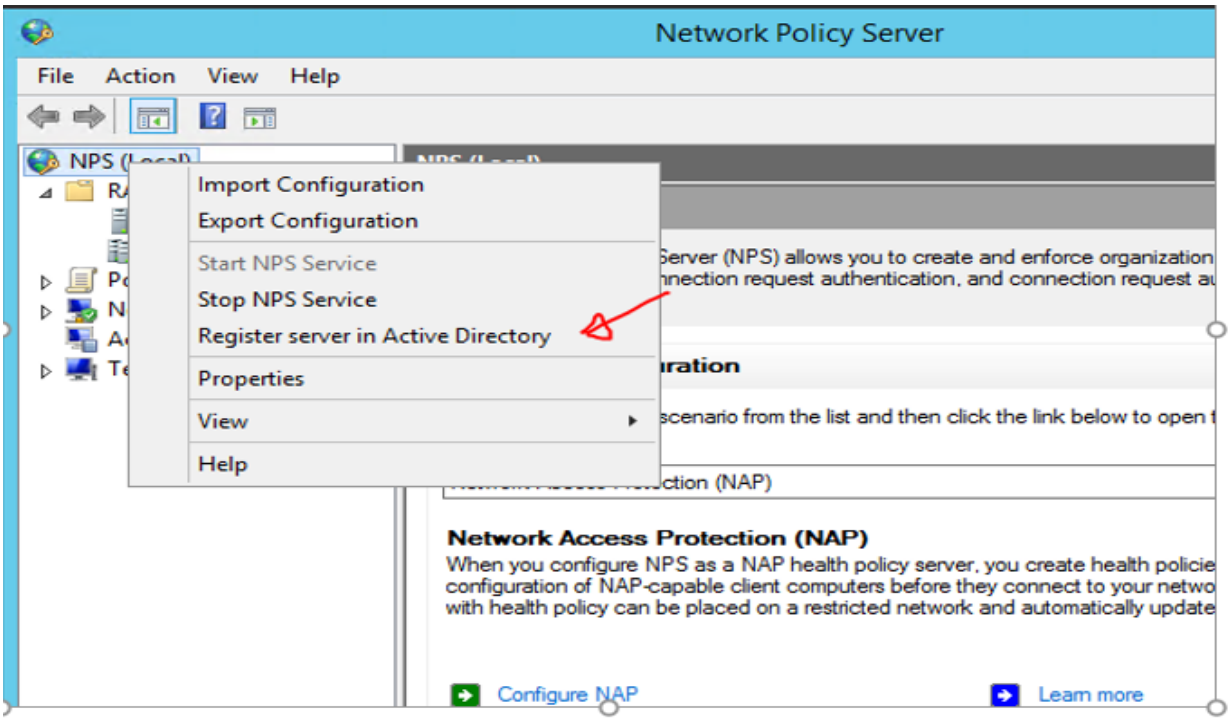
Hostname	IP address	Roles	Domain Name
Mgmt-AD	10.100.2.3	Active Directory, DNS, Network Policy Server (Radius)	Mgmt.lab

4091 • To setup Radius services on Windows 2012 R2, install the **Network Policy Server** role. This
4092 can be done from **Server Manager** >> **Add Roles and Features** Wizard as shown below



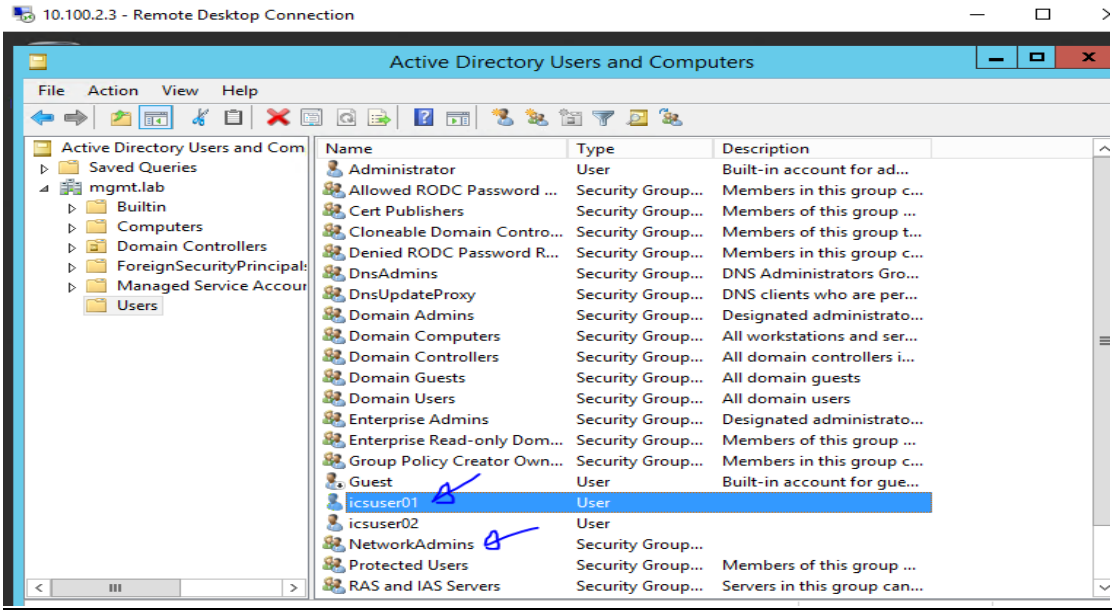
4093

4094 • Open the Network Policy Server Console, Click on **Register Server in Active Directory**
4095

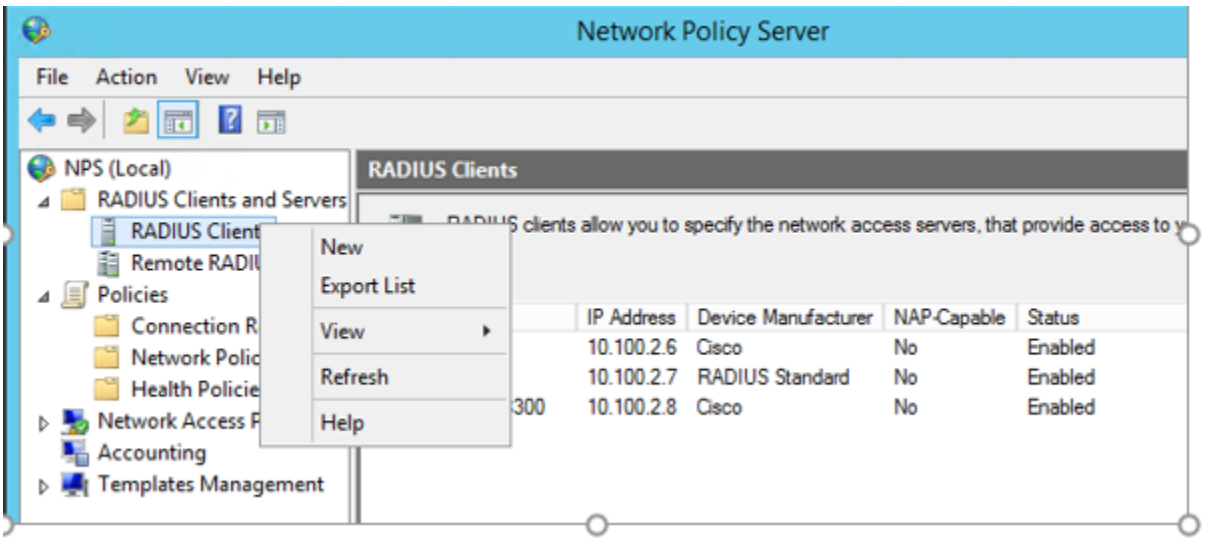


4096
4097

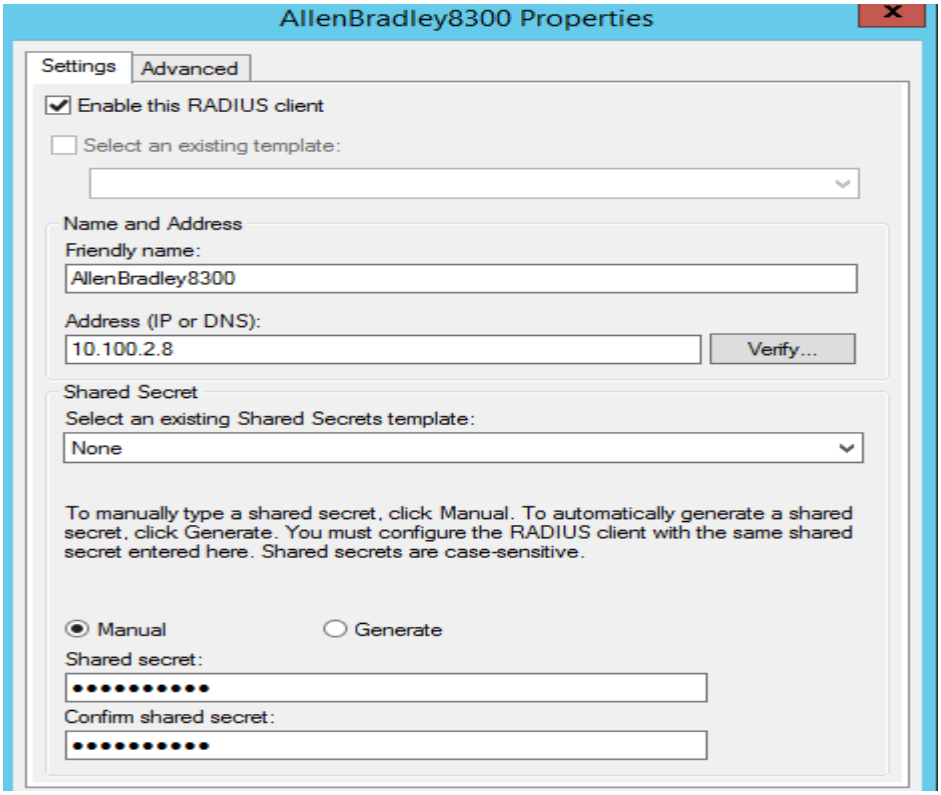
- Create user accounts in AD. A User account called "**icsuser01**" and a Security Group "**Network Admins**" were created in our **Mgmt.lab** domain. The **icsuser01 user** was added to the Network Admins group.



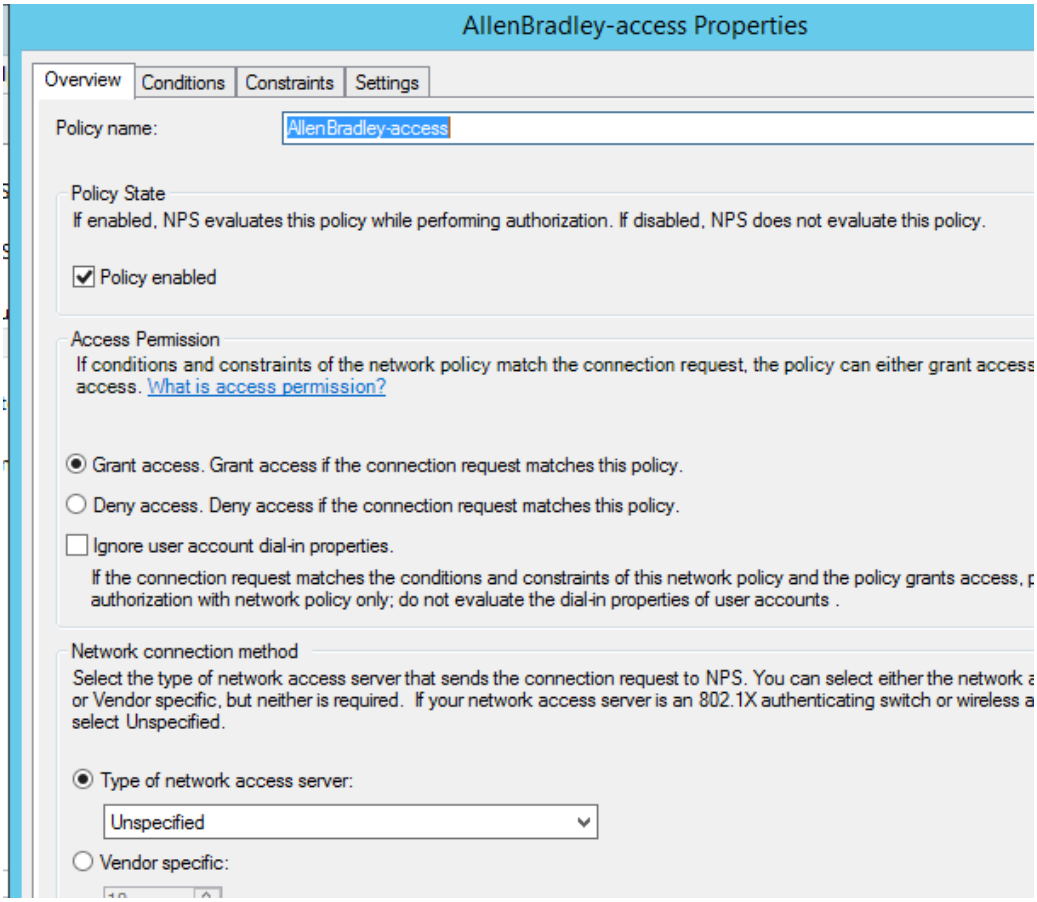
- Create Radius Clients and Policies in NPS:
  - Launch the **Network Policy Server** snap-in to create a Radius client for the Network Device you did like to integrate. A Radius client was created for the Boundary Firewall (Allen Bradley) of the Process Control System.



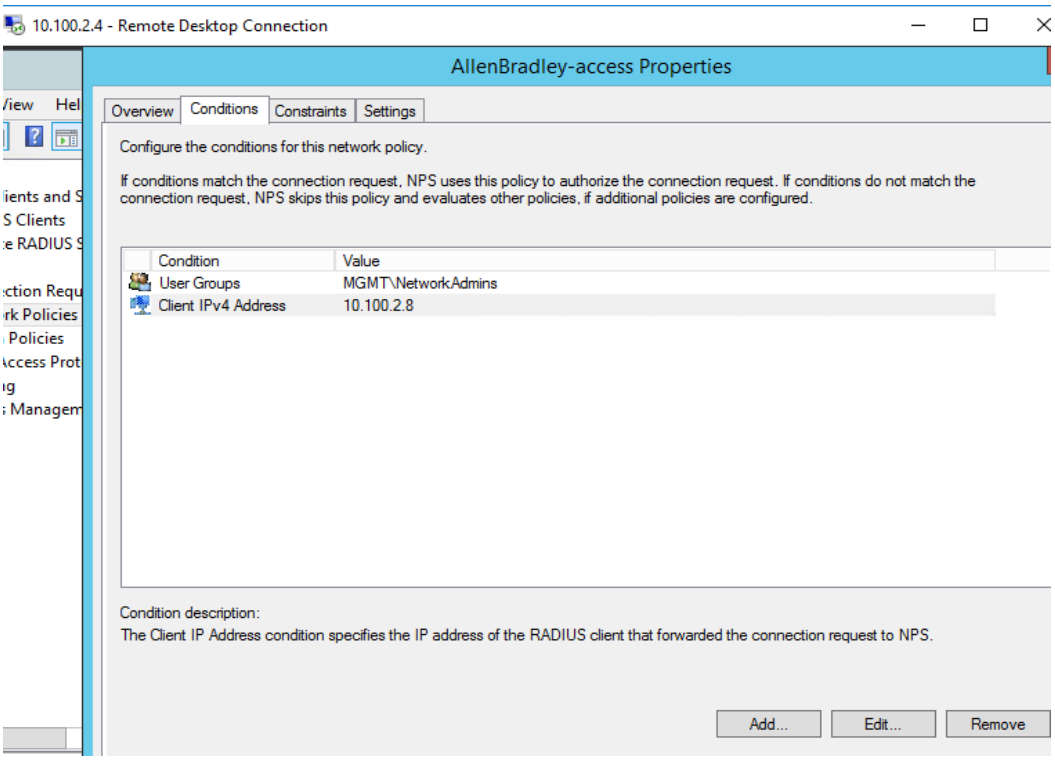
- Enter a matching name of the Network Device, IP address of the management interface and create a "passphrase ". Hit OK when done. This will create the Radius client. Make sure you can ping the Management IP of the network device from the Radius server



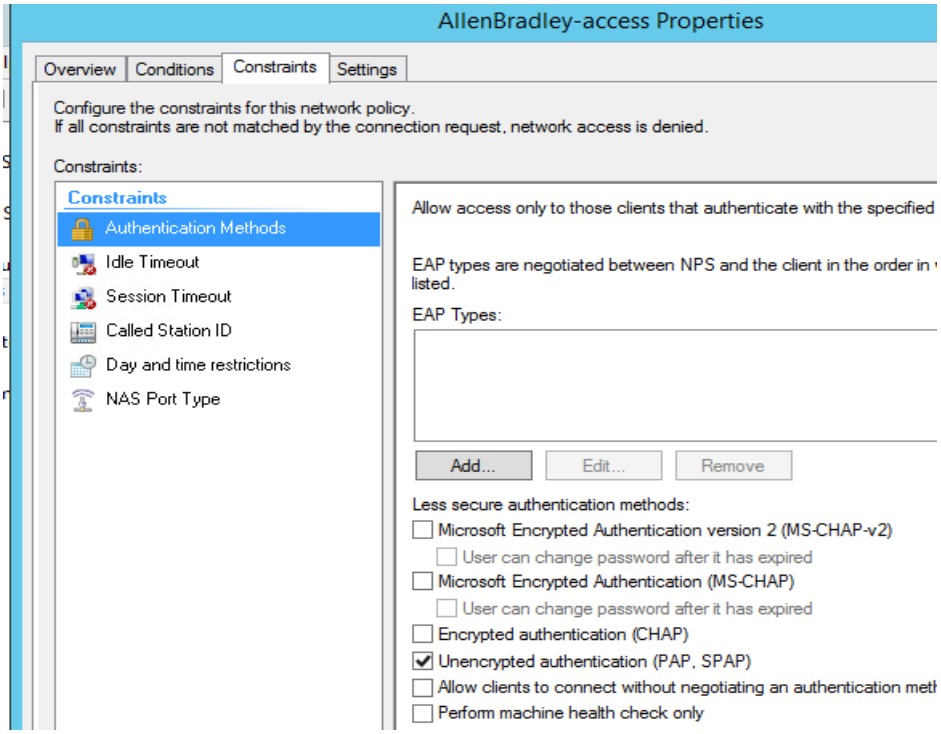
- Next, under Policies >> Network Policies >> Create a new policy for the radius client. The below image shows the network policy created for the Allen Bradley firewall



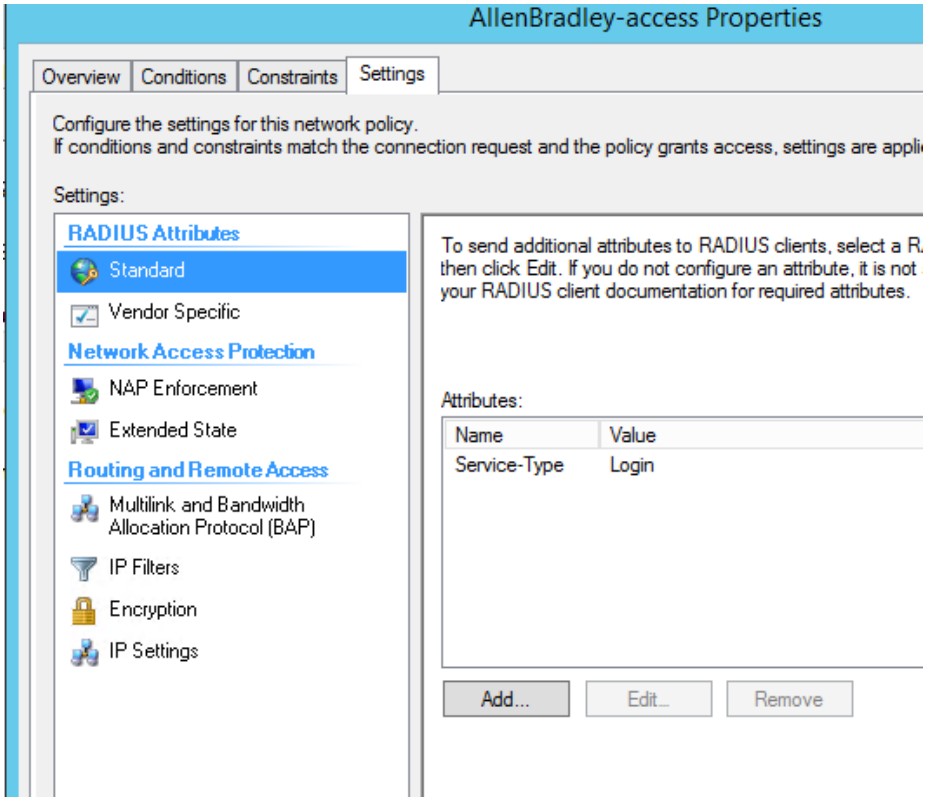
- Under “Conditions”, click on the ADD button, look for “user/groups option”, select the “Network-Admins” security group we setup earlier in our AD. This will allow users from this group to login as admins for managing the switch. Also add another condition to check for the IP address of our Allen-Bradley. Look for “Client IPv4 address” option, enter the IP address of our Allen-Bradley and add it. Below is how the Conditions page should like once both conditions are added. Hit Next to proceed to the next screen.



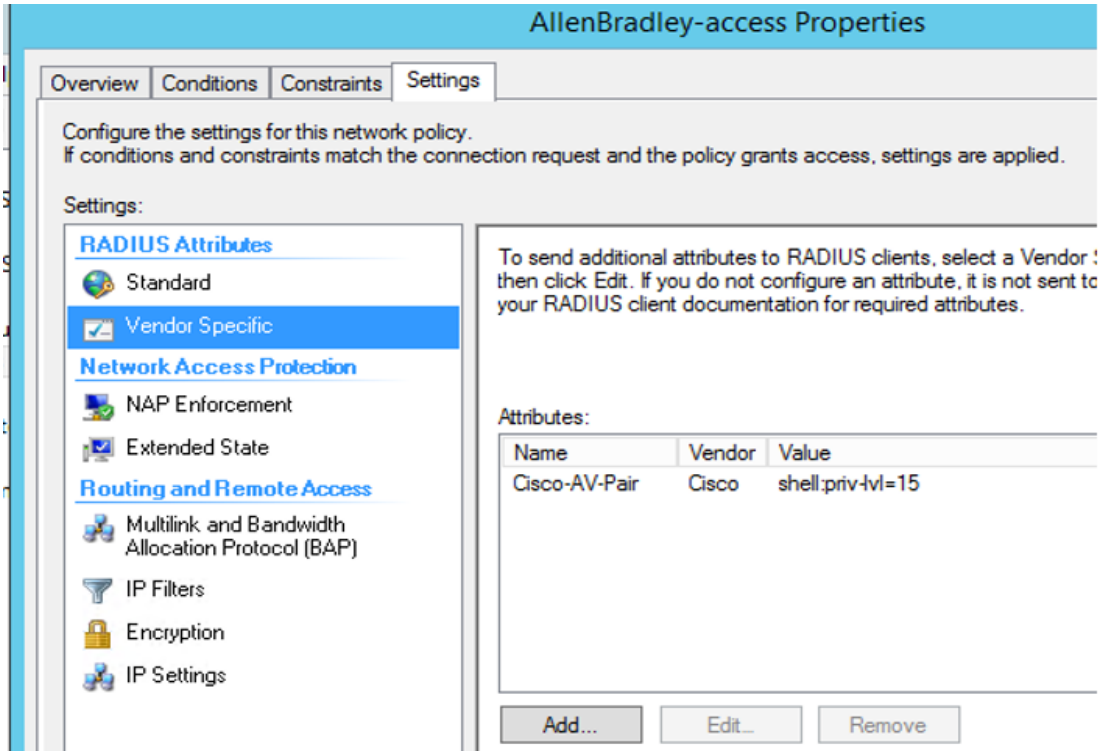
- Under Authentication methods choose the "**PAP, SPAP"** method as Cisco IOS supports these ones. Click **Next** to proceed to the Settings page.



- Under **Settings** >> **Radius Attributes** >> **Standard** >> Remove the 2 default attributes. Click **ADD** to add a new attribute with **Name = "Service-Type**" and **Value = "Login"** as shown below.



- Under Vendor Specific Attributes, add a new attribute by selecting "Cisco-AV-pair" from the list, Vendor= "**Cisco**" and value = "**shell:priv-lvl=15**". This will allow the user to login with privilege level =15 meaning admin privileges. Click on **OK/Apply** button to save the changes



- Configuring Boundary Firewall for Radius Authentication:

  - The following commands were run on the Allen Bradley Boundary firewall to enable it to authenticate against the above Radius server.

```
# enable
# configure terminal
# aaa new-model
# aaa authentication login default group radius local
# aaa authorization exec default group radius local
# radius server host < IP address of our radius server>
# radius server-key <passphrase>
# quit
# wr mem
```

4.9.6 Highlighted Performance Impacts

The following performance measurement experiment was performed for the Active Directory service while the manufacturing system was operational:

PL002.1 Active Directory service active with non-OPC accounts being configured as non-Administrator privilege.

There was no performance impact to the manufacturing process observed during the experiment. However, performance impact was observed at the implementation of the Active Directory (AD) service. At the initial implementation, the team focused on the Active Directory installation and user configuration, but not knowing the need for DCOM configuration initially, causing unplanned production interruption. DCOM and user account configuration for every OPC client have to be modified to use AD instead of local authentication. Without modification, the OPC client failed to communicate with the OPC DA server and caused all OPC data exchange to cease operation. This failure caused the manufacturing process entered the emergency shutdown state.

Another impact observed at implementation was the **time synchronization** source with the AD. Authentication failed due to time discrepancy between hosts and AD. It is because the hosts were synchronized to a different time source than the AD and the time difference was greater than 5 minutes. When the host joins the AD domain, each host should use the same time source as AD. For example, all hosts in PCS use AD as the time source, and AD uses an external NTP server as its time source.

Care should be taken to ensure proper operation of the Active Directory service. Failure in authentication causes error in operation of the OPC server, which handles all the data exchange of the controller and the plant operation. The manufacturing process entered emergency shutdown state because the controller lost the ability to communicate to the sensors and actuators. Redundancy and backup is highly recommended. Ability to switch between primary and secondary AD should be seamless to avoid impact to the system.

There was no significant impact to the network performance observed. For example, the round trip time from OPC to HMI is mostly the same with the Active Directory.

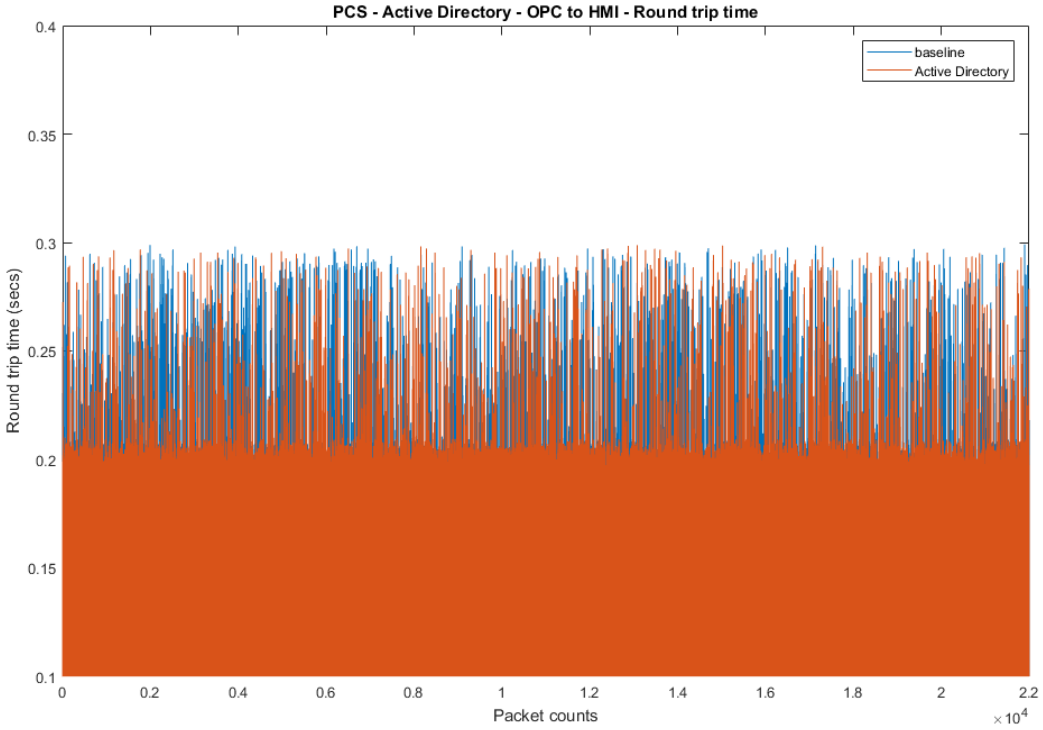


Figure 4-16 Packet round trip time from OPC to HMI with Active Directory.

The controller is another major component required modification to use Active Directory. The Controller authenticates against the AD server. The controller also has the updated DCOM so that it can continue to communicate with the OPC server. The packet round trip time from the Controller to OPC was slightly elevated, with a small number of packets had a slightly increased round trip time. There was no significant increase in inter packet delay from the Controller to OPC observed.

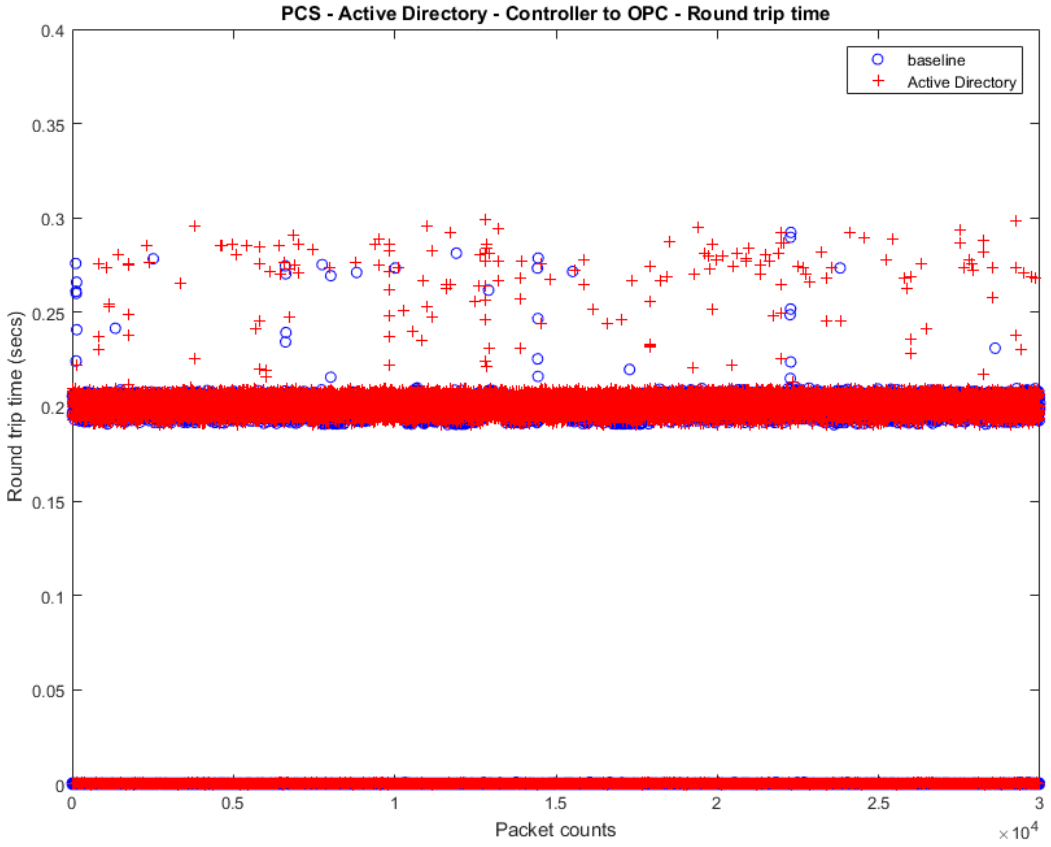


Figure 4-13 Packet round trip time from Controller to OPC with the Active Directory enabled (red)

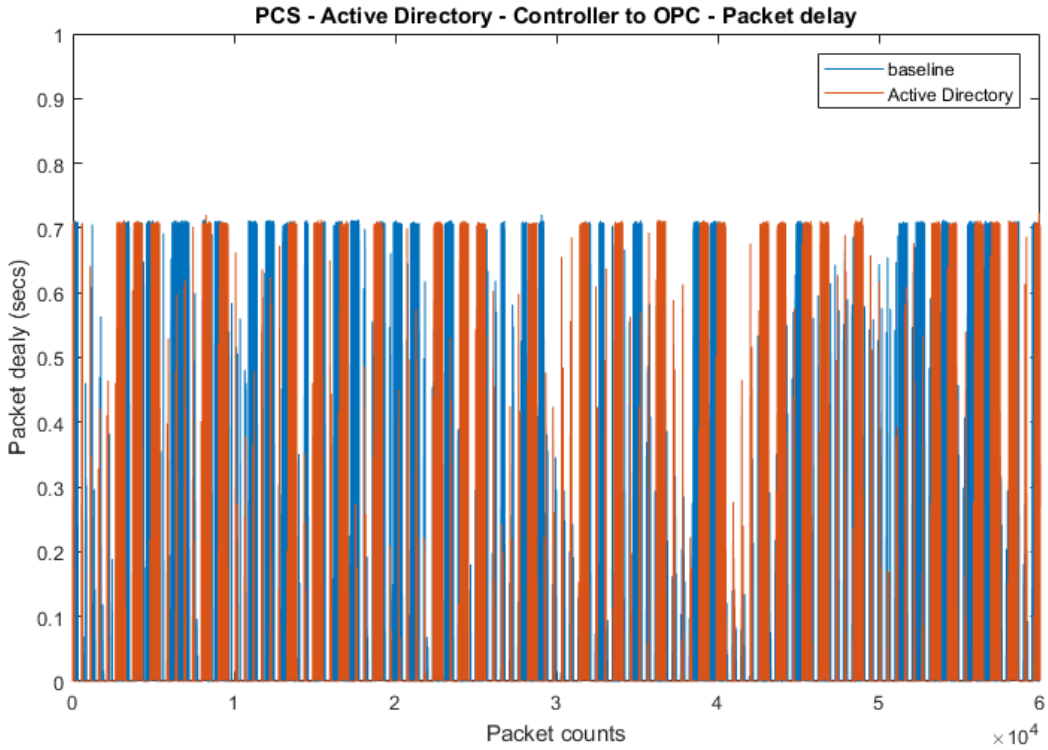


Figure 4-14 Inter packet delay of Controller to OPC with the Active Directory enabled (red)

There was no significant performance impact to the manufacturing process observed with the use of Active Directory. For example, the product flow rate remained consistent with and without the use of Active Directory.

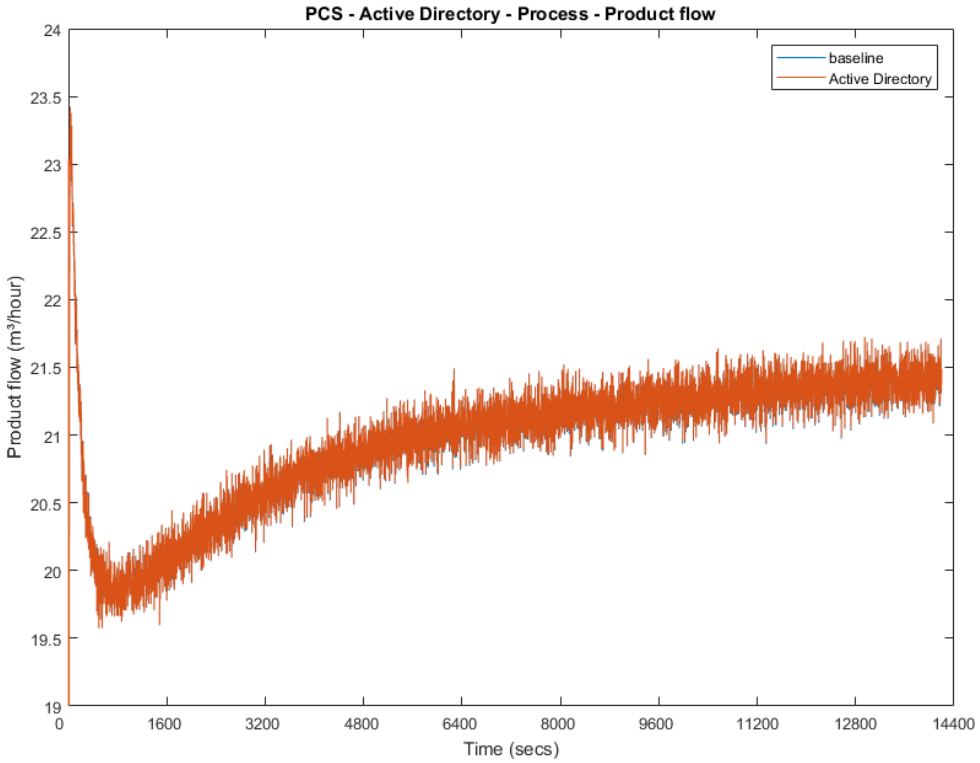


Figure 4-19 Manufacturing process product flow rate during the use of Active Directory (red)

A misconfiguration on the Active Directory cased the manufacturing process to enter the emergency shutdown state in about 600 seconds of the experiment time due to the reactor pressure too high

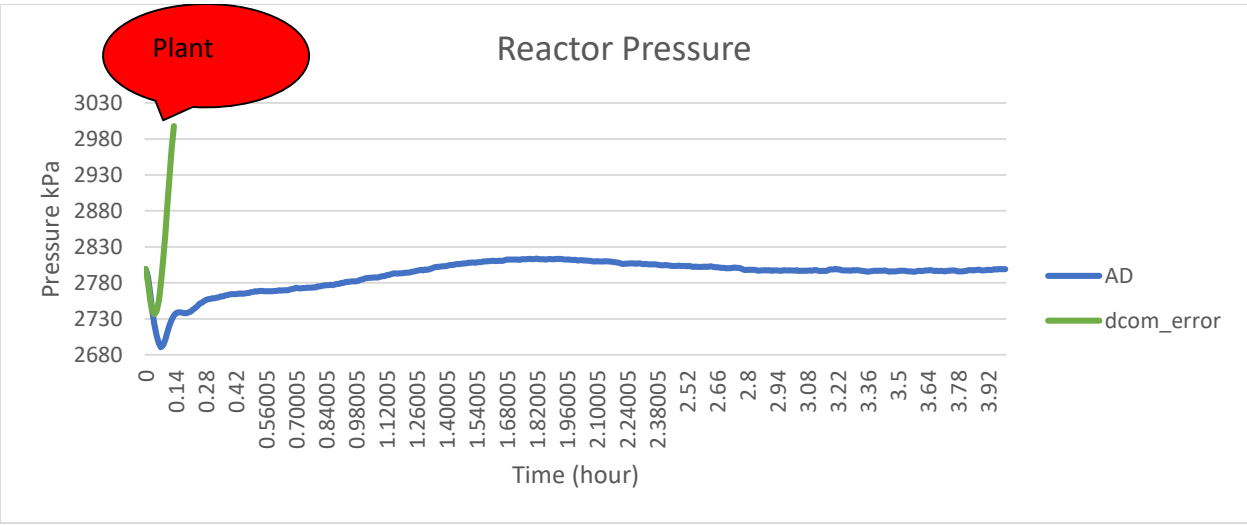


Figure 4-20 Plot of the manufacturing process reactor pressure. The process entered emergency shutdown mode when DCOM communication failed.

4219

4220 ### 4.9.7 Link to Entire Performance Measurement Data Set

4221 **Active Directory KPI data**

4222 **Active Directory measurement data**

4223

4.10 Symantec Endpoint Protection

4.10.1 Technical Solution Overview

Symantec Endpoint Protection:
Symantec Endpoint Protection (SEP) is a complete endpoint protection solution from Symantec. It delivers superior, multilayer protection to stop threats regardless of how they attack your endpoints. SEP integrates with existing security infrastructure to provide orchestrated responses to address threats quickly. Its lightweight SEP agent offers high performance without compromising end-user productivity. SEP also defends against ransomware and other emerging threats with multilayered protection that fuses signatureless technologies like advanced machine learning, behavior analysis and exploit prevention with proven protection capabilities like intrusion prevention, reputation analysis and more.[22]

Points to Consider:

- Next Generation Antivirus / Endpoint protection solution to prevent against virus attacks and emerging cyber threats such as zero-day attacks, ransomware etc.
- OS Platform independent: The endpoint agents are supported on Windows and Linux.
- Comes with a lightweight agent and virus definition sets that require minimal network bandwidth.
- Diverse Feature set: Core capabilities include Antivirus, Host Firewall, Intrusion Prevention, Host Integrity, System lockdown, Application White listing and USB Device Control.
- Centralized Management: All endpoints, rule sets, policies can be centrally managed from the Symantec Endpoint Manager console.
- The Symantec Manager component is supported only on Windows OS.
- The Linux agent requires the OS kernel on Linux systems to be at a certain level for installation. In addition, the Linux agent is a 32-bit installer. If installing on a 64-bit Linux system, it requires certain 32-bit packages/libraries to be installed as a pre-requisite. This may conflict with some of the existing packages on the system.
- The endpoint agent on each system by default needs to communicate outbound with a range of public IP addresses for its Reputation analysis and Global Threat intelligence feature. It is recommended to allow this traffic from your firewall to leverage the advanced features of the product.
- **Important**: System reboot is required to complete the installation process on clients/endpoints. Plan ahead of time.

[22] Symantec Endpoint Protection: https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-14-en.pdf

4258

4259

4260 ### 4.10.2 Technical Capabilities Provided by Solution

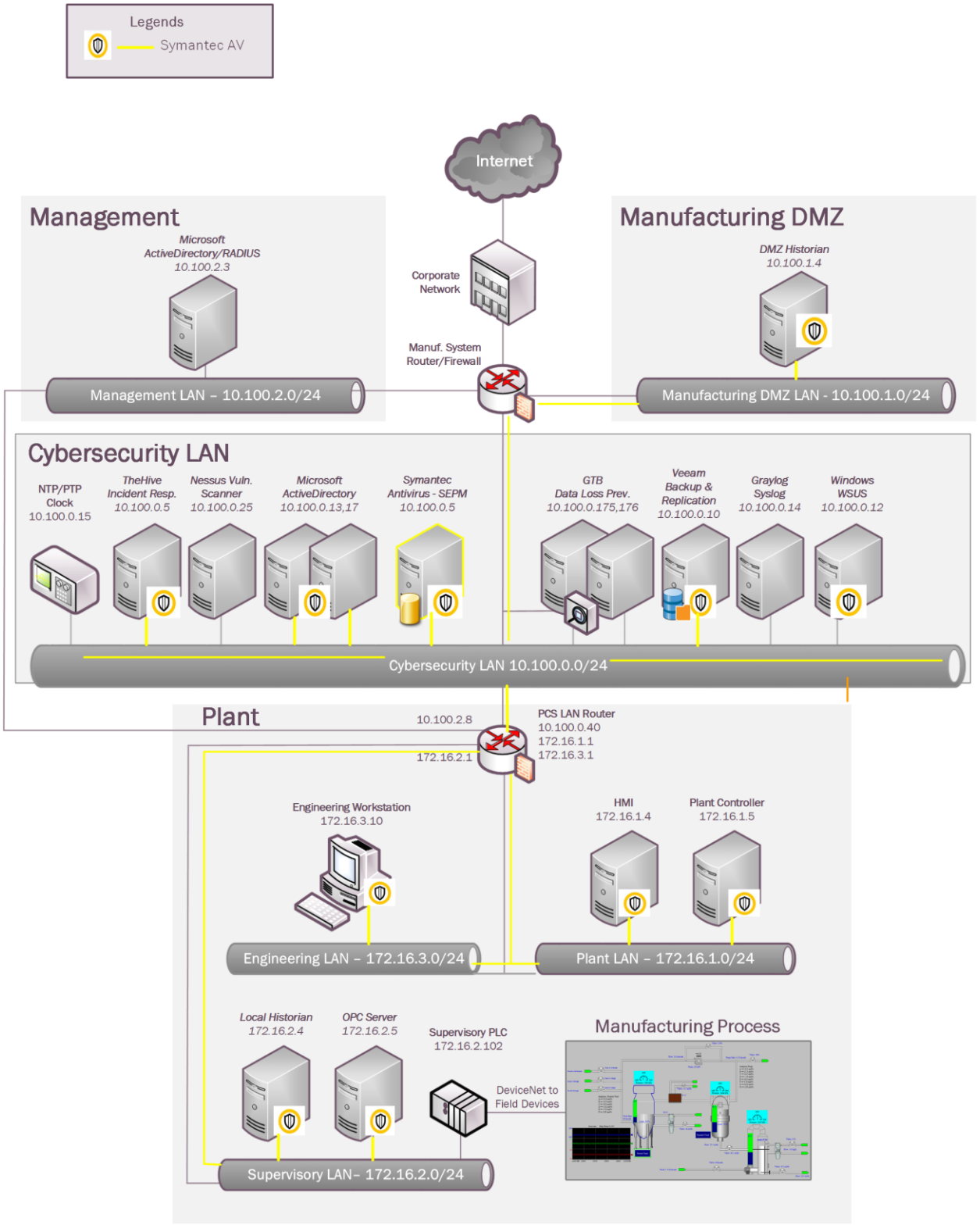
4261 Symantec Endpoint Protection provides components of the following Technical Capabilities
4262 described in Section 6 of Volume 1:

4263 - Anti-virus/malware

4264 ### 4.10.3 Subcategories Addressed by Implementing Solution

4265 PR.AC-1, DE.CM-3, DE.CM-4

4.10.4 Architecture Map of Where Solution was Implemented



4.10.5 Installation Instructions and Configurations

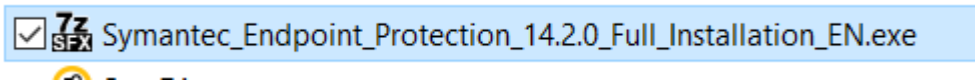
Setup Overview:

Setup consists of a single Symantec Endpoint Protection Manager (SEPM) instance in the Cybersecurity LAN network. This central instance communicates with all the endpoint agents deployed on to the Process Control systems. Likewise, all endpoints report their status to the Manager server. The communication ports required to be opened are different for Windows clients as compared to Mac/Linux clients. Detailed list of firewall ports can be obtained from Symantec website. The SEP Manager server downloads its daily signature updates from the Symantec cloud servers, so this necessary traffic was allowed to pass thru the Manufacturing System Firewall.

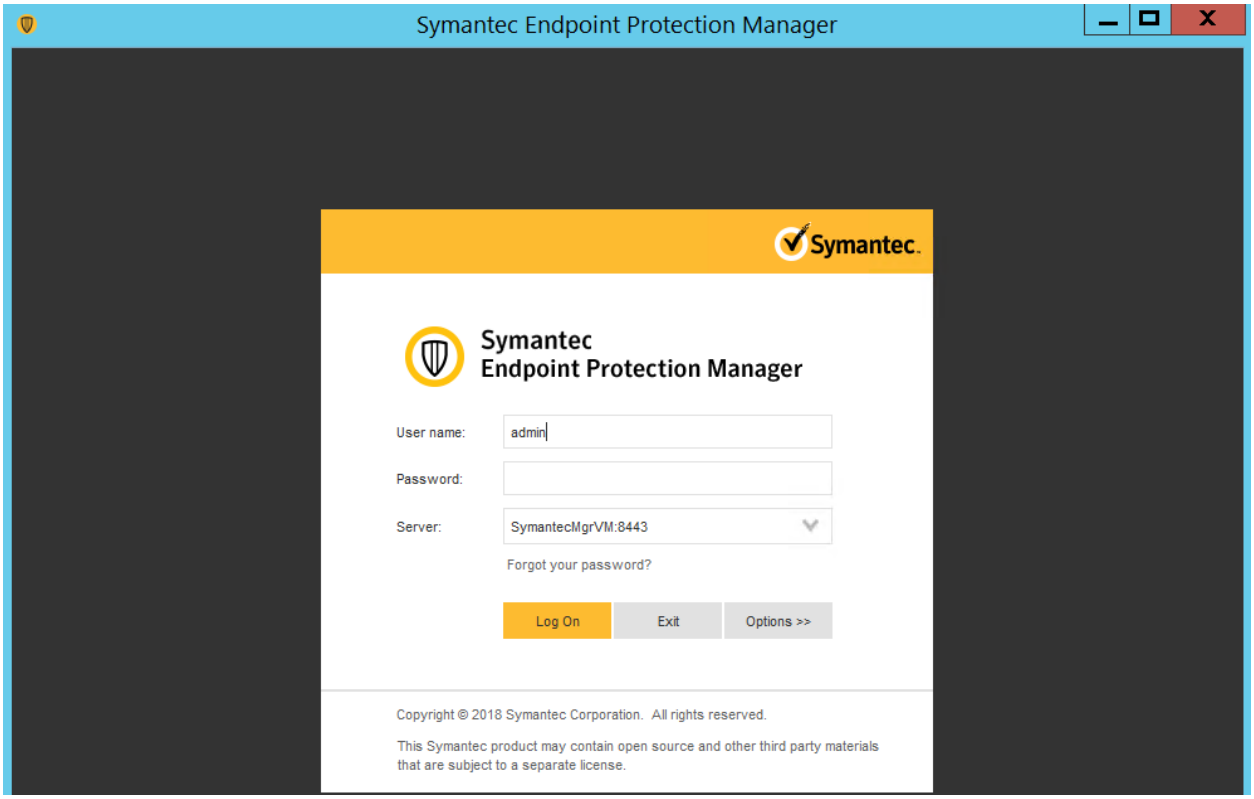
Details of the software used

Product Name	Version
Symantec Endpoint Protection Manager (SEPM)	14.2 Build 758
Symantec Endpoint agent for Windows (Client)	14.2.758.0000

Installation of SEP Manager:

- SEPM is supported only on Windows server platforms. A Windows Server 2012 R2 virtual machine was setup in the Cybersecurity LAN to install the SEPM component.
- Upon purchase, there will be a license file emailed to you along with the link to download the install binaries. Download the zip bundle from the Symantec website. Extract the zip file which will be like the one below depending on whatever is the latest version available.
  - 

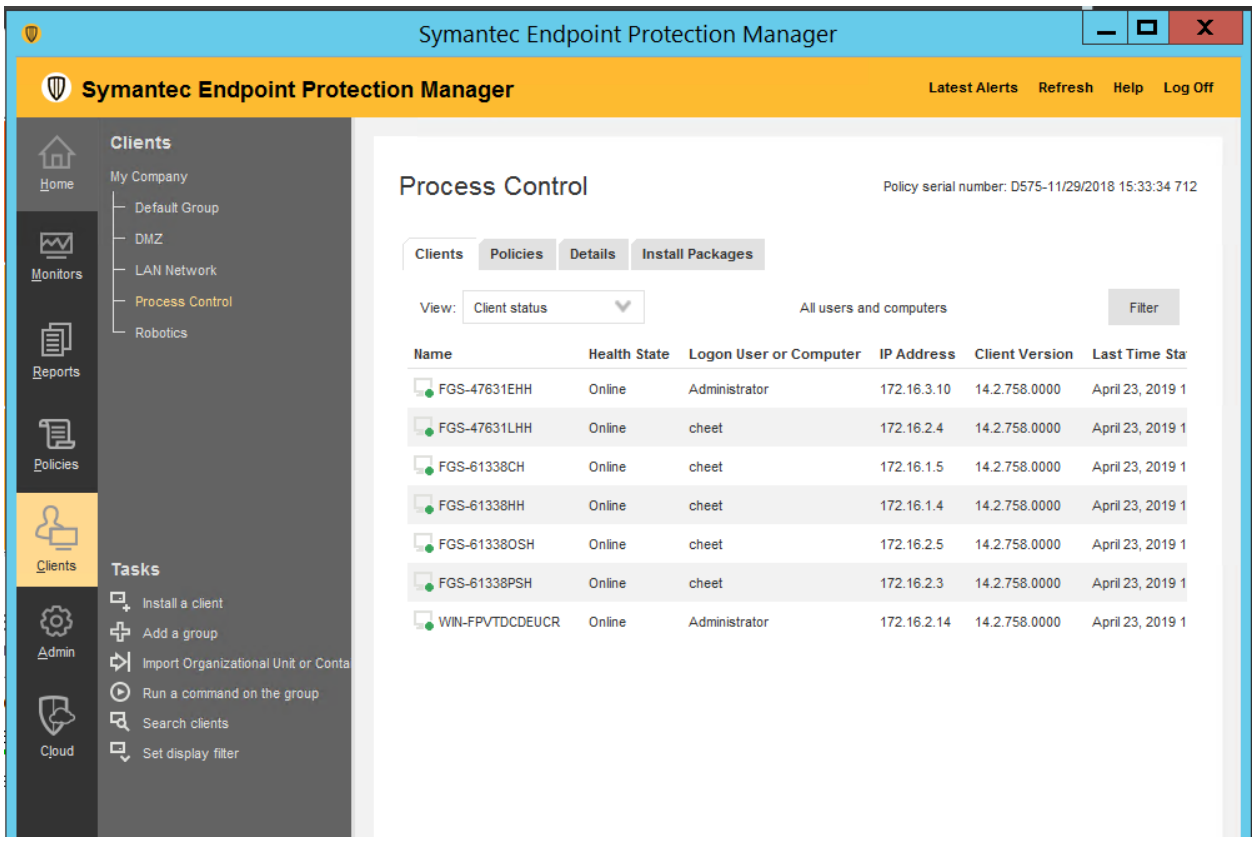
- Open the extracted folder and run the **Setup.exe** file. Mid-way during the setup, the install wizard will prompt to select a password for the admin user. Enter a strong password and hit **Next**.
- On the **Backed Database** selection page, there are two options - "**Embedded**" and "**MS SQL Server**". Choose the **Embedded database** if you do not have a MS SQL Server. Follow the on-screen instructions and complete the installation wizard. Reboot the server once done.
- Launch the SEP Manager console and login with the admin user created earlier.



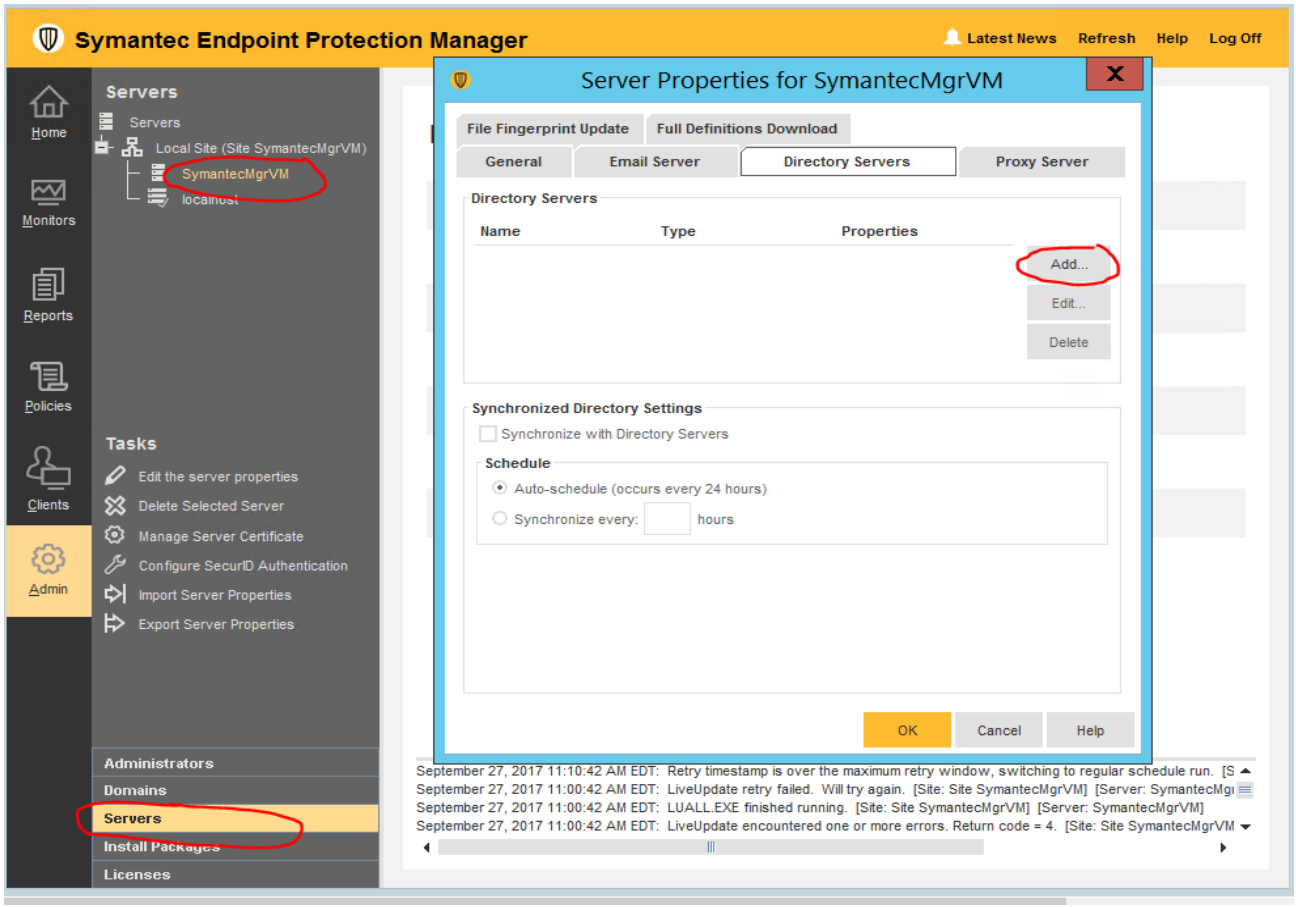
- Upon completing the installation of Symantec Endpoint Manager, the next steps are to activate the license, configuring client groups to group devices and installing the antivirus agent on each endpoint/client system.
- Link to Official Symantec Endpoint Protection v14 installation guides - https://support.symantec.com/en_US/article.DOC9449.html
- Ensure to open the necessary ports on the firewall for communication between the SEPM server and endpoints. A complete list of ports is available at https://support.symantec.com/en_US/article.HOWTO81103.html

Custom Configuration of SEPM server

- The following client groups were created to group devices from each of the systems. Upon installing the AV agent on the endpoints, the devices were moved to their respective groups.



- For integrating SEP Manager with AD/LDAP server, click on **ADMIN** >> **Servers** >> **Local Site** >> **<Server Name>** >> **Edit Server Properties** >> **Directory servers.** Click further on "**ADD**" button as shown below to configure domain details. Once done, logout and try logging in back with your AD credentials.



- Similarly, Email server can be configured by clicking on the "Email Server" tab.

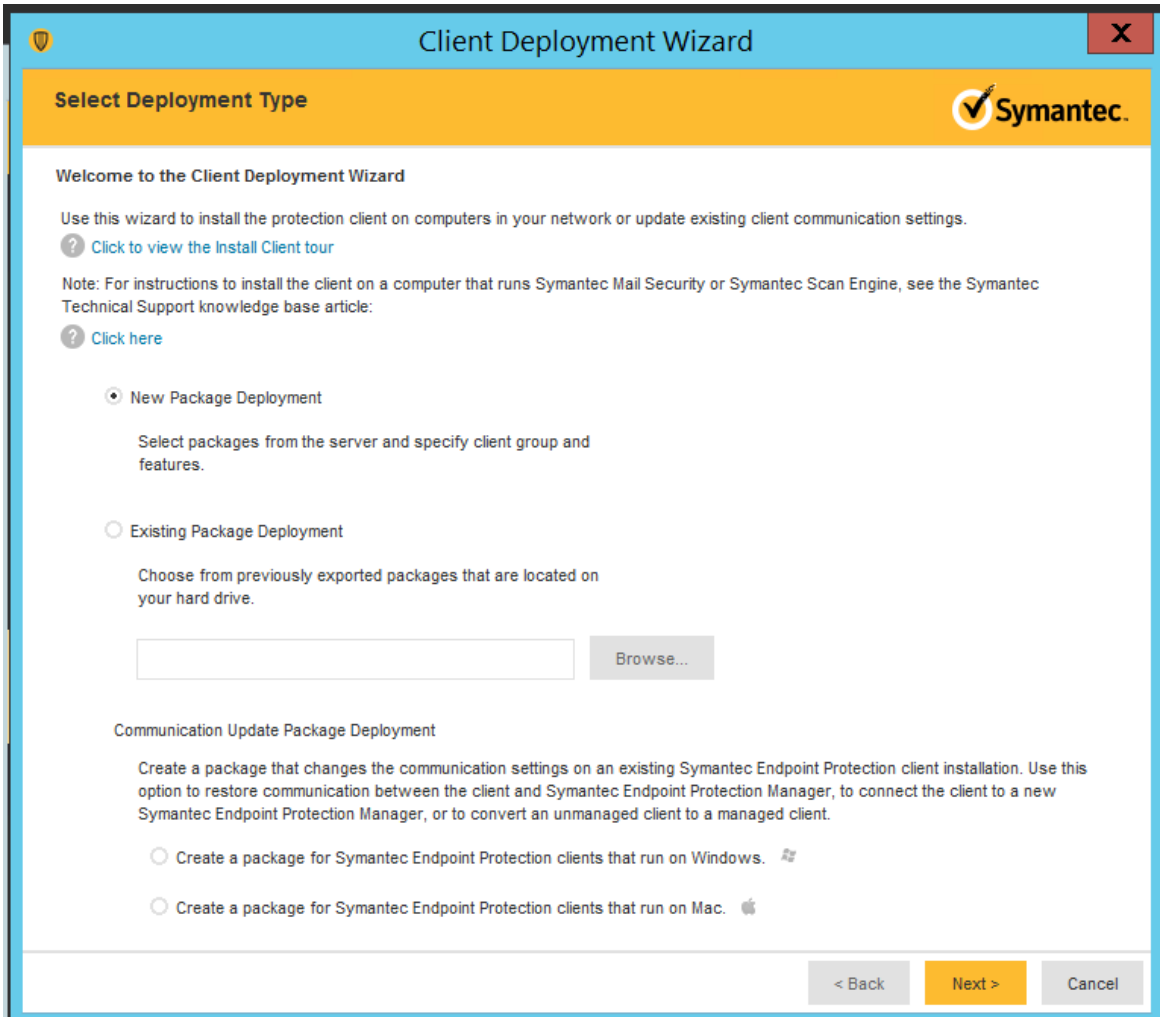
Getting started with Endpoint installs

High level steps:

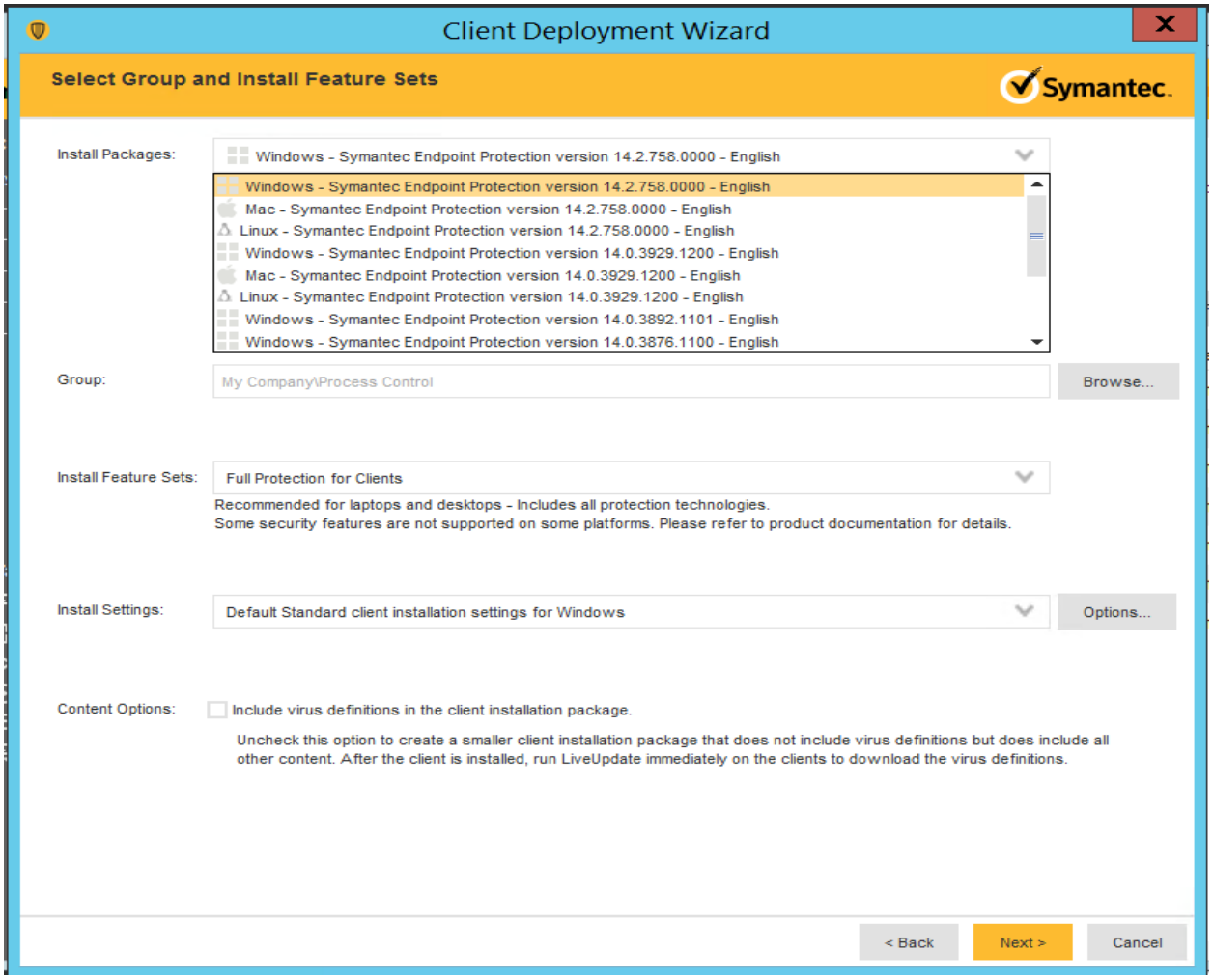
- Create a deployment package specific for a client group
- Deploy the package from the SEPM server to the endpoint using Network Deployment options or manually copy over the package to the endpoint for installation.
- Restart the endpoint. Verify the device shows up in the SEPM console.

Creating a deployment package:

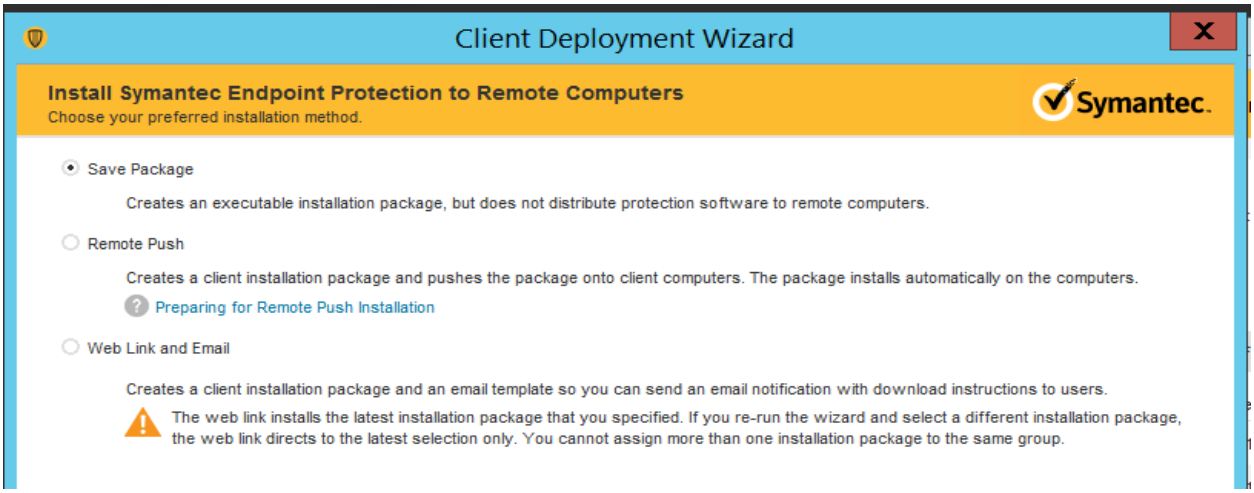
- Login to the Symantec Manager console, click on **CLIENTS** >> **<Group Name>** where the device needs to be in >> Click on **Install client under TASKS**. For instance, to create a deployment package for the group "**Process Control**", click on that group name followed by **Install Client** option.
- Select "**New Package Deployment**" if this is your first agent installation of that group. If you have already deployed the agent on other systems of this group, you can re-use the same package and skip this wizard completely.



- Click "**Next**" >> Choose the appropriate OS Platform as per the endpoint OS, from the dropdown list of **Install Packages**. You will notice the Group Name is already pre-populated. This ensure the client will be placed directly in that group upon install. Under **Content Options**; Select "**Include virus definitions in the client installation package**" [optional]. Click **Next**.

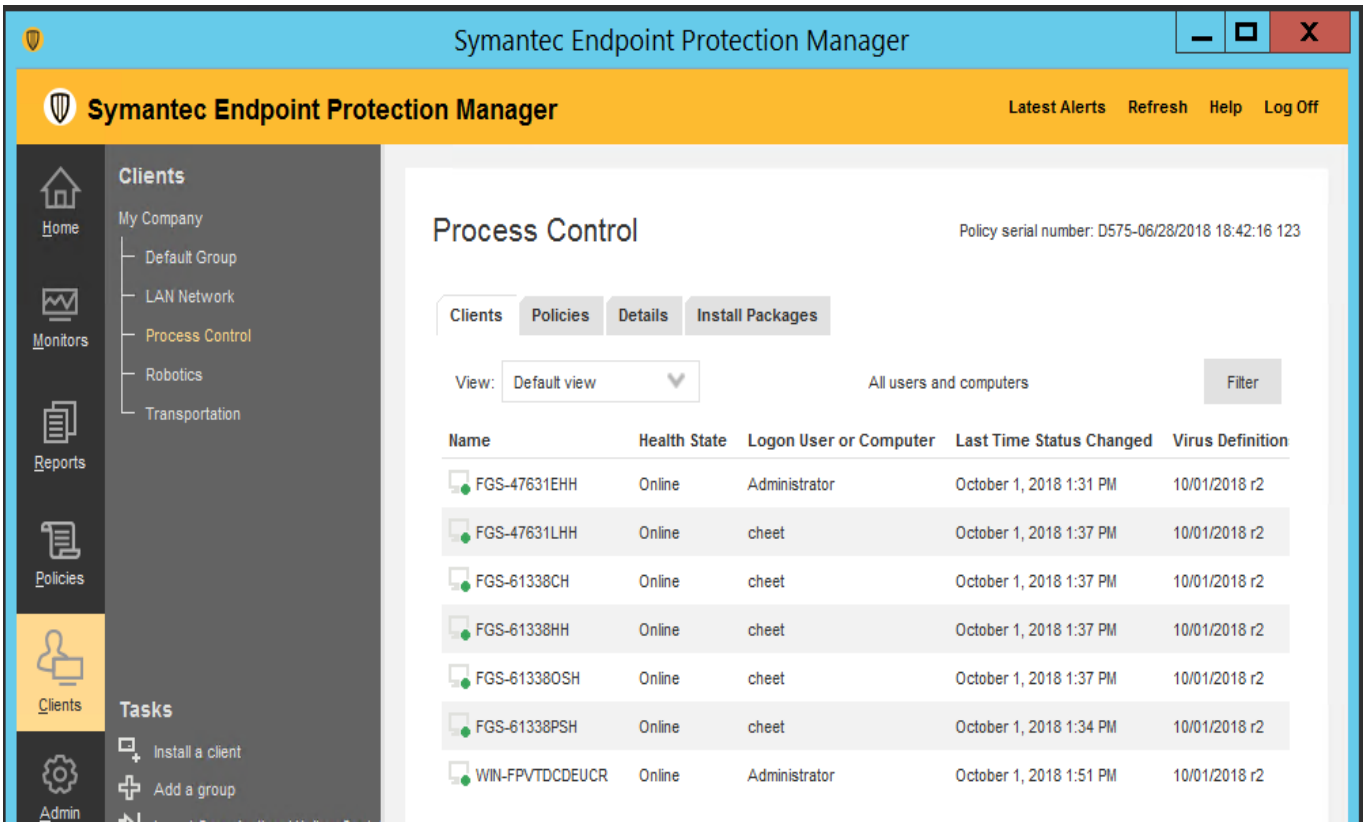


- On the next page, choosing the "**Save Package**" will create a local installer which needs to be copied over the target machine manually and the "**Remote Push**" will make the SEPM server perform a network deployment to the target machine(s). Choose your preferred option and hit **Next**.



Installing the AV on Process Control System

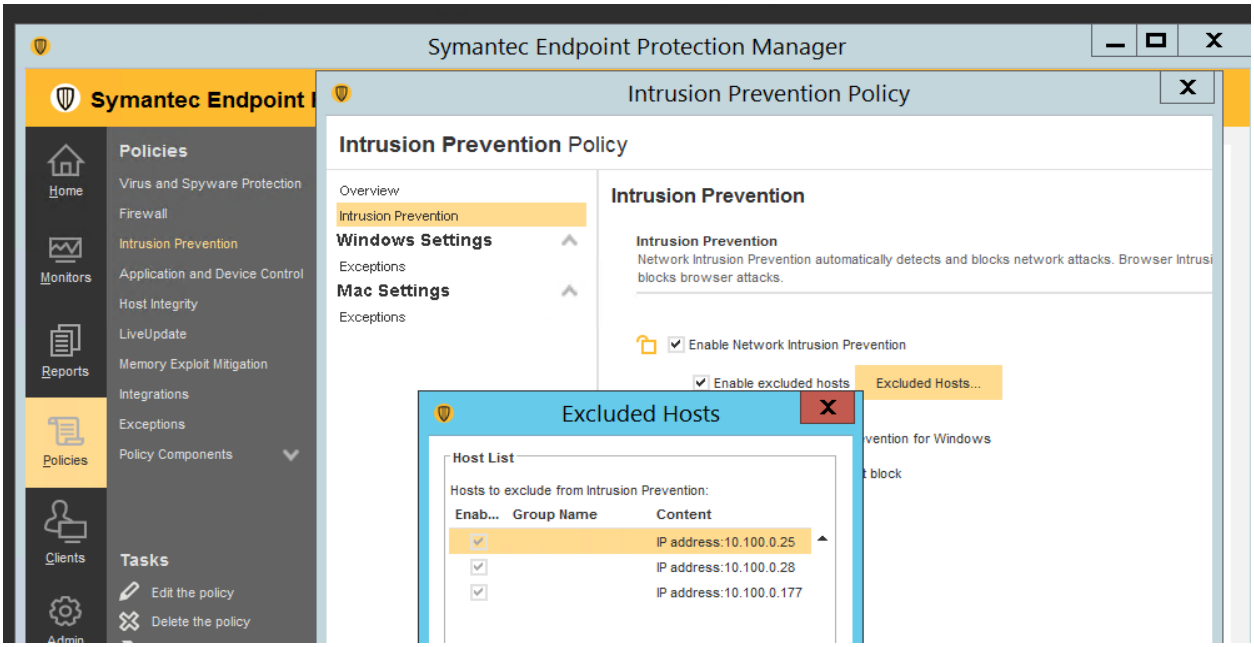
- An installation package was first created as described in the previous section by selecting "**Process Control**" group and install package as "**Windows**". The executable installer was then manually copied over to each Windows system in the network and run.
- Upon installation, the system requires a **restart**. All systems were rebooted post installation.
- The SEPM console on the central server was checked to confirm all the clients from the group were reporting **green** **ONLINE** and their **Virus Definitions** were current.



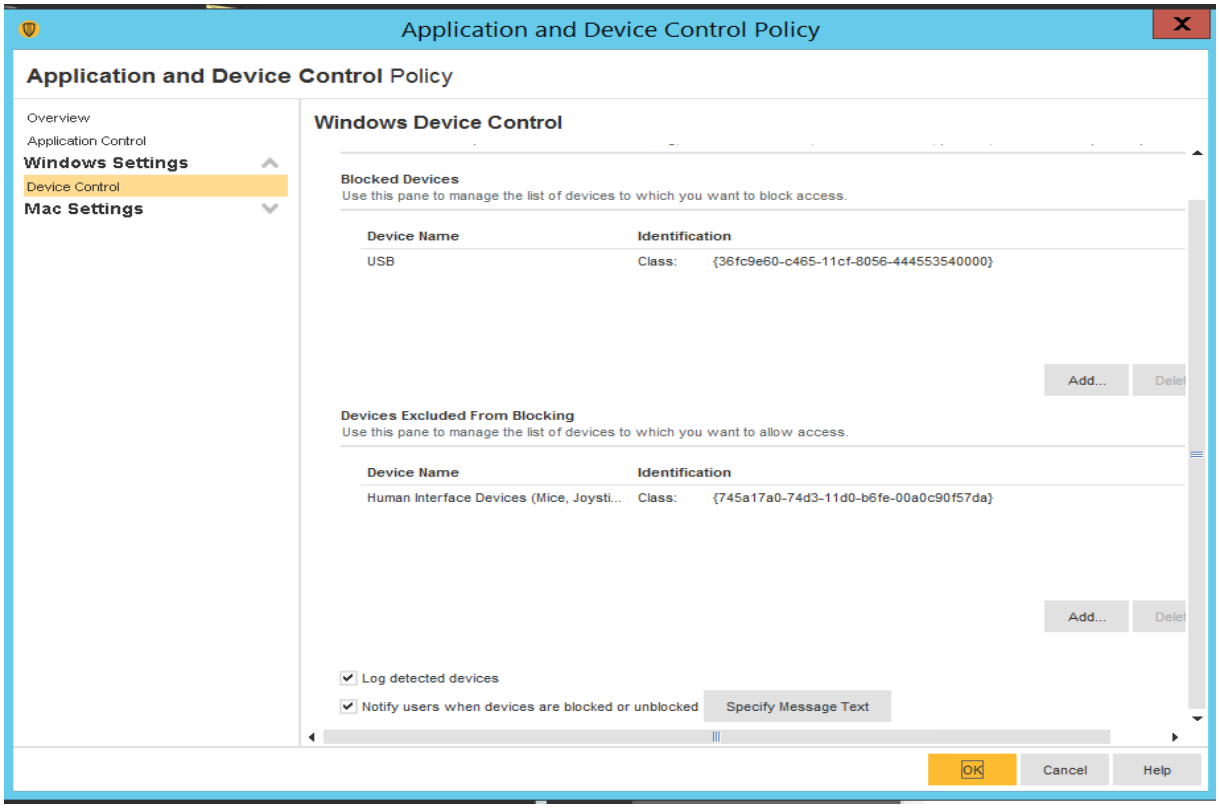
- The official install guide for Windows systems can be found at https://support.symantec.com/en_US/article.DOC9445.html

Additional Configuration

- Symantec AV on each system by default blocks any port scan related traffic. If you have a vulnerability scanner or security tools in your environment, ensure those IP addresses are whitelisted in the SEPM console. The recommended way to do this is by creating a policy under **Policies** >> **Intrusion Prevention** >> **Excluded Hosts** and linking it to the appropriate client group. The figure below shows the settings page of excluded hosts.



- To setup device control such as restricting USB devices, create a policy under "**Application and Device Control**". Detailed instructions can be found here. Below shown image shows the USB policy implemented in our use case.



Lessons learned

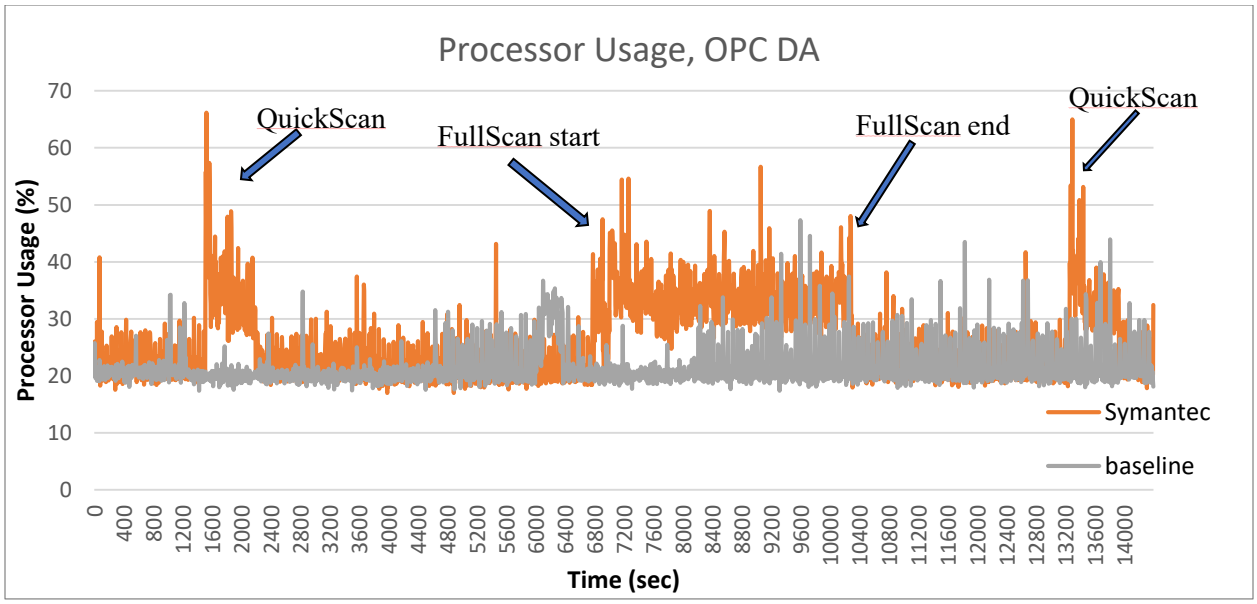
- Using Symantec's Firewall: SEP also provides a firewall for clients. Firewall rules control how the client protects the client computer from malicious traffic. When you install the console for the first time, it adds a default Firewall policy to each group automatically. Similarly, a client typically gets default firewall settings if a firewall policy is not configured from the console. Ensure to disable Windows OS or Host OS firewall if using Symantec's firewall.

4.10.6 Highlighted Performance Impacts

The following performance measurement experiment was performed for the Symantec anti-virus tool while the manufacturing system was operational:

Experiment PL008.2- Symantec AV scan

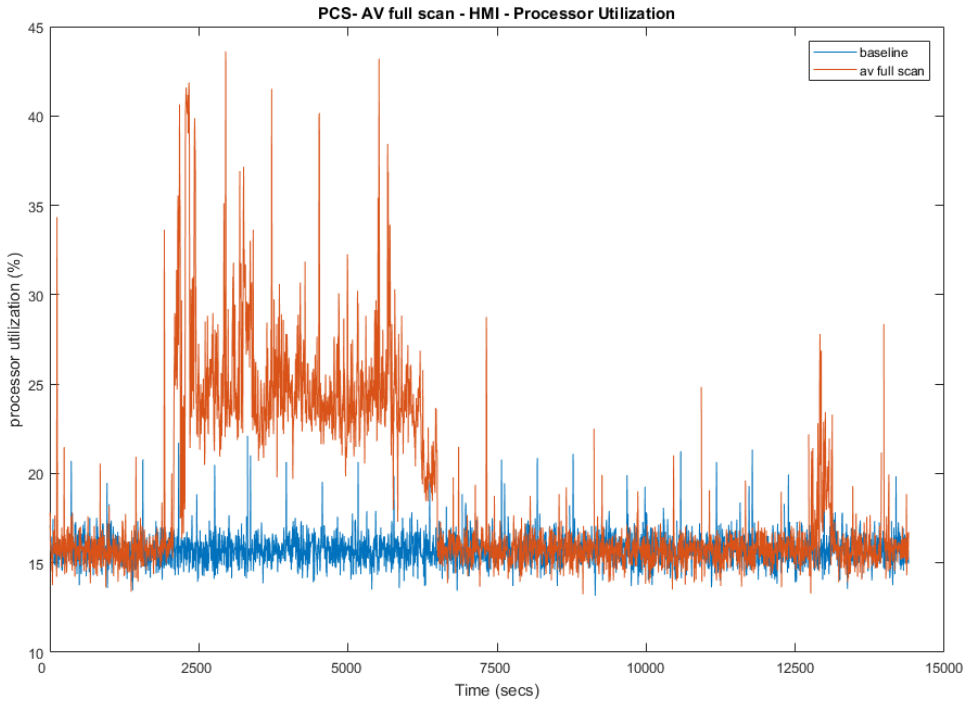
During the Symantec anti-virus scan, sizeable performance impact was observed on the host processor Utilization. However, no significant performance impact was observed on the manufacturing process. A full Symantec scan can take up a considerable amount of processor power.



4394

4395 **Figure 4-21 Plot of processor utilization of the OPC computer during the Symantec anti-virus scan (Red), and**
4396 **the baseline processor utilization (gray)**

4397 No significant performance impact to the network was observed. For example, the packet round
4398 trip time between the OPC and PLC remained mostly the same.



4399

4400 **Figure 4-22 Plot of processor utilization of HMI computer during a Symantec scan (red) and without a**
4401 **Symantec scan (blue)**

No significant performance impact to the network was observed. For example, the packet round trip time between the OPC and PLC remained mostly the same.

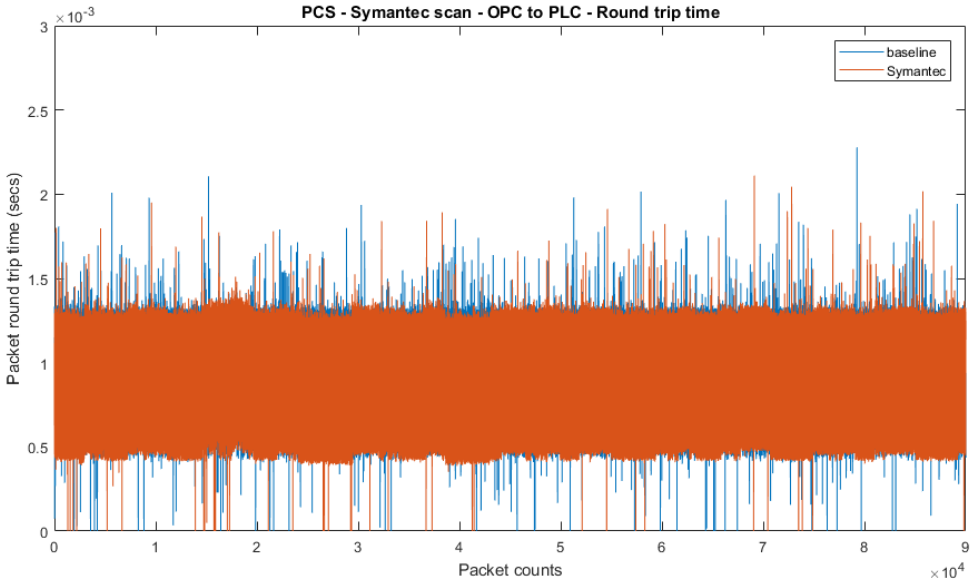


Figure 4-23 Packet round trip time between OPC and PLC during Symantec scan (red)

There was no significant impact to the manufacturing process observed. The product flow and the reactor pressure remain very close to the baseline measurement during the Symantec scan.

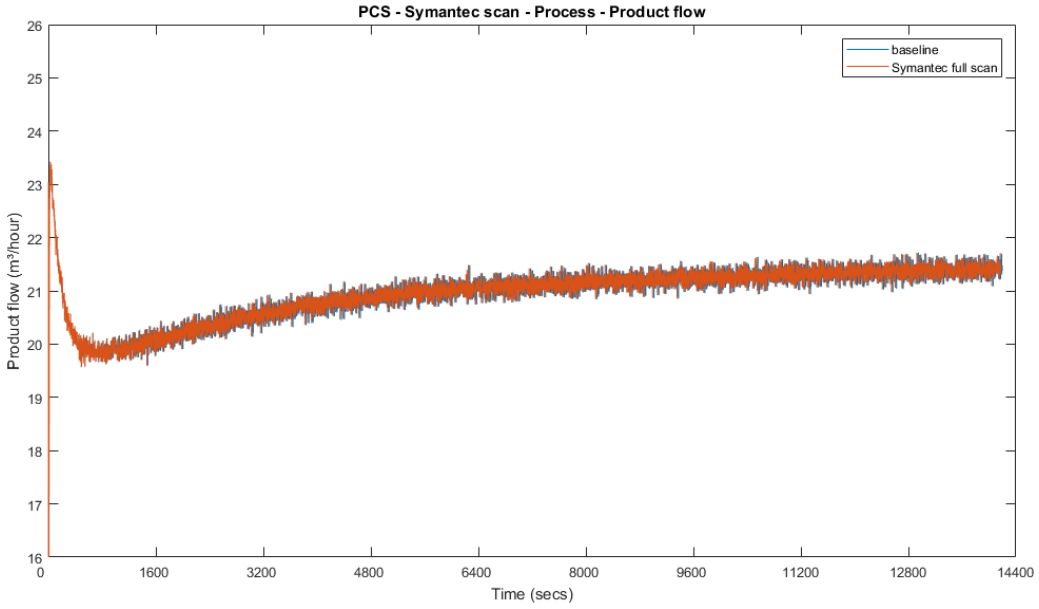


Figure 4-24 Manufacturing process product flow rate

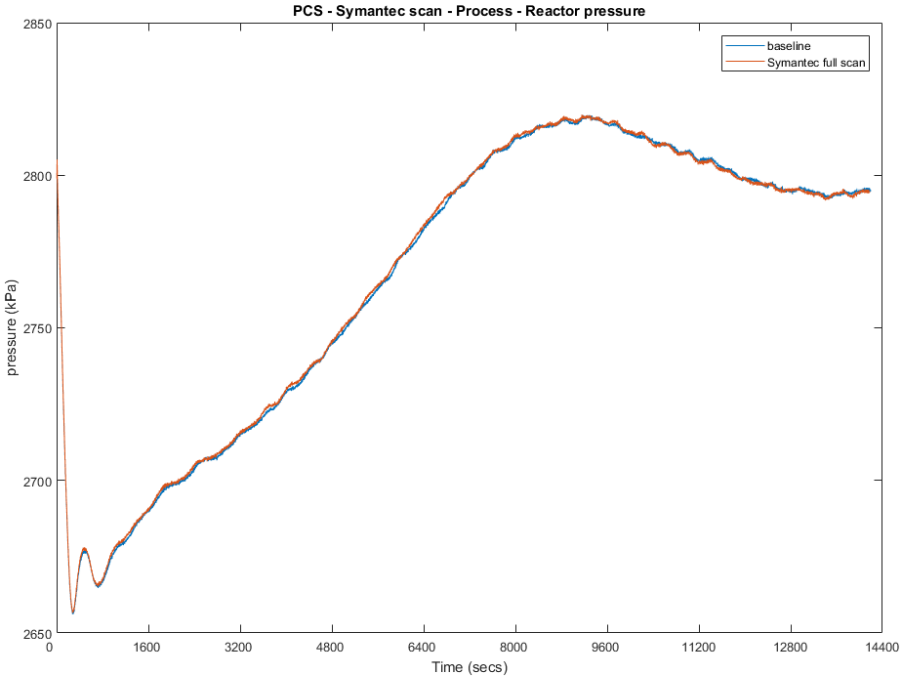


Figure 4-25 Manufacturing process Reactor pressure

It is hypothesized that the impact to the processor utilization was caused by the Symantec AV during the scan. In the case of the PCS system, the normal processor utilization is relatively low and therefore the increased usage did not cause any performance impact to the manufacturing process. If the normal utilization of the host is close to 100%, there is potential performance impact due to the increase utilization during scan time.

4.10.7 Link to Entire Performance Measurement Data Set

Symantec AV KPI data

Symantec AV measurement data

4.11 Tenable Nessus

4.11.1 Technical Solution Overview

Nessus Professional is a vulnerability assessment software from Tenable. It features high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery and more. Nessus supports technologies such as scanning operating systems, network devices, next generation firewalls, hypervisors, databases, web servers and critical infrastructure for vulnerabilities, threats and compliance violations.[23] It supports both authenticated and unauthenticated scans.

Points to consider:

- Easy to setup, User friendly dashboard, fast scanning and can be configured to work in a distributed environment.
- Support for Industrial Protocols such as MODBUS, DNP3 etc. It has the necessary plugins to detect vulnerabilities on ICS/SCADA systems making it ideal to use in OT environments.
- Comes with a variety of Out-of-box policy and configuration templates.
- No limit on number of IPs or number of assessments you can run.
- Support for scanning devices behind a firewall.
- No integration available with LDAP or AD in the Professional edition.
- Multiple user accounts not supported for logging in to the Web UI.

4.11.2 Technical Capabilities Provided by Solution

Tenable Nessus provides components of the following Technical Capabilities described in Section 6 of Volume 1:

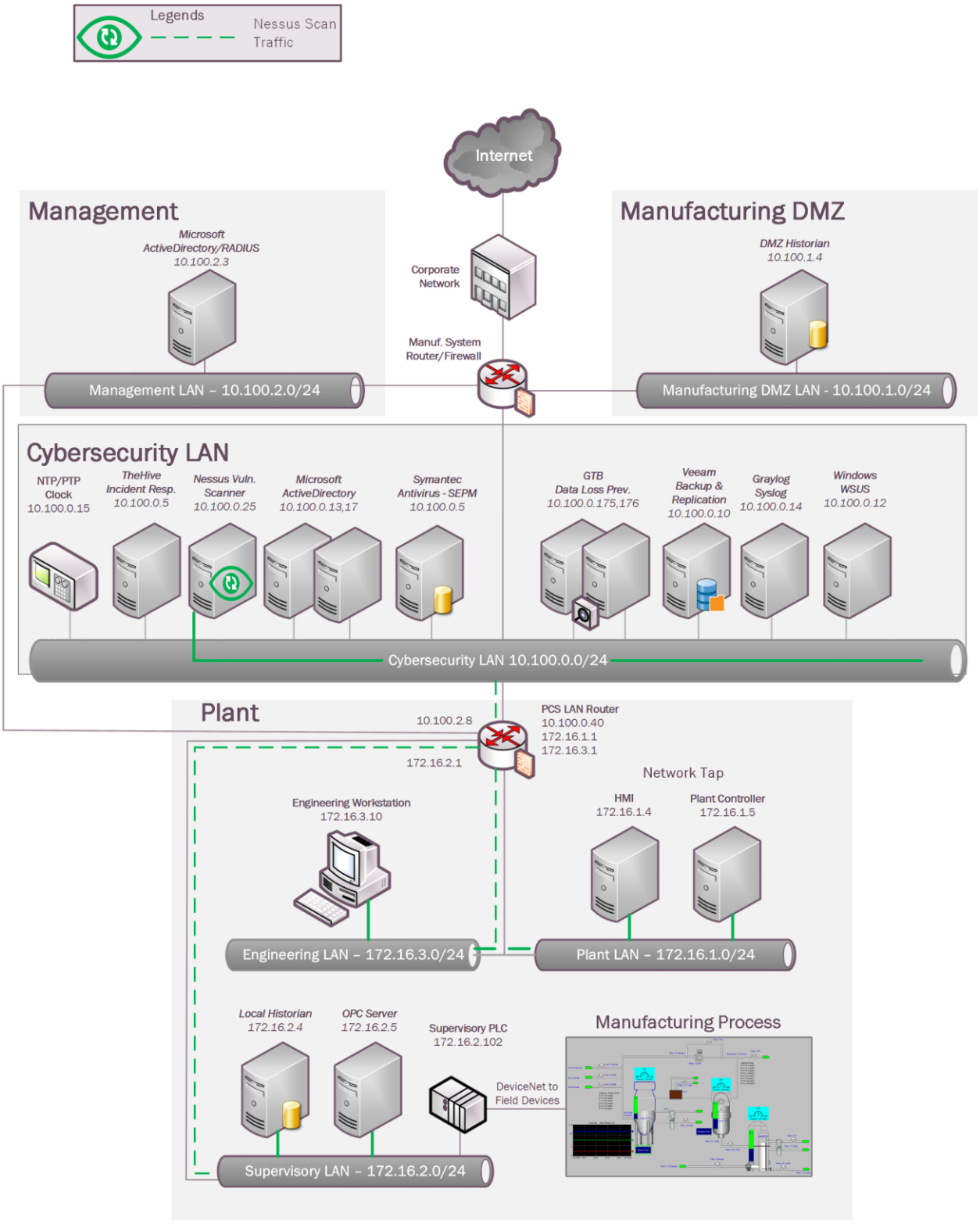
- Vulnerability Scanning
- Vulnerability Management

4.11.3 Subcategories Addressed by Implementing Solution

ID.AM-3, ID.AM-4, ID.RA-1, DE.CM-4, DE.CM-8

[23] Nessus Professional: http://info.tenable.com/rs/934-XQB-568/images/NessusPro_DS_EN_v8.pdf

4.11.4 Architecture Map of Where Solution was Implemented



4.11.5 Installation Instructions and Configurations

Details of the solutions implemented:

Name	Version
Nessus Professional	7.2.0

Setup Overview:

- A Nessus Professional 7.x version package file was downloaded from Tenable website and was installed on a Windows 2012 R2 Virtual machine in the Cybersecurity-LAN network. Nessus is supported on Windows, Linux and Mac OS platforms. Detailed installation instructions can be found in official product guide. [24]

- Ours was a single instance deployment. For distributed environments, Nessus supports distributed architecture of having multiple Nessus servers called as remote scanners linked to a central Nessus manager instance.

- During the setup, the wizard will prompt for registration. The Registration process and updates can be configured either in online or offline mode. An online mode is suitable for environments where Nessus server is connected to the internet while an offline mode is for air-gapped environments. Detailed instructions for registering Nessus offline can be found in the product guide. Upon completion, Nessus can be accessed via https://<IP address of Nessus server>:8834

- The Nessus server needs to have network connectivity from whichever networks or subnets that are intended to be scanned. In addition, if performing authenticated scans then appropriate firewall rules should be in place to allow SSH, WMI or SNMP traffic depending on the type of hosts. If performing unauthenticated scan, the firewall should be allowed for any-any communication between the Nessus server and target network.

Configuration:

- The Process Control Network has direct network connectivity with the Cybersecurity-LAN network, therefore no additional configuration was required other than allowing ports for WMI communication for scanning the Windows systems located in the Process Control network.

[24] Nessus Official Documentation: https://docs.tenable.com/nessus/Content/GettingStarted.htm

- The following is a list of settings that must be true for credentialed (authenticated) scans to run successfully on Windows systems. All of these were enabled on the client (target) machines of Process Control System.

    1. The Windows Management Instrumentation (WMI) service must be enabled on the target. (https://technet.microsoft.com/en-us/library/cc180684.aspx)

    2. The **Remote Registry** service must be enabled on the target.

    3. File and Printer Sharing must be enabled in the target's network configuration.

    4. An SMB account must be used that has local administrator rights on the target. (You can use a domain account, but that account must be a local administrator on the devices being scanned.)

    5. Ports 139 (TCP) and 445 (TCP) must be open between the Nessus scanner and the target.

    6. Ensure that no Windows security policies are in place that block access to these services. See below for more information.

    7. The default administrative shares (i.e. IPC$, ADMIN$, C$) must be enabled (AutoShareServer = 1). These are enabled by default and can cause other issues if disabled (http://support.microsoft.com/kb/842715/en-us).

- Run all commands from an elevated Command prompt or PowerShell (Right click **CMD** > **Run as administrator**) on a host in the same network as the target

    1. This command will see if we can access the IPC$ share without a username (This is how Nessus tests to see if SMB is running):
    Change x.x.x.x with the target's IP address. net use \\x.x.x.x\ipc$ /user:""

    2. If this returns "Failed to connect to the IPC$ share anonymously." then SMB is not running correctly.

- For SMB log-on test, run the following commands, with "username" being the username of the account and "password" as the password for the account being used for the scan:

    net use \\x.x.x.x\ipc$ /user:username password

    net use \\x.x.x.x\admin$ /user:username password

These commands should return "The command completed successfully." If it does not, then the credentials did not work or do not have sufficient privileges.

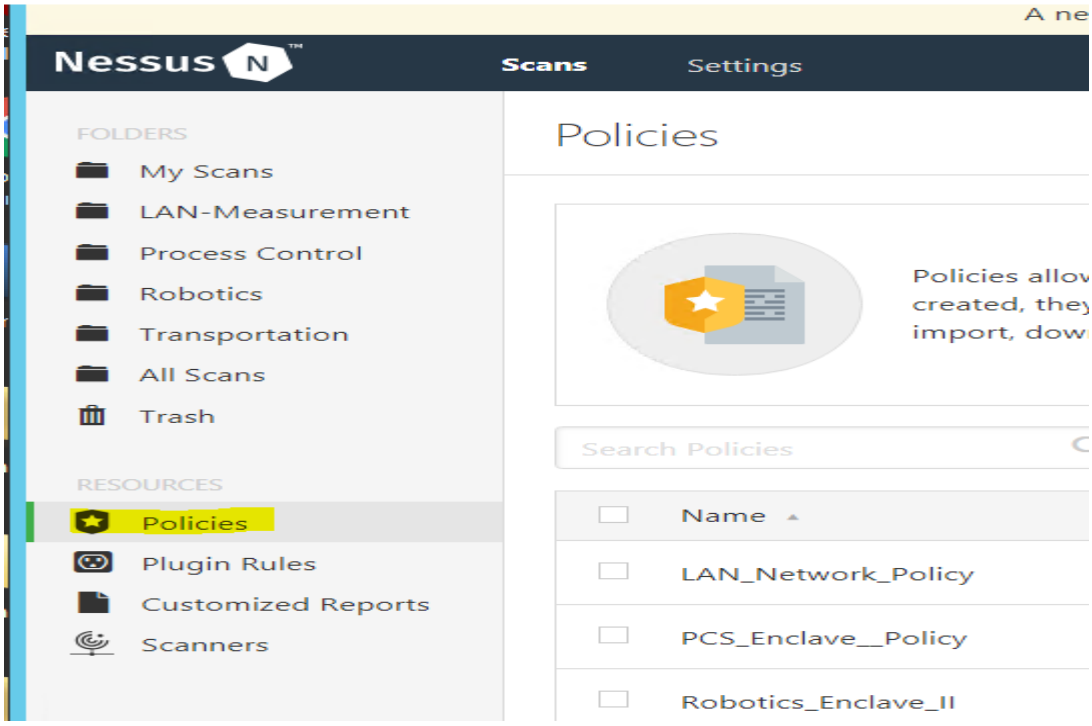
- Run the following command to check if the remote registry is running:

reg query \\x.x.x.x\hklm

If this returns registry keys, the service is running and accessible. If this returns "ERROR: The network path was not found." then the service is not running and must be enabled.

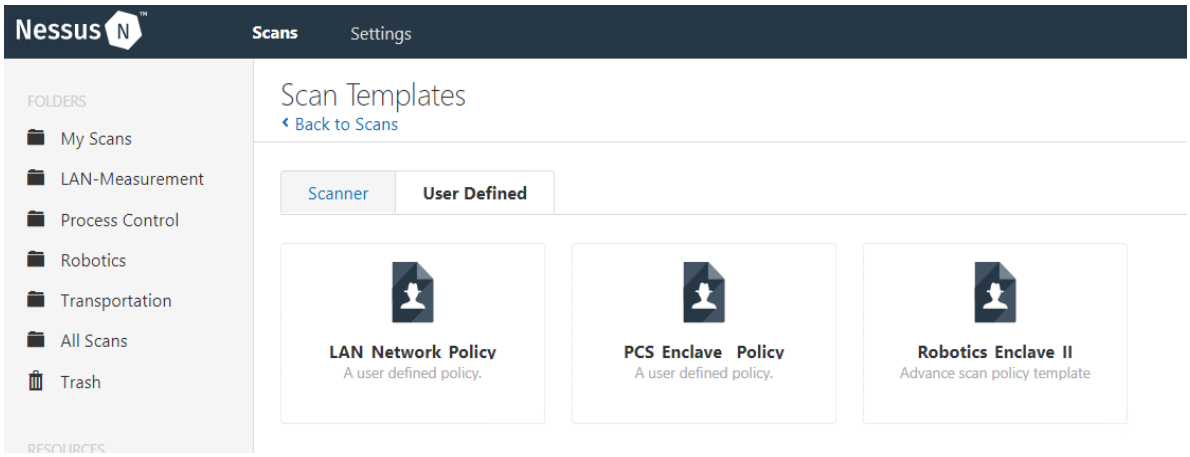
To have a successful credential scan, these commands should not return errors.

- It is recommended to use the "**Policy**" feature of Nessus for performing **credentials check**s, A Policy lets you create a scan template where in device credentials and other custom settings can be saved for scanning assets. Once created, a policy can then later be assigned to a scan.
- To create a policy, Click on "**Policies**" from the left-side explorer bar and further click on "**New Policy**" button.



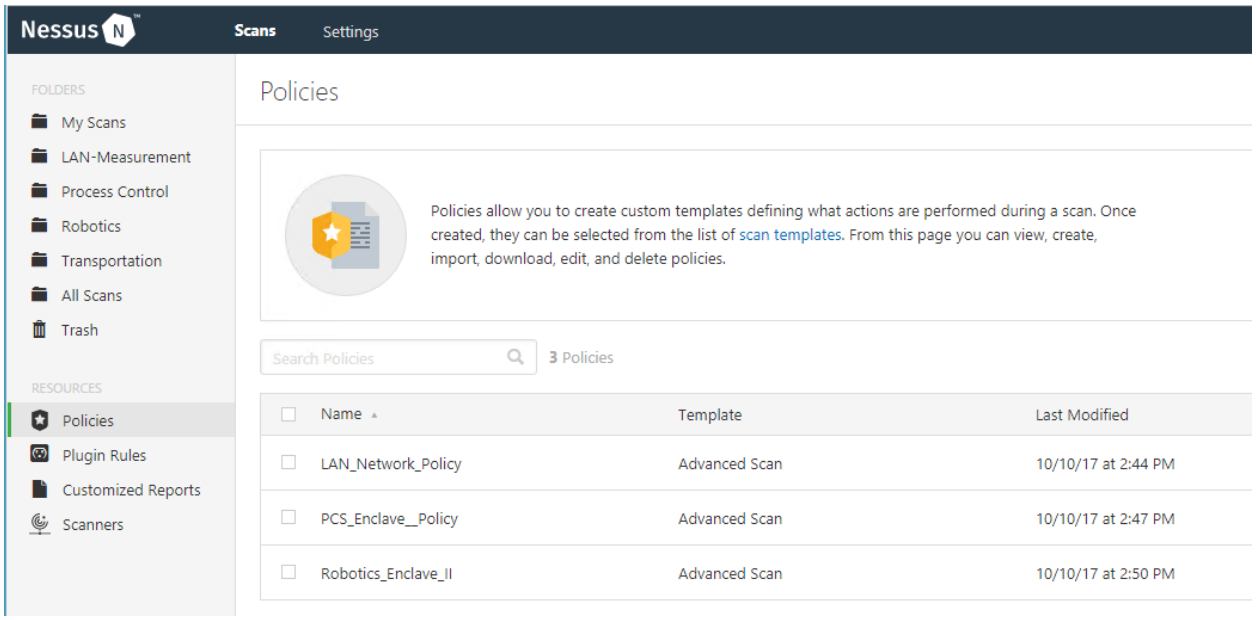
- Choose from any on the default templates available. The "**Advanced Scan**" template was selected for our use. Click on "Credentials" tab under a template to configure host based credentials (SSH, Windows, SNMP, etc.). Hit **Save** when done.

- Next, Create a Scan. On the home-page, click "Scans" from left-side explorer bar >> **New Scan >> User Defined >> Select <Policy> >>** Enter **a Name, Description** and **Network Range or Host IP addresses. Hit Save.**

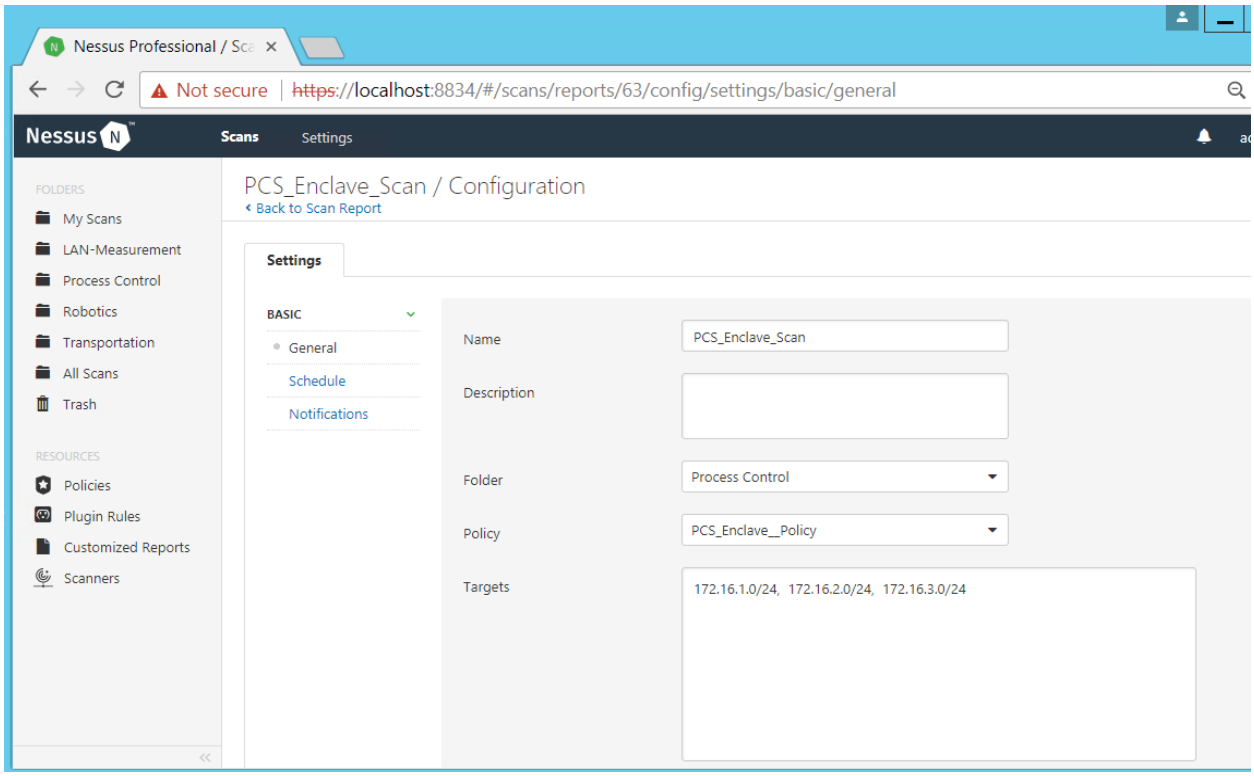


- Click **"All Scans"** >> Click on the **<Scan>** created above >> Under **Policy**, Select the appropriate Policy from the drop down list to associate the scan with a policy. Click **Save**.

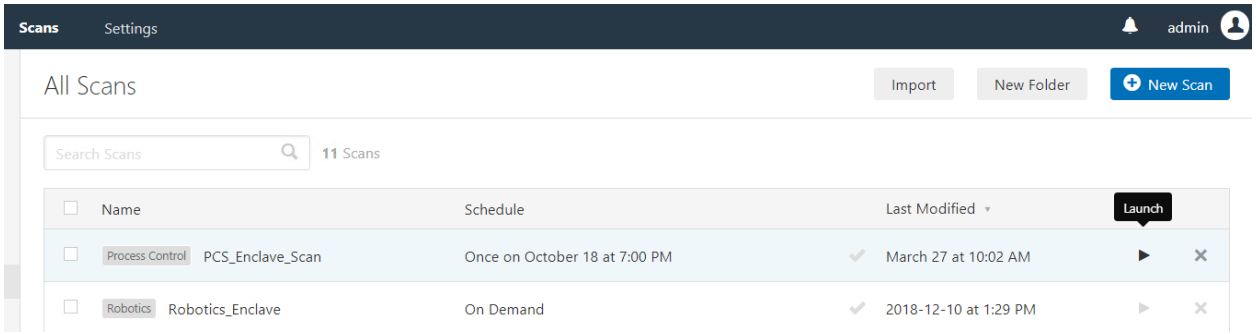
- The figure below shows the different policies created in our Nessus Manager specific to each system. The policy for this Process Control system is named "**PCS_Enclave_Policy**"



- The figure below shows the corresponding scan job settings which has the "**PCS_Enclave_Policy**" assigned to it



- To kick-off a manual on-demand scan, click on the launch button next to the scan.



4.11.6 Highlighted Performance Impacts

The following performance measurement experiment was performed for the Nessus vulnerability assessment tool while the manufacturing system was operational:

Experiment PL006.1- Nessus vulnerability network scan

There was no significant performance impact to the manufacturing process was observed during the Nessus vulnerability scan. No significant network traffic increased during the Nessus scan was observed. For example, the packet round trip time from the Controller to OPC stayed mostly constant throughout the Nessus scan.

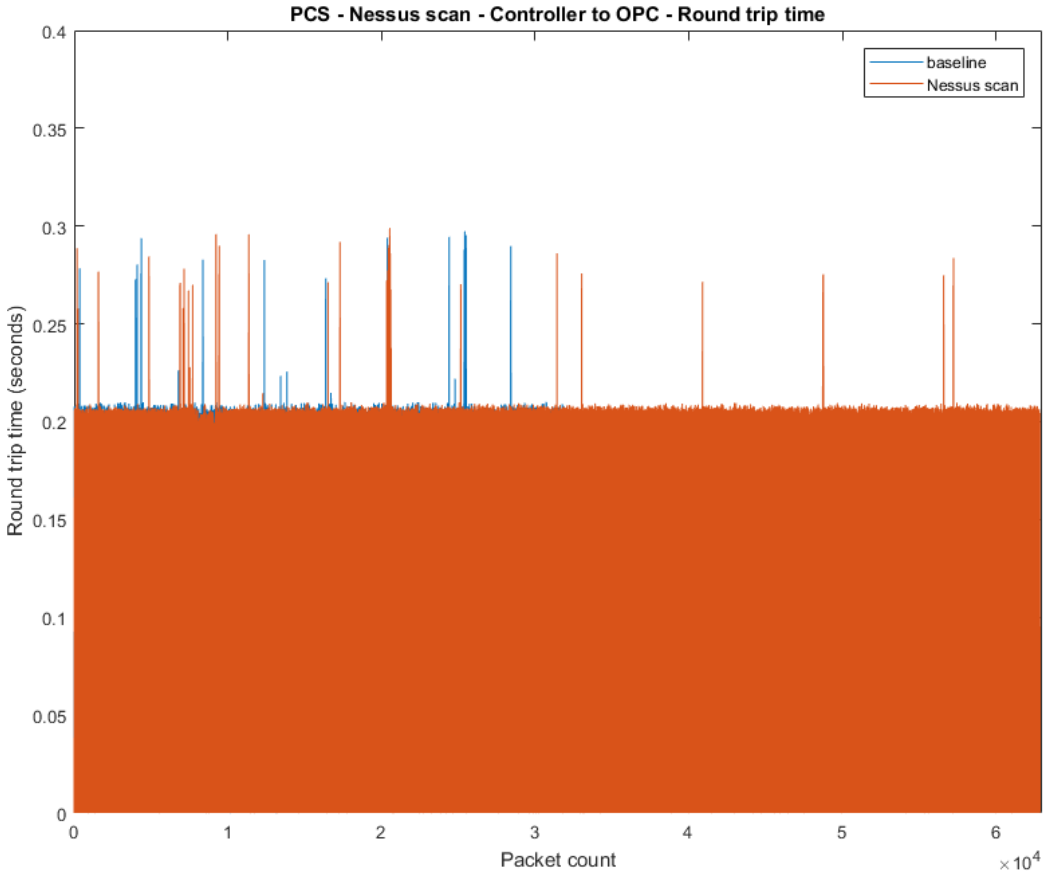


Figure 4-26 Packet round trip time from Controller to OPC during Nessus scan

Some part of the system recorded a slightly increased network traffic, for example, the network utilization and average bit rate from OPC to HMI during the Nessus scan was about 14.11% and

1.41Mbit/sec respectively, while the baseline is 13.81% and 1.38Mbit/sec respectively The network utilization from PLC to OPC during the Nessus scan was about 2.2% higher than baseline.

The performance of the manufacturing process mostly remained the same. For example, the product flow and the reactor pressure remained align with the baseline measurement.

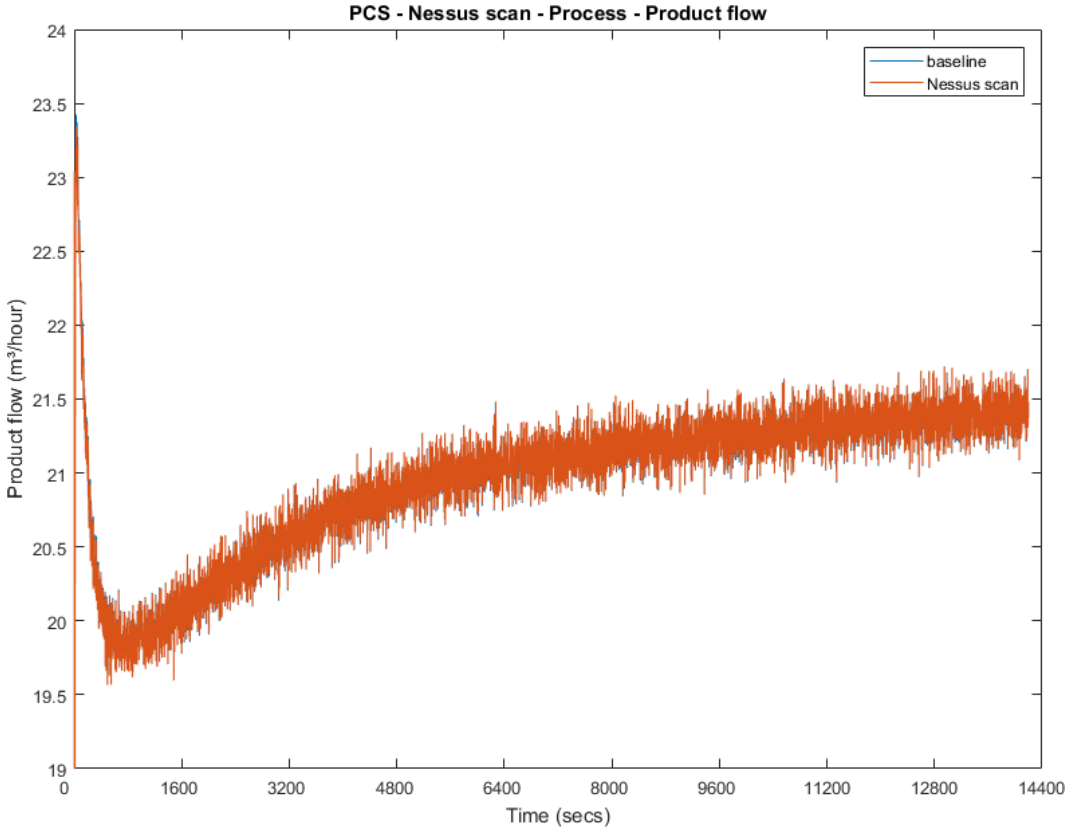


Figure 4-27 Manufacturing process product flow rate at Nessus scan

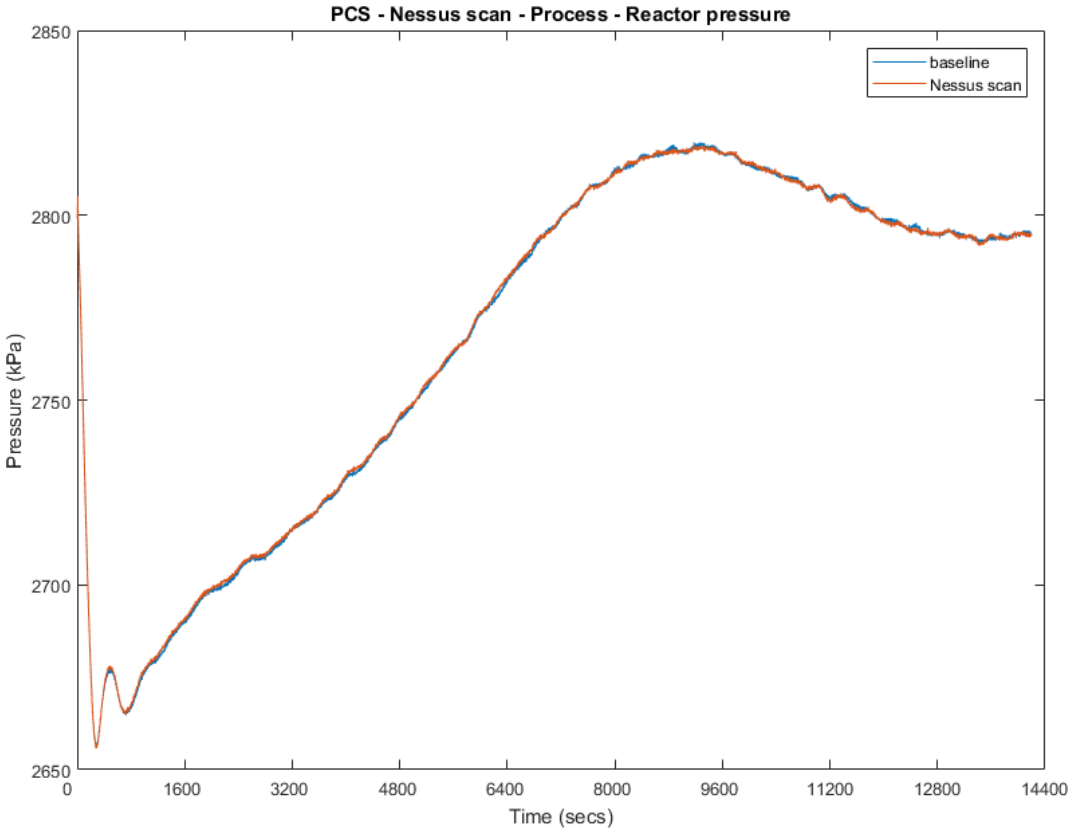


Figure 4-28 Manufacturing process reactor pressure at Nessus scan

4.11.7 Link to Entire Performance Measurement Data Set

Nessus KPI data

Nessus measurement data

4.12 NamicSoft

4.12.1 Technical Solution Overview

NamicSoft Scan Report Assistant, a parser and reporting tool for Nessus, Burp, Nexpose OpenVAS and NCATS.[25]

4.12.2 Technical Capabilities Provided by Solution

NamicSoft provides components of the following Technical Capabilities described in Section 6 of Volume 1:

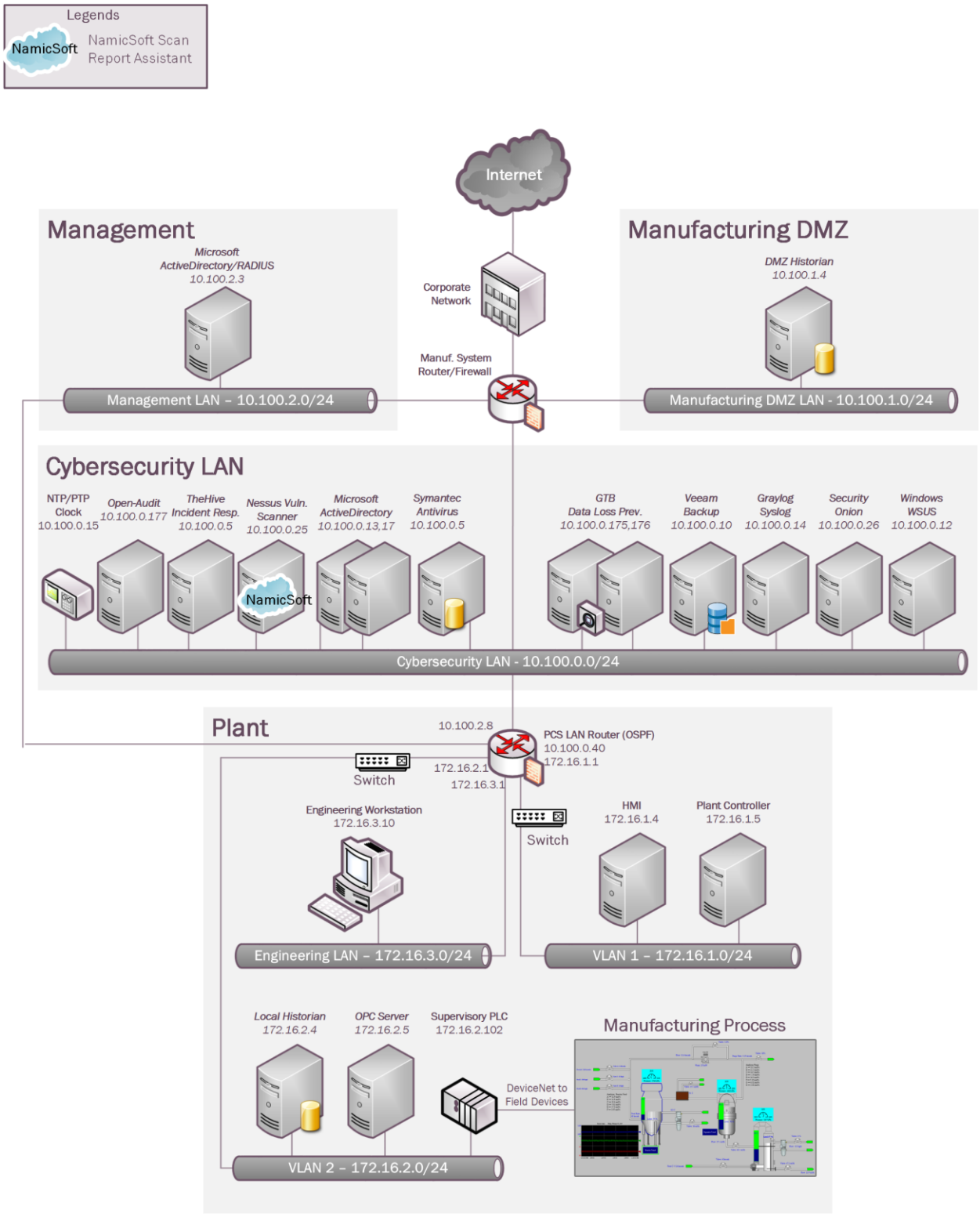
- Vulnerability Management

4.12.3 Subcategories Addressed by Implementing Solution

ID.RA-1, DE.CM-4, RS.MI-3

[25] Namicsoft https://www.namicsoft.com/

4.12.4 Architecture Map of Where Solution was Implemented



4.12.5 Installation Instructions and Configurations

Details of the solutions implemented:

Name	Version
NamicSoft Scan Report Assistant	3.5.0

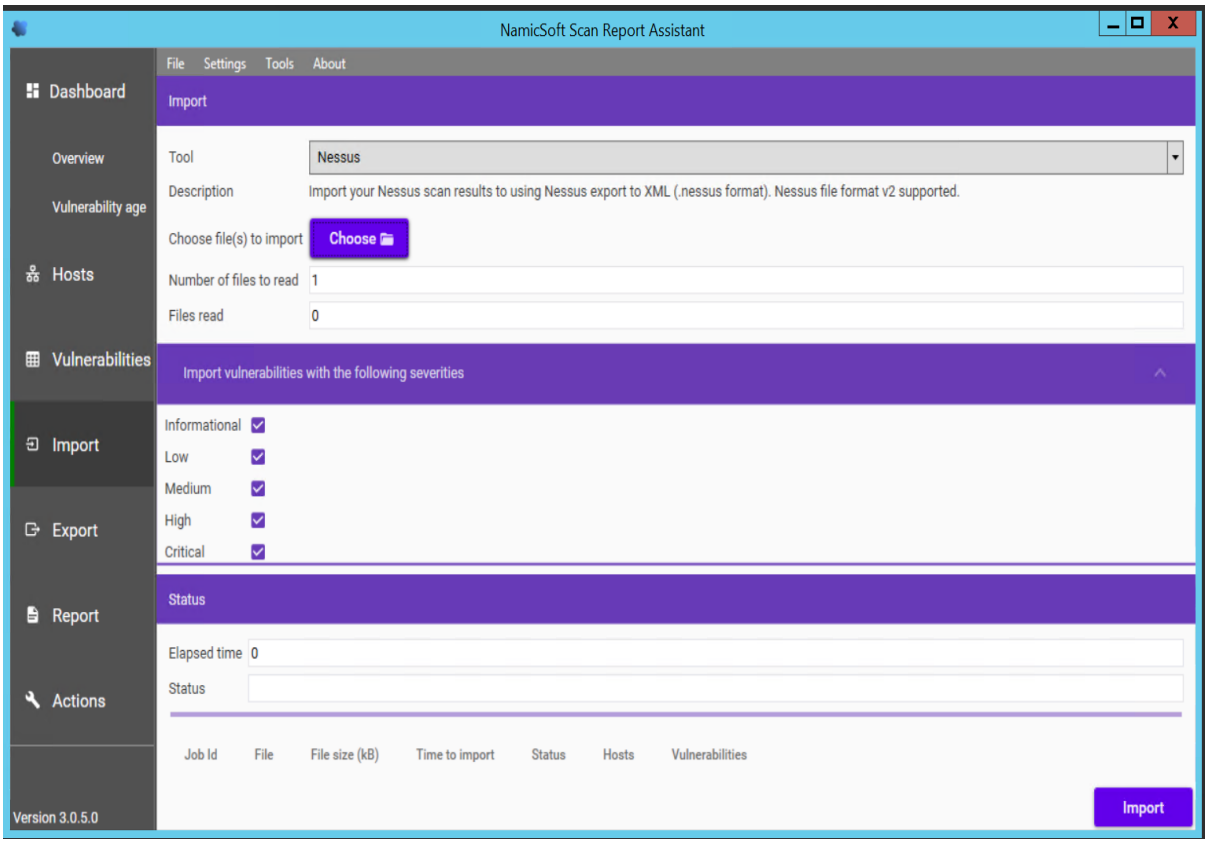
Setup:

- Download NamicSoft from https://www.namicsoft.com and run the installer on a Windows PC. NamicSoft is currently supported on 64-bit Windows with .Net Framework 4.5 installed
- The installation is tied to a user account. Any changes made by a user would not be visible to a different user logging in to the same system.
- If using for the first time, the installation will prompt for a license file. If a license is not entered, it runs in free mode. The free mode is limited to five hosts.
- NamicSoft was installed on the Nessus Server itself in the Cybersecurity LAN network of our Process Control System.

Configuration for reporting Nessus scans:

- Export a Scan Report of **nessus** format from the Nessus web interface.
- Launch NamicSoft Report Assistant. Click **Import** on left-side explorer, select **Nessus**

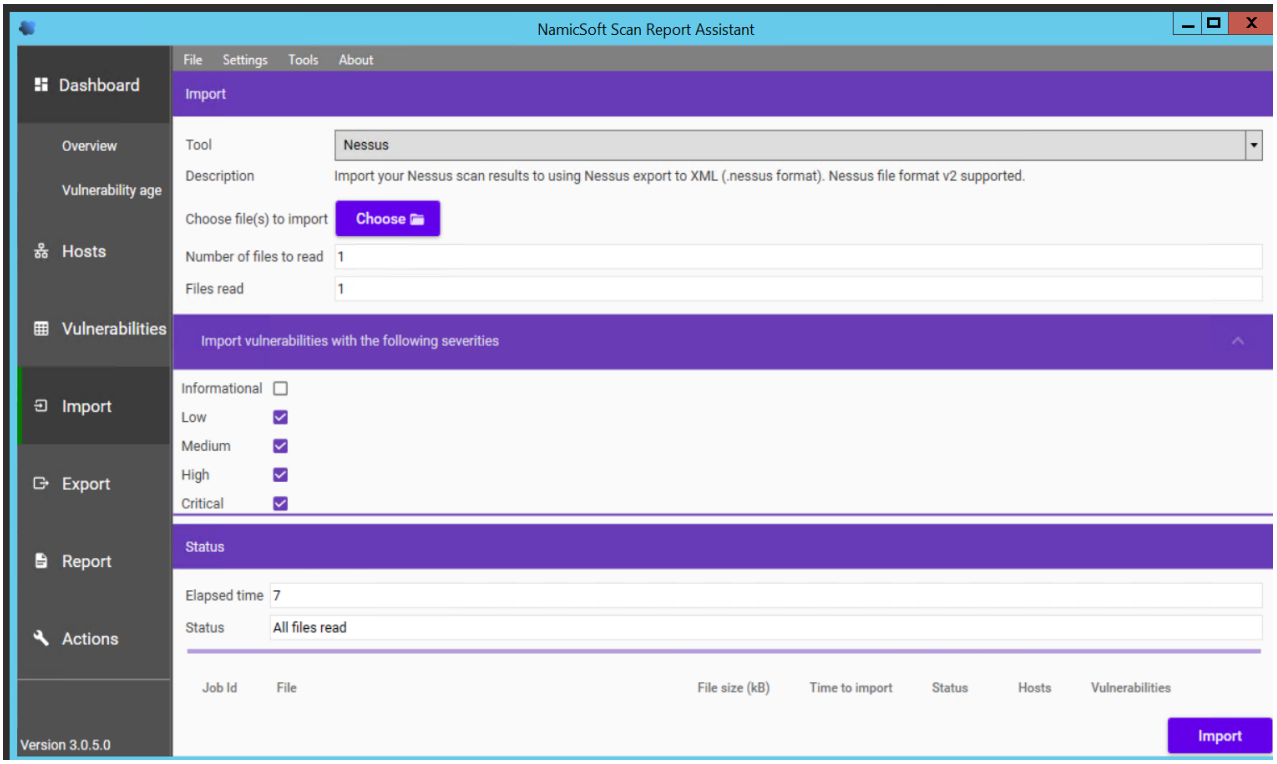
- Click on **Choose** button to import files



- Browse to the nessus scan report. Under **Import Vulnerabilities with following vulnerabilities, C**heck / Un-check whichever severity of vulnerabilities you wish to be included in the report. Click **Import**

4637 The below image shows "Informational" type being excluded. When the **Import** finishes, the
4638 Status bar should display **All files read**

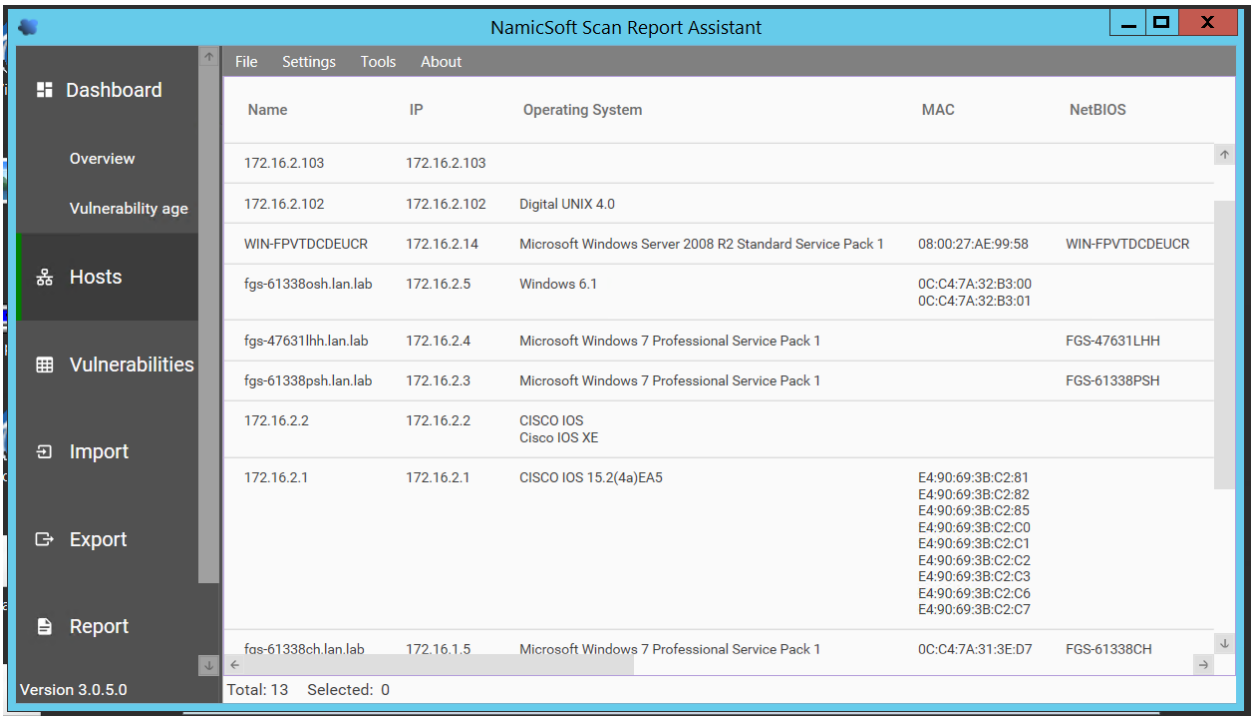
4639

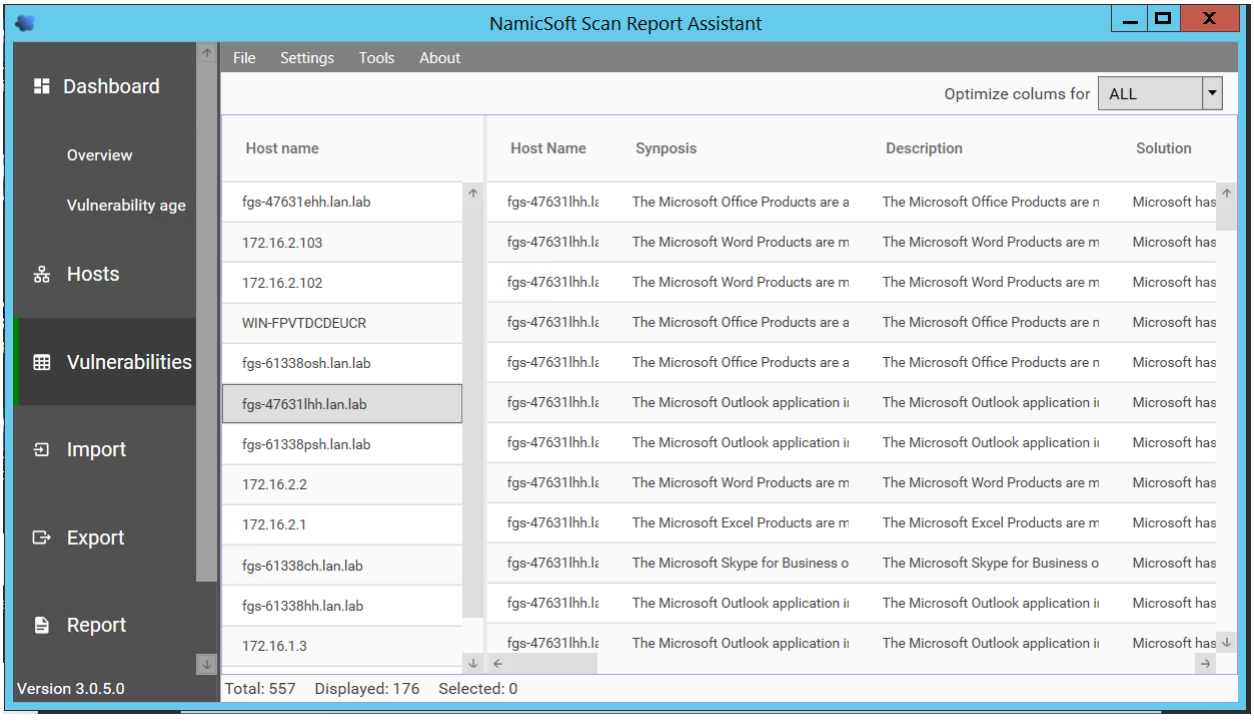


4640

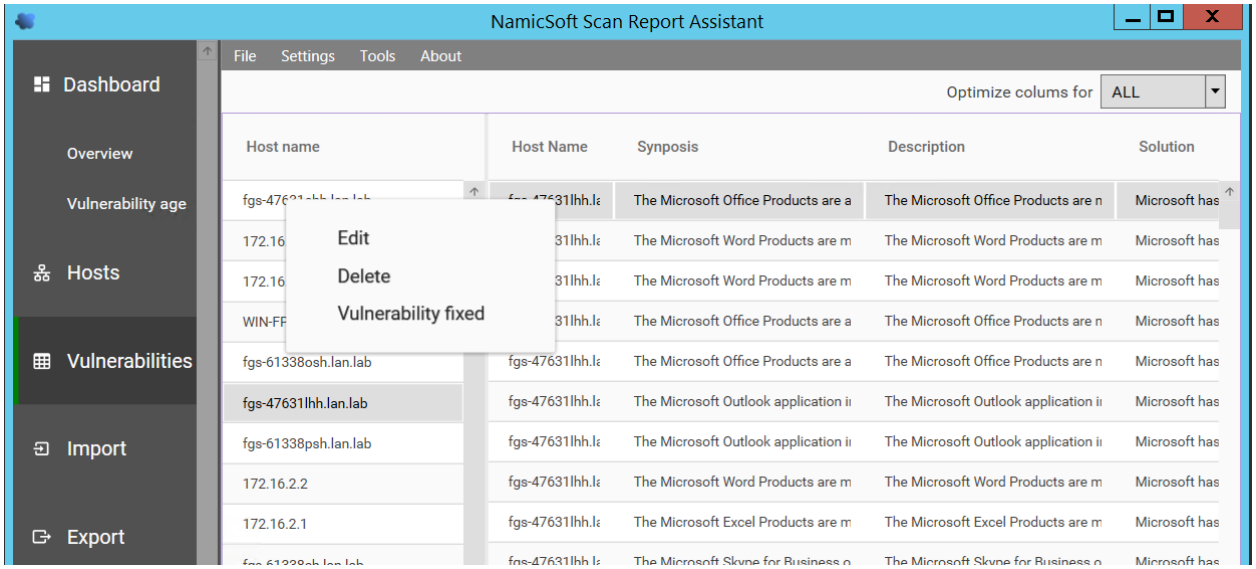
4641

- Upon completion of Import, go to **Hosts** page to view all the hosts level summary. Similarly, clicking on **Vulnerabilities** page shows all the vulnerabilities



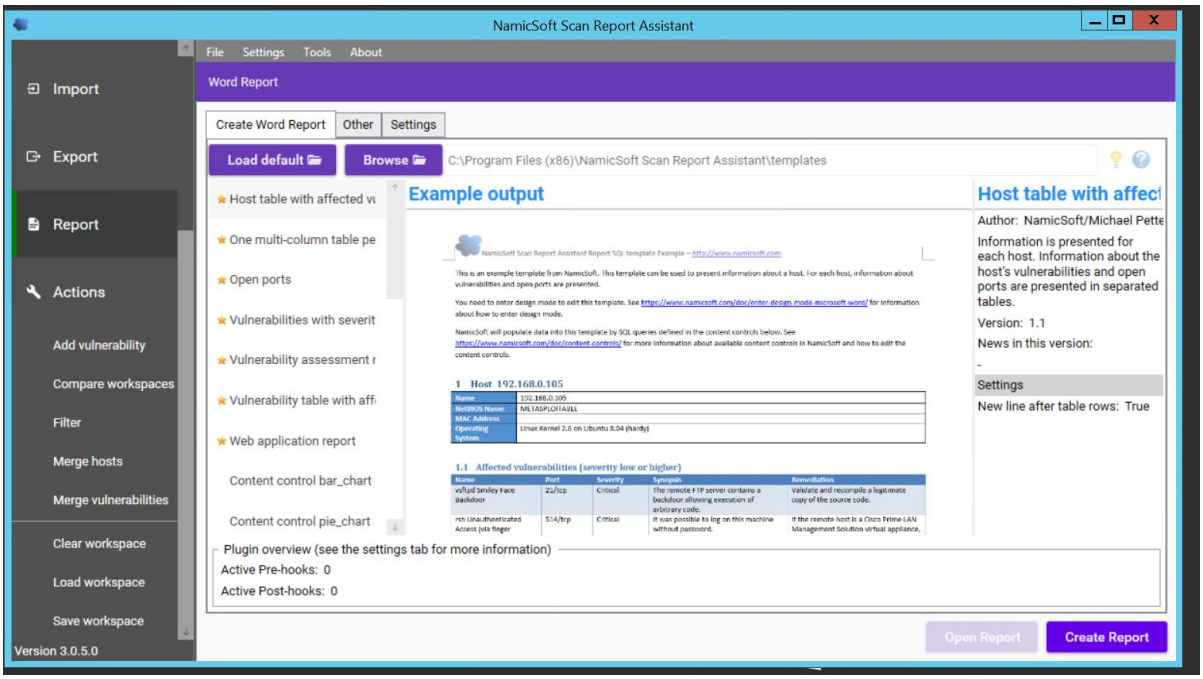


To mark a Vulnerability as Fixed, select the Vulnerability >> Right Click >> Vulnerability Fixed.

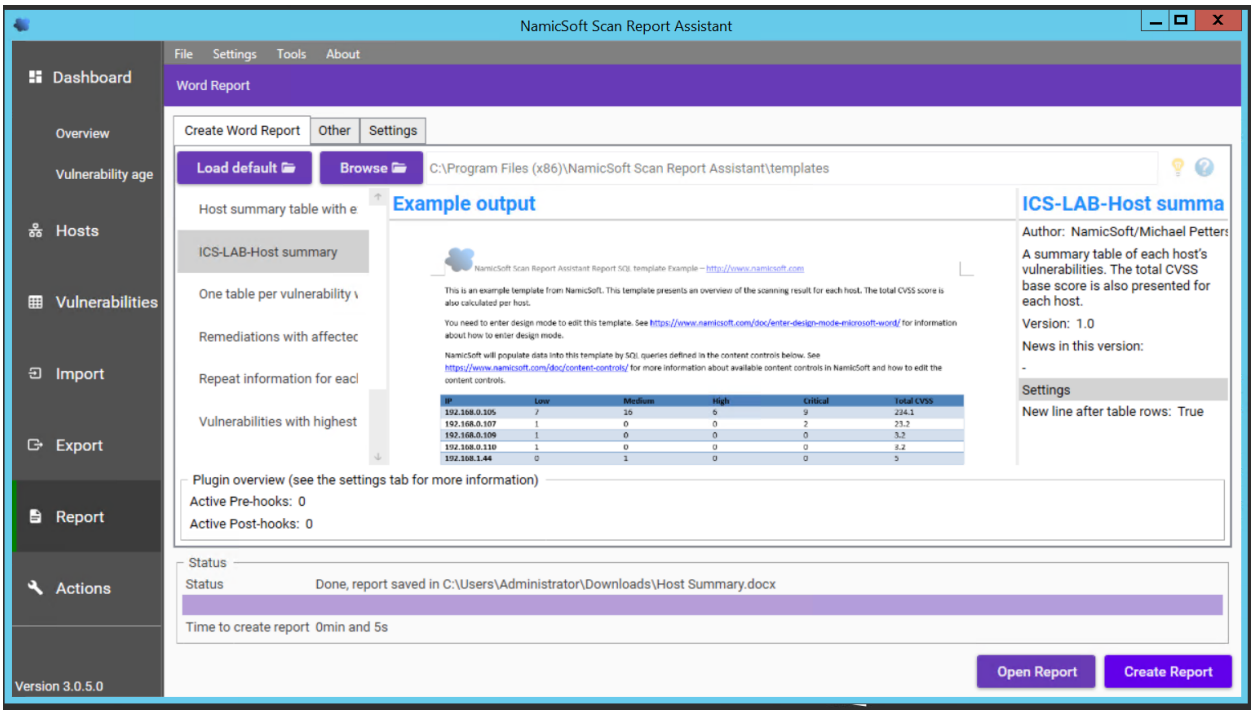


- Under **Actions**, click on **Save Workspace**. Ensure to **Save your workspace** after every change made. When running NamicSoft the next time, you can load this saved workspace file.

- To generate a Report, click on **Report.** You can select one of the default reporting templates from the list or create a custom one. To use a default template, select one from the list >> **Create Report.**



- To view the Report, click **Open Report.**



- To create a custom template, copy one of the template files located under **C:\Program Files(x86)\NamicSoft Scan Report Assistant\templates** and save it to a different folder. Open the copied file in MS Word to begin editing. The image below shows a customized template file created for CRS system. This report generates a summary of hosts and their respective vulnerabilities based on the Severity level.

National Institute of Standards and Technology
U.S. Department of Commerce

Vulnerability Assessment Report

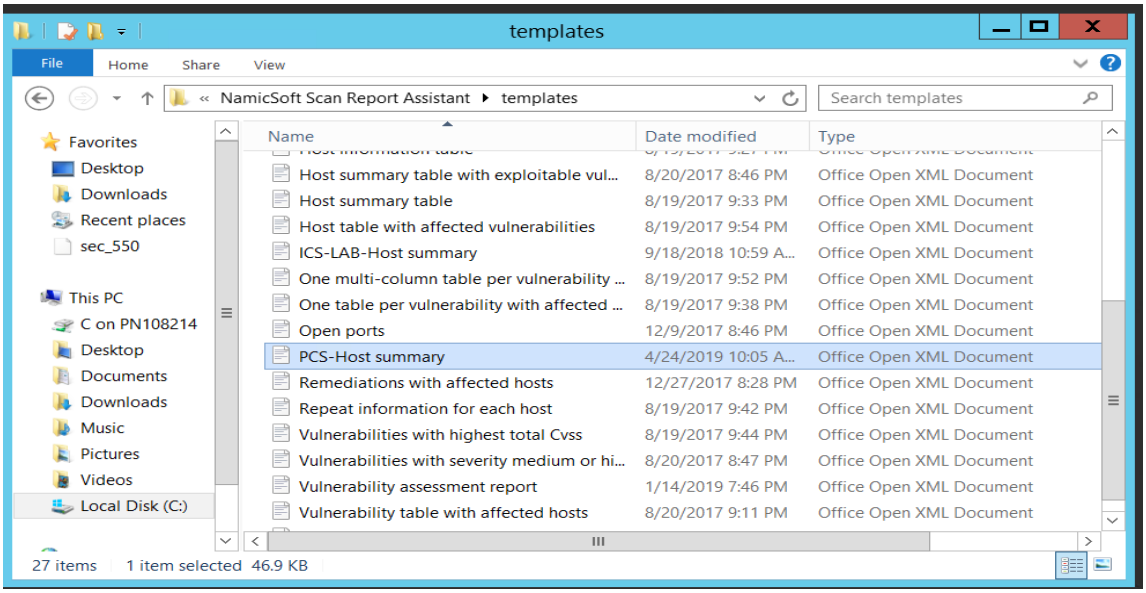
Process Control System Vulnerability Scan Summary

IP	Hostname	Low	Medium	High	Critical	Total CVSS
DummyValue	DummyValue	DummyValue	DummyValue	DummyValue	DummyValue	DummyValue

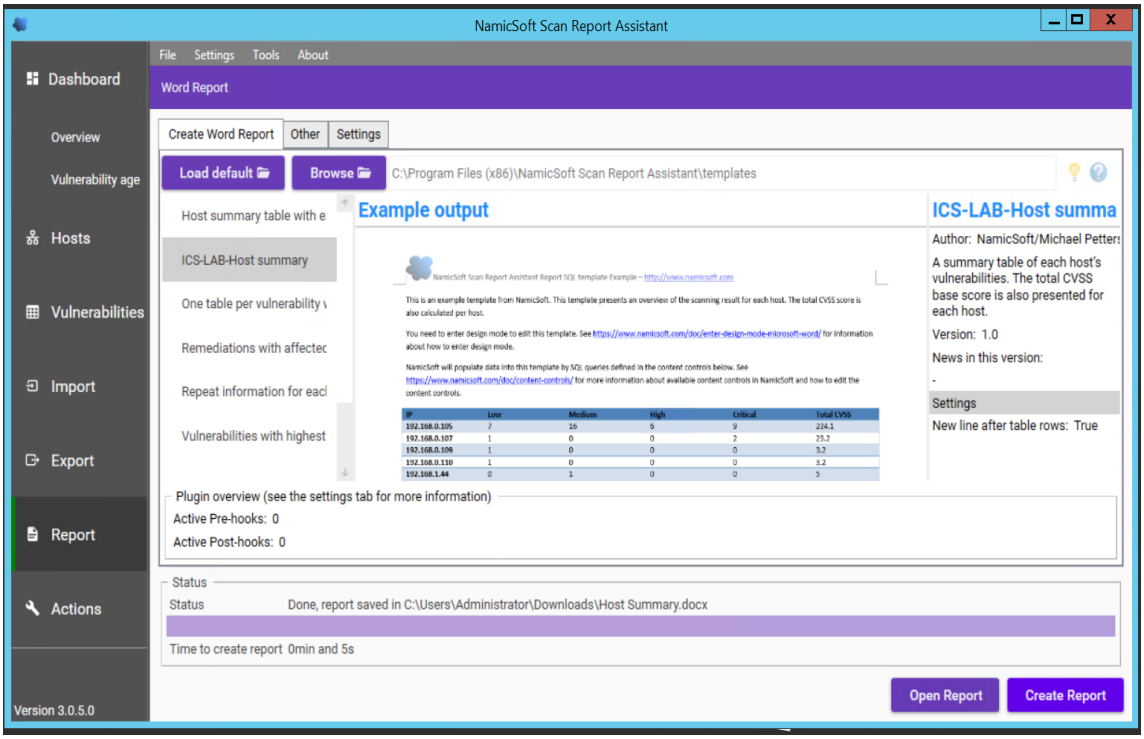
SELECT DISTINCT x.ip, x.hostname, (SELECT COUNT(*) FROM queryTable y WHERE severitynumber=3 AND y.ip=x.ip), (SELECT COUNT(*) FROM queryTable y WHERE severitynumber=2 AND y.ip=x.ip),(SELECT COUNT(*) FROM queryTable y WHERE severitynumber=1 AND y.ip=x.ip), (SELECT COUNT(*) FROM queryTable y WHERE severitynumber=0 AND y.ip=x.ip), (SELECT ROUND(SUM(cvssBaseScore),1) FROM queryTable y WHERE y.ip=x.ip) FROM queryTable x ORDER BY ipSortValue

A summary table of each host's vulnerabilities. The total CVSS base score is also presented for each host.
1.0
-
NamicSoft/Michael Pettersson Solutions AB
Host summary table Image.PNG

- Detailed instructions for creating custom reports are available on the NamicSoft website under https://www.namicsoft.com/doc/content-controls/
- Save your changes and give the file a suitable name. Copy this file back to the "Templates" directory. For instance, the below image shows our customized file – **PCS- Host Summary** copied back to the templates folder.



- Launch NamicSoft again. The custom report should now appear under the list. Select it and click on **Create Report.**



- The output should appear as per your changes.

Vulnerability Assessment Report

Process Control System Vulnerability Scan Summary

IP	Hostname	Low	Medium	High	Critical	Total CVSS
172.16.1.1	172.16.1.1	4	6	2	0	58.6
172.16.1.3	172.16.1.3	1	6	0	0	36.2
172.16.1.4	fgs-61338hh.lan.lab	3	26	39	6	542.3
172.16.1.5	fgs-61338ch.lan.lab	3	24	42	5	547.6
172.16.2.1	172.16.2.1	4	6	2	0	58.6
172.16.2.2	172.16.2.2	0	6	0	0	33.6
172.16.2.3	fgs-61338psh.lan.lab	2	23	41	5	538.3
172.16.2.4	fgs-47631lhh.lan.lab	3	40	122	11	1420.3
172.16.2.14	WIN-FPVTDCDEUCR	3	18	92	11	1047.5
172.16.3.10	fgs-47631ehh.lan.lab	0	0	0	1	10

- To report on Vulnerabilities remediated based off the previous vulnerability scans, use the "**Compare Workspaces**" feature under Action Menu

    - Load Nessus result from your previous scan. Save as a workspace.
    - Clear the workspace in the GUI (or restart NamicSoft)
    - Load Nessus results from the latest scan
    - Open Actions --> Compare workspaces. Choose **Compare** with current workspace and point Workspace 2 to your workspace saved earlier.
    - Choose Excel output file (target)
    - Click "Compare Workspaces"

4.12.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the use of NamicSoft due to its installation location and how it was used (i.e., the software performed offline analysis of vulnerability data captured by other software at a location external to the manufacturing system).

4.12.7 Link to Entire Performance Measurement Data Set

N/A

4.13 The Hive Project

4.13.1 Technical Solution Overview

A scalable, open source and free Security Incident Response Platform, tightly integrated with MISP (Malware Information Sharing Platform), designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.[26]

4.13.2 Technical Capabilities Provided by Solution

The Hive Project provides components of the following Technical Capabilities described in Section 6 of Volume 1:

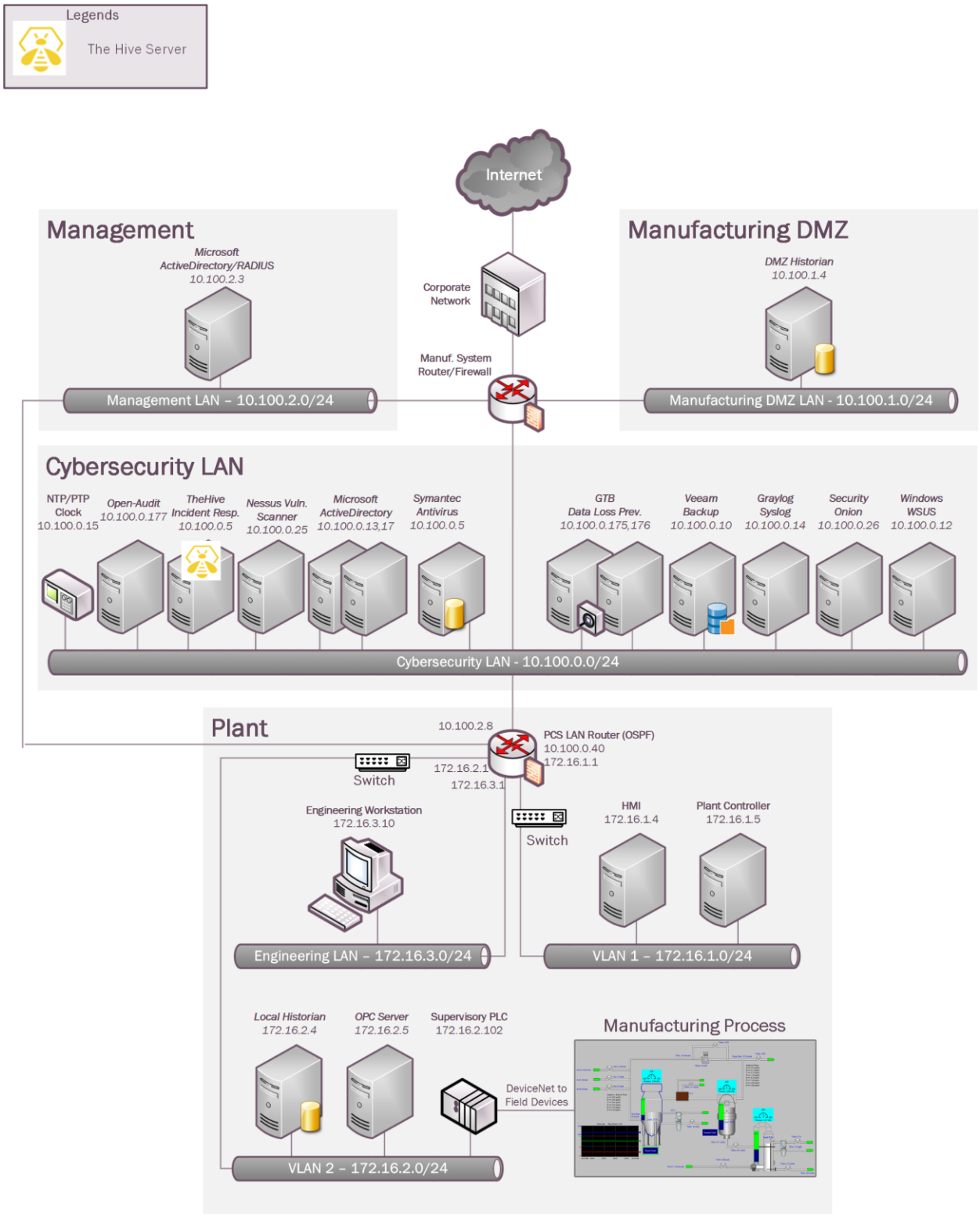
- Incident Management

4.13.3 Subcategories Addressed by Implementing Solution

RS.MI-2 and RS.MI-3

[26] The Hive Project: https://thehive-project.org/

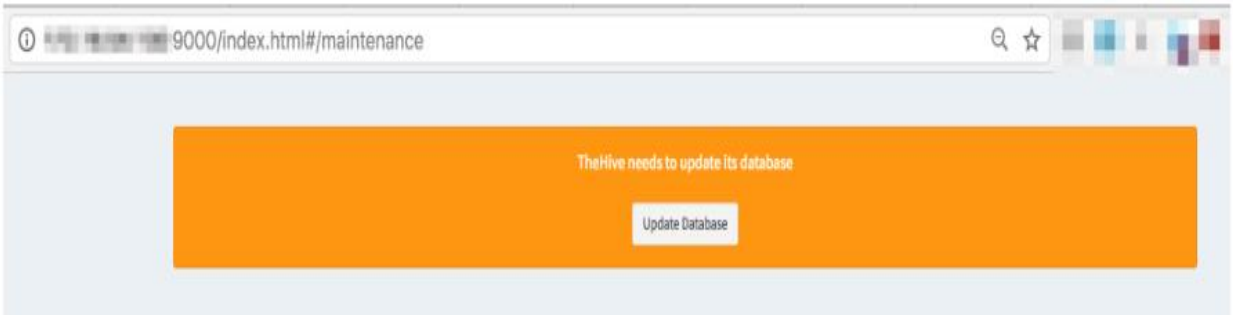
4.13.4 Architecture Map of Where Solution was Implemented



4.13.5 Installation Instructions and Configurations

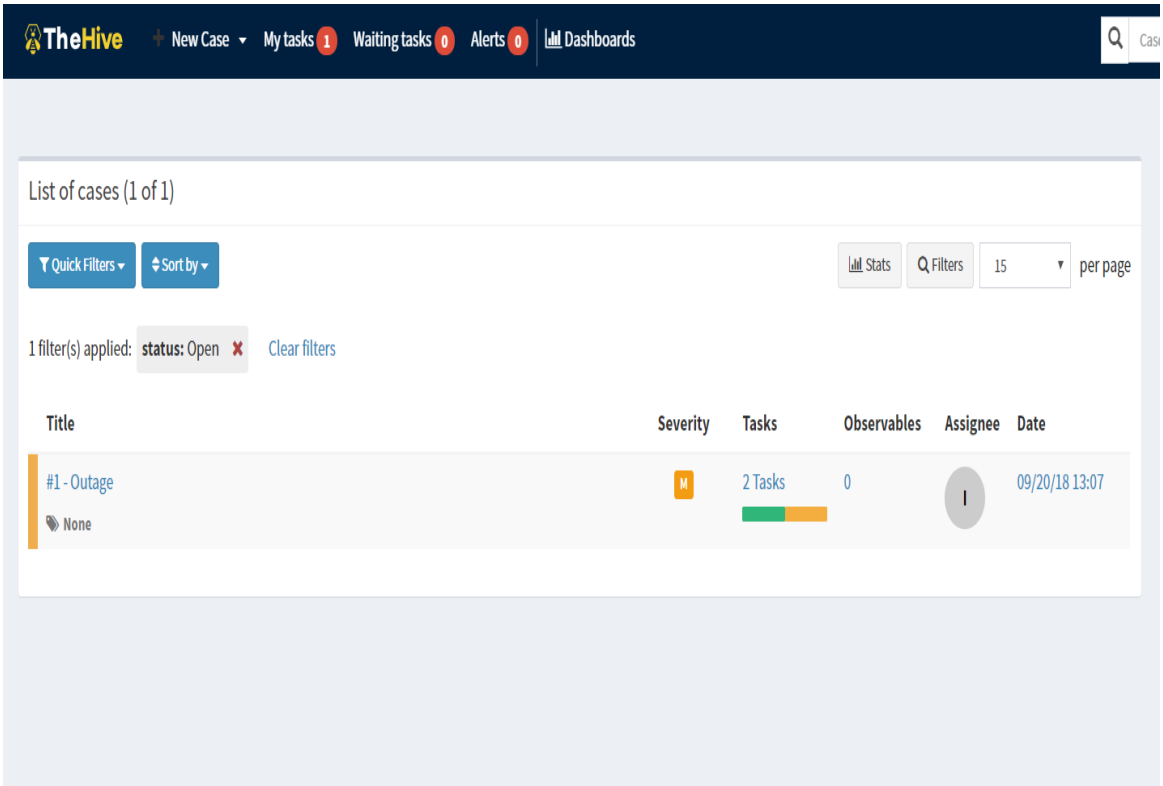
Setup:

- The Hive Project's website provides detailed setup guide for Linux platform. Additionally, there is a preconfigured training VM available for non-production environments. This can be downloaded from https://github.com/TheHive-Project/TheHive
- The preconfigured VM was deployed in our environment. Deploy the ova file on a Hypervisor and assign the VM a static IP address. Once done, the URL of application is
- http://IP_OF_VM:9000
- The first time you access **TheHive**, you'll need to create the associated database by clicking on the **Update Database** button as shown below:

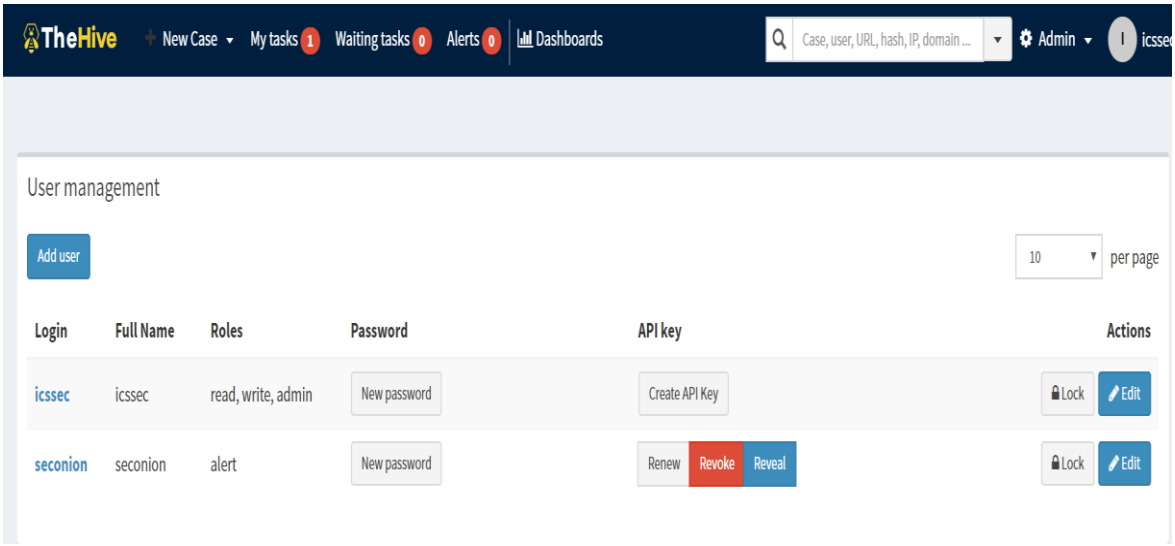


- Follow the wizard to setup a user account. Login to TheHive url with these credentials.

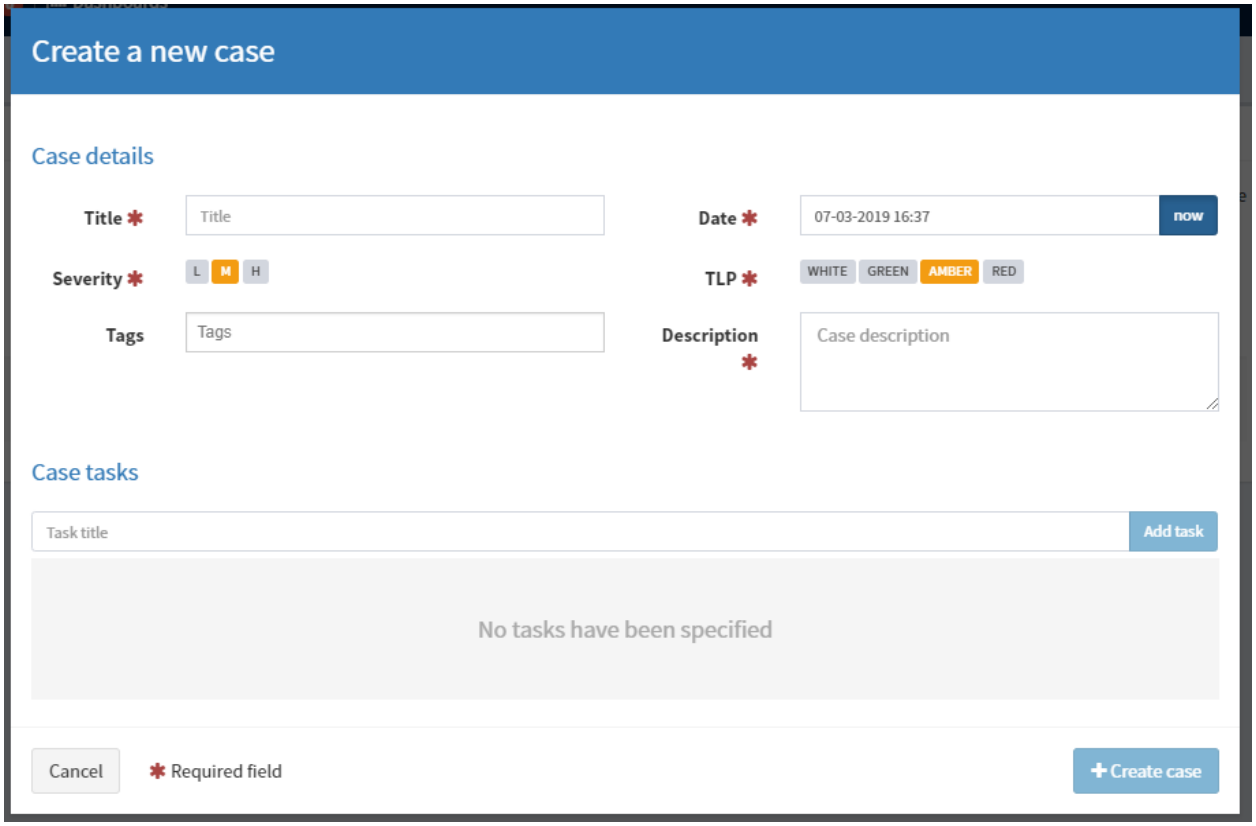
- The default page will show you a List of Cases assigned to your account



- User accounts can be created by going to **Admin** >> **Users** >> **User Management** page. Click on "+Add User" to create a new user.



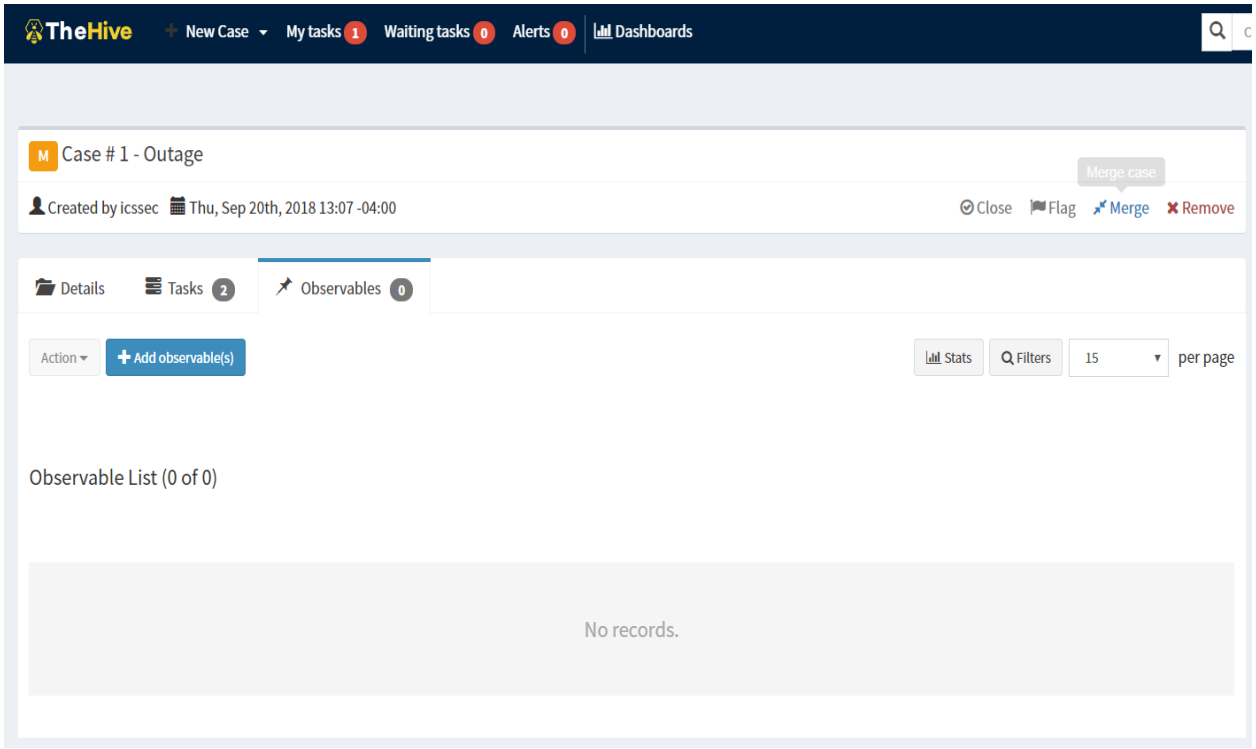
- To create a new Incident / case, click on the "New Case" menu option and fill in all the details. Hit "Create Case" button when done.



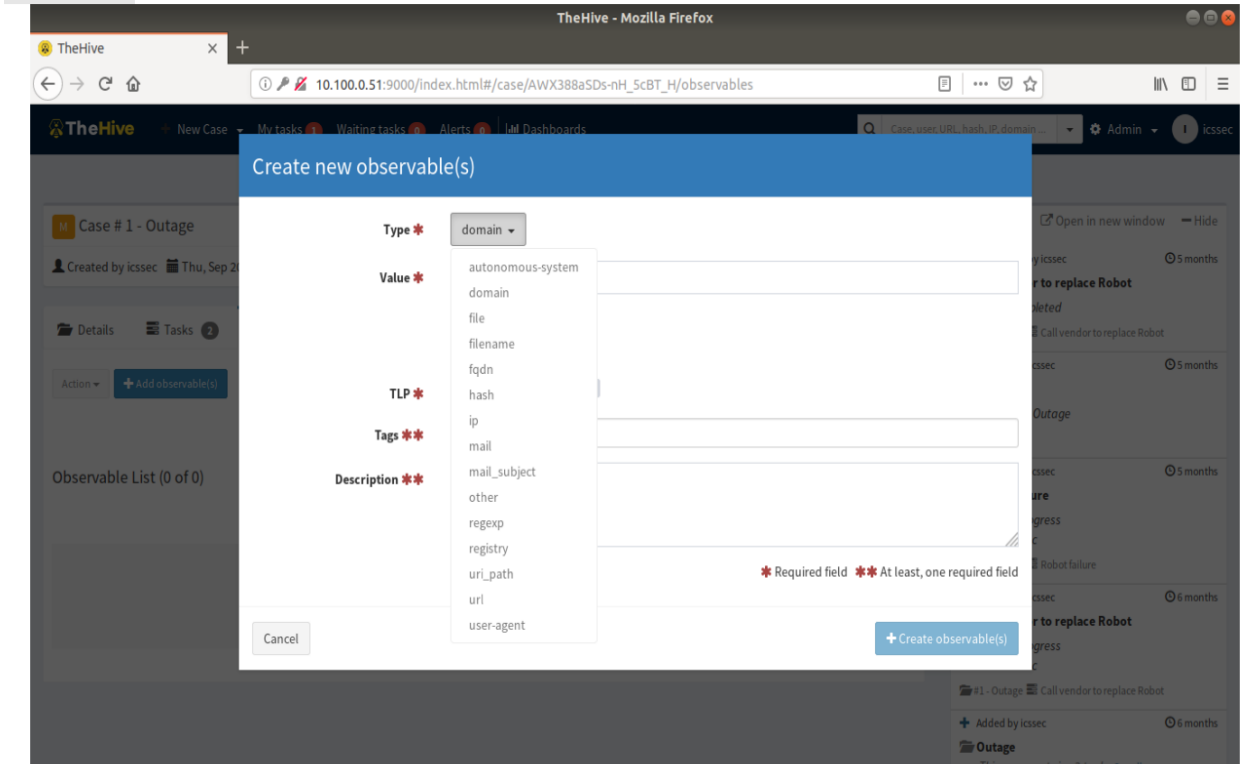
- Once you've created a case, you can create, assign, and track tasks within a case. A task can be useful to track status updates or notes within a case. Click on "**+Add Task**" to add a task description under a case. Each task can be individually assigned to an analyst for the work to be performed. By default, a task doesn't have an owner until someone clicks into it, or "takes" it from the Waiting tasks queue in the top menu bar.

- Custom Case templates can be created via the Case Template Management Screen. Click on **+New Template** button to create a new template of your own.

- Custom "Observables" such as domain names, IP addresses, files, filenames etc. can be added to a case by clicking on "**Observables**" tab >> **+Add Observables**. In addition, observables can also be marked as Indicators of Compromise (IOC).



4756
4757



4758
4759

- Analysts can use "Cortex" engine to perform detailed analysis on observables or IOCs such as domain names, IP addresses, hashes. This can be achieved by enabling or creating Analyzers in Cortex. The default URL for Cortex Web UI is http://<CORTEX_IP>:9001

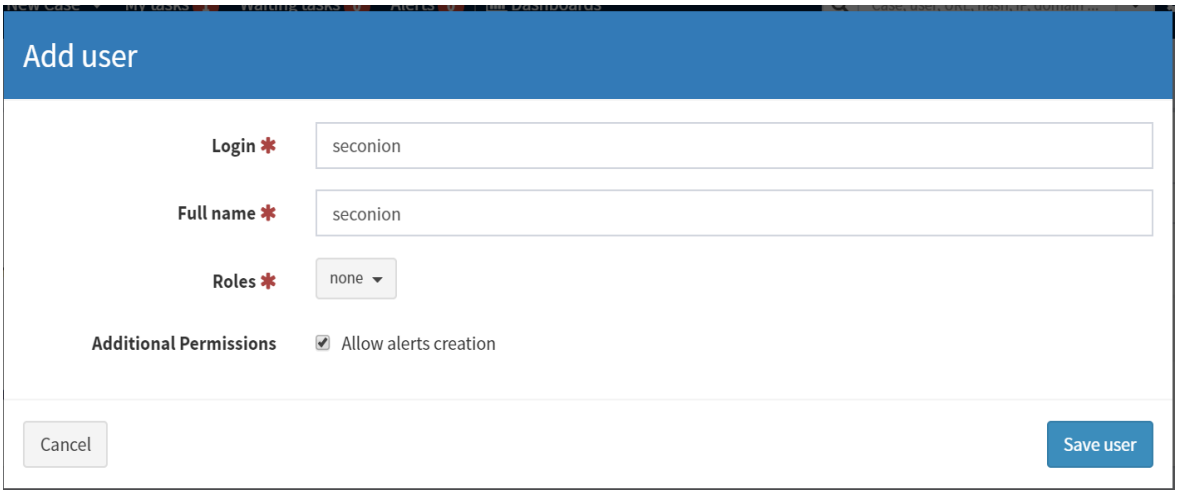
  The high-level steps in configuring Cortex are:

  i. Setup Cortex
  ii. Create an Administrator account
  iii. Create an Organization
  iv. Create an Organization Administrator account
  v. Enable or Configure Analyzers
  vi. Integrate with the Hive instance

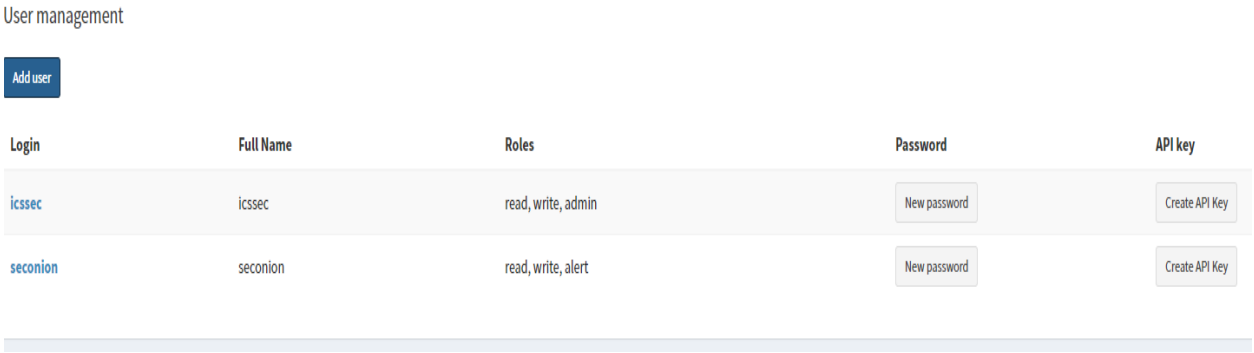
  Detailed instructions on setting up Cortex are available at https://github.com/TheHive-Project/CortexDocs

Integration with Security Onion

- Integration with other products can be done via API keys to connect with the Hive. A dedicated user account was created for this purpose with permissions to "Allow alerts creation". Ensure **Roles: None** is set for security purposes of this user account.



- An API key was created for this user, by clicking on "**Create API Key**" for this dedicated user account



- Our Security Onion instance was integrated with the Hive Instance to create a case for IDS alerts generated by Security Onion. This was accomplished by creating a new rules file **hive.yaml** under the **/etc./elastalert/rules** directory of the Security Onion server. Detailed instructions are available at https://securityonion.readthedocs.io/en/latest/hive.html#thehive .

Extract from our hive.yaml

```
# hive.yaml
# Elastalert rule to forward IDS alerts from Security Onion to a specified TheHive instance.
#
es_host: elasticsearch
es_port: 9200
name: TheHive - New IDS Alert!
type: frequency
index: "*:logstash-ids*"
num_events: 1
timeframe:
   minutes: 10
buffer_time:
   minutes: 10
allow_buffer_time_overlap: true

filter:
- term:
   event_type: "snort"

alert: hivealerter

hive_connection:
  hive_host: https://10.100.0.51
  hive_port: 9000
  hive_apikey: APIKEY
```

4.13.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the use of the Hive Project due to its typical installation and usage location (i.e., external to the manufacturing system).

4.13.7 Link to Entire Performance Measurement Data Set

N/A

4.14 Microsoft EFS

4.14.1 Technical Solution Overview

EFS is file level encryption tool provided by Windows. The Encrypted File System, or EFS, provides an additional level of security for files and directories. It provides cryptographic protection of individual files on NTFS file system volumes using a public-key system.[27]

4.14.2 Technical Capabilities Provided by Solution

Microsoft EFS provides components of the following Technical Capabilities described in Section 6 of Volume 1:

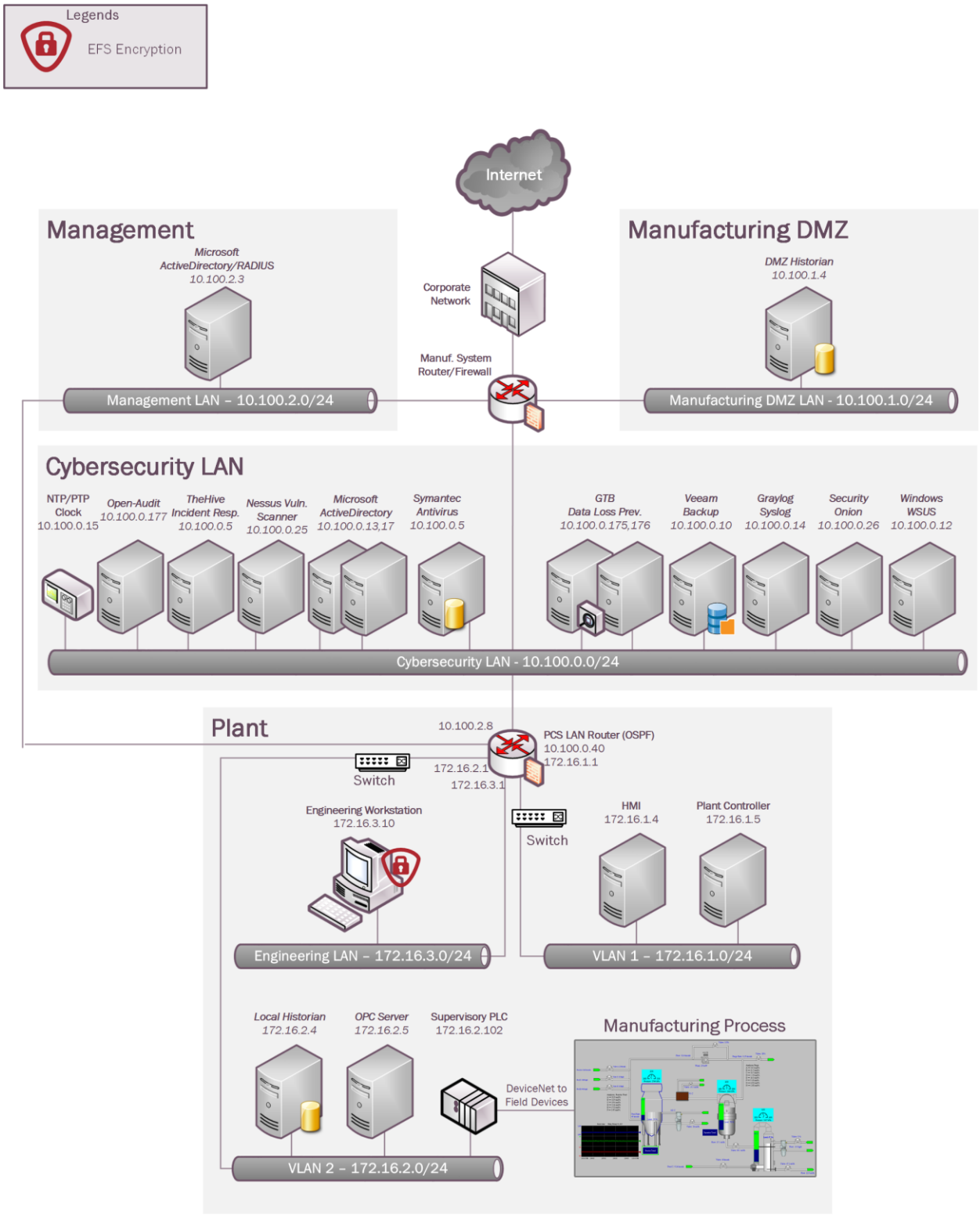
- Encryption

4.14.3 Subcategories Addressed by Implementing Solution

PR.DS-5

[27] https://docs.microsoft.com/en-us/windows/desktop/fileio/file-encryption

4.14.4 Architecture Map of Where Solution was Implemented



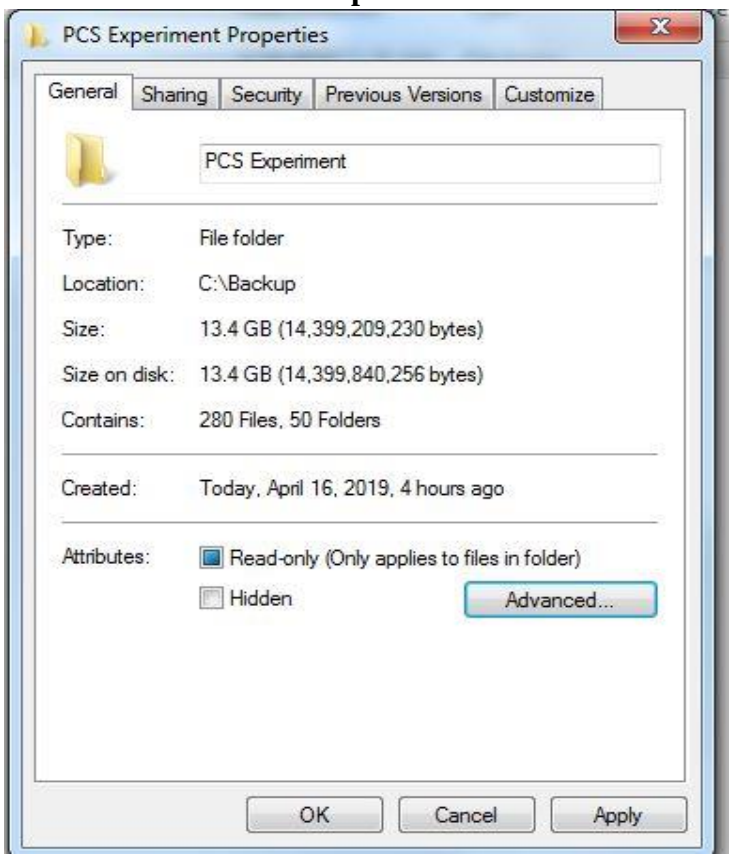
4.14.5 Installation Instructions and Configurations

Setup:

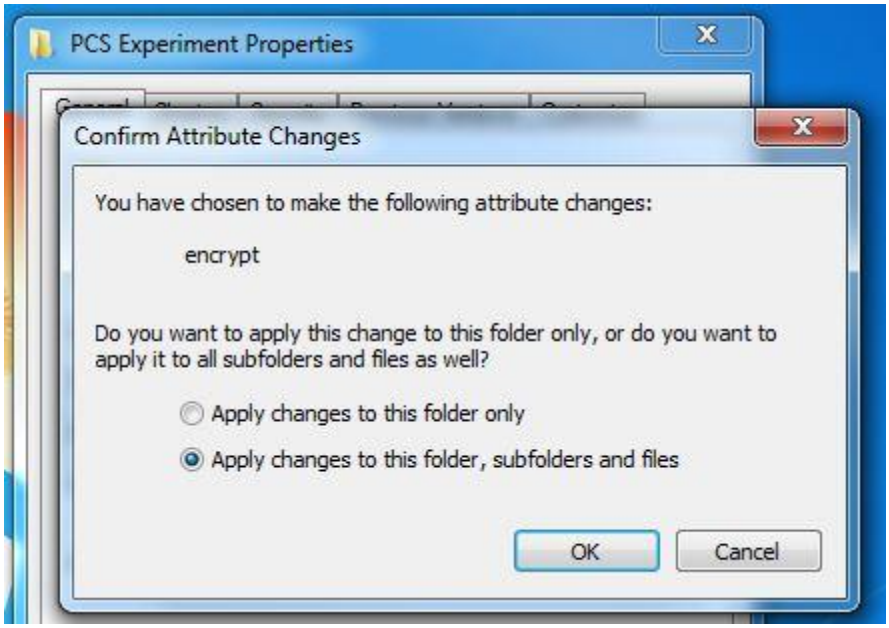
Note: These steps were performed on the below system

Hostname	IP_Address	OS
Engineering Workstation	172.16.3.10	Windows 7 Professional 64bit

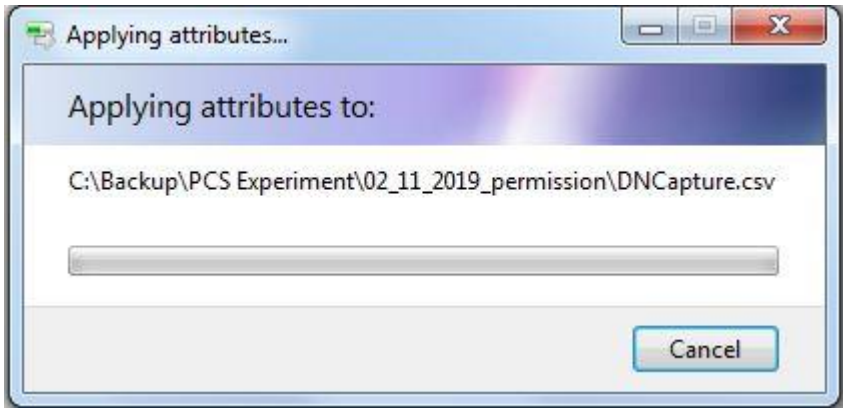
- Windows EFS was used to encrypt confidential folders on the Windows workstation of Process Control System.
- To begin encrypting, select a parent folder which you wish to encrypt. Right Click on the Folder Name >> Click **Properties** >> **General Tab** >> Click **Advanced**



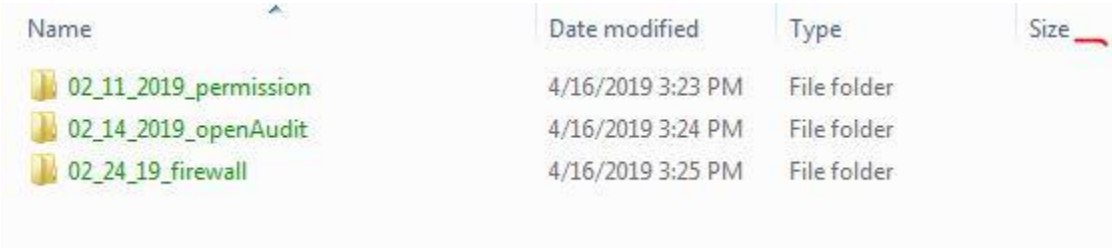
- Under Confirm Attribute Changes, choose how extensive you want the encryption to be, click **OK.** We recommend selecting the option of "**Apply changes to folder, subfolders and files**"



- Click **Apply.** This will begin the encryption process.



- Upon encryption, the subfolders or file names would change to Green color as shown below Any new folder added to this parent folder will be automatically encrypted.

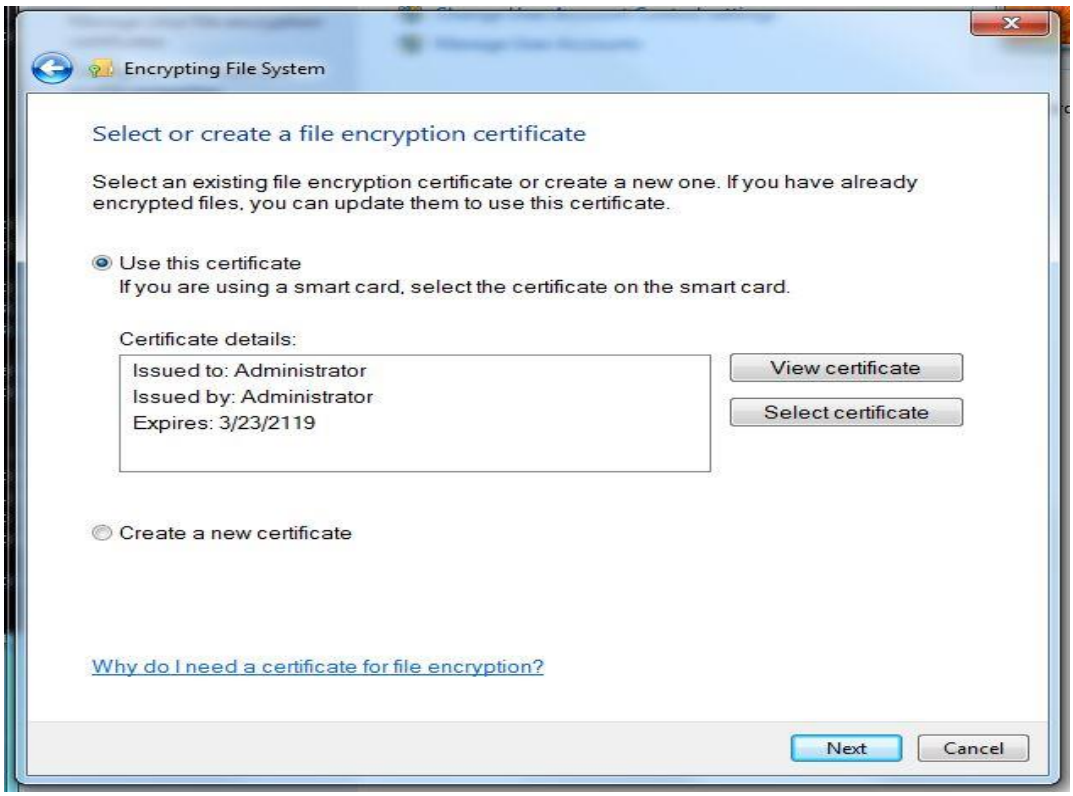


Backing up the Encryption Key

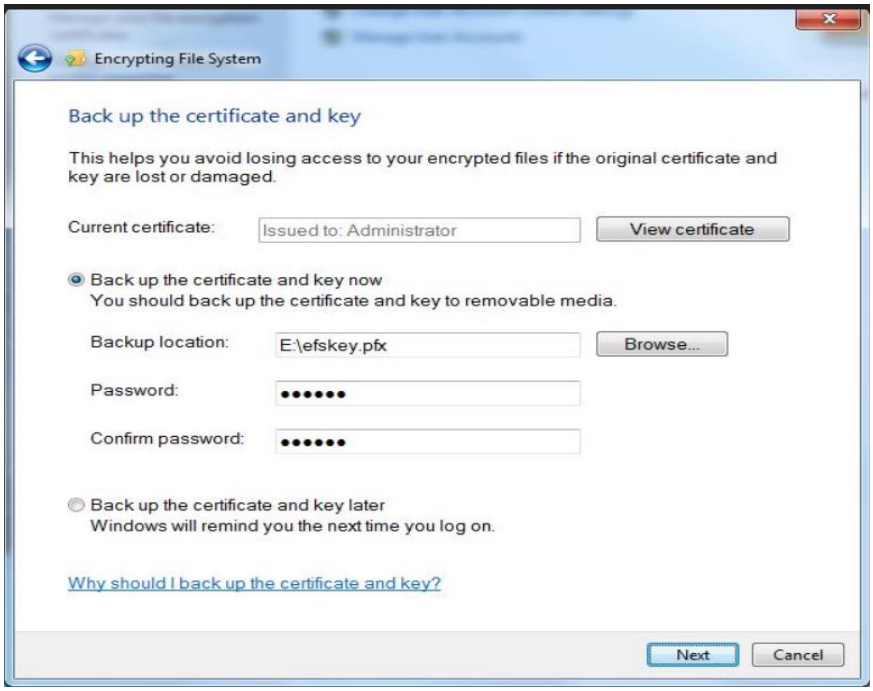
- When a file or folder is encrypted for the first time, a pop-up message saying "Backup your encryption key" should appear in the task-bar. Double click to launch the backup process.
- Alternatively, this process can also be launched manually by going to **Control Panel** >> All Control Panel **Items** >> **User Accounts** >> **Manage your encryption certificates**
  Note: This process is different for a Windows 10 system.

- Click **Next**

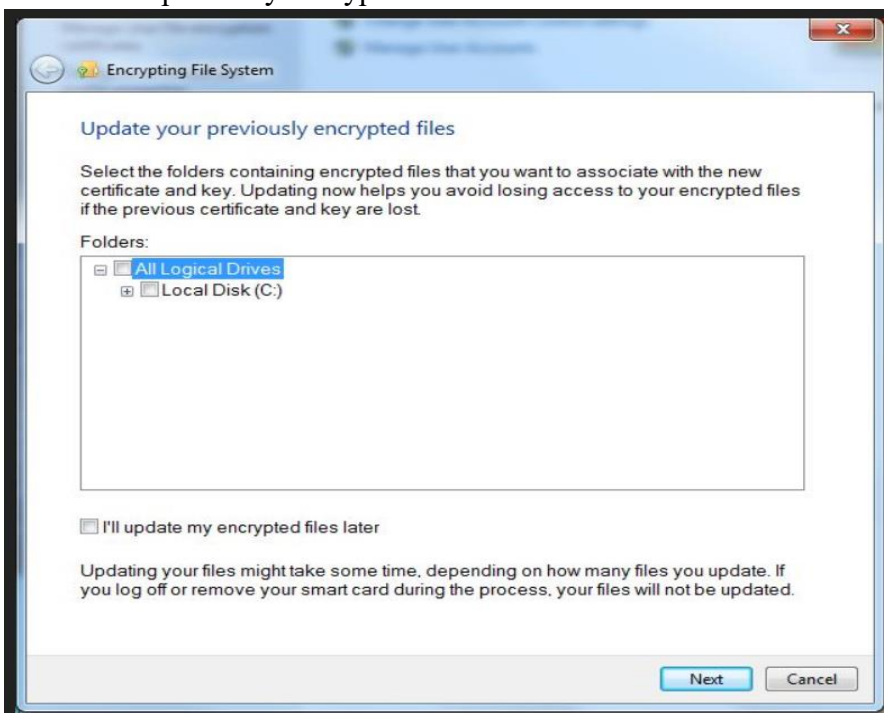
- Select existing Certificate or Create a new one. It is safe to go with the default option



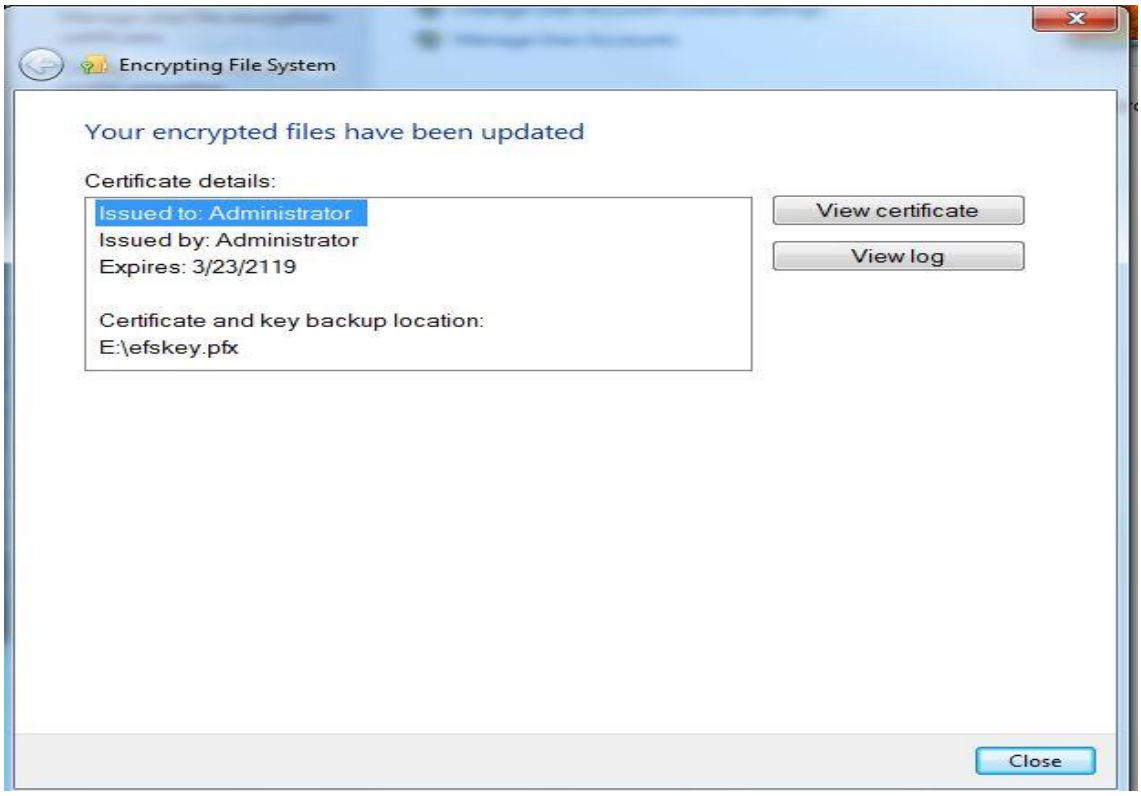
- Select "**Backup the Certificate and Key Now**". Click **Browse** to choose a destination for saving the pfx bundle file. For instance: a USB drive. Enter a password for added protection.



- Select the appropriate folder to associate with the new certificate and key OR Alternatively select "I'll update my encrypted files later". Click **Next**



- A confirmation message as below will be shown next. This completes the backup of the Recovery key



Using Encrypted files on a Different Computer

If you want to use your encrypted files on another computer, you need to export the EFS certificate and key from your computer or the USB backup and then import it at the other computer.

4.14.6 Highlighted Performance Impacts

The following performance measurement experiment was performed for the Microsoft EFS tool while the manufacturing system was operational:

Experiment PL013.1- Enable file level encryption on HMI host

The FactoryTalk HMI application has a designated file folder to contain the log files for the HMI data. EFS tool was used to encrypt the data log file in this experiment.

There were noticeable performance impacts to the computing resources observed when the EFS was activated for the data log files, especially at the initial operation of the HMI. The processor utilization was noticeable higher from 450 seconds to 750 seconds experiment time and occasionally higher throughout the first 3000 seconds. The disk write operation was significantly higher in the first 800 seconds of the experiment time. The HMI application attempted to access the data log files at the initialization stage and therefore most of the impacts were observed at the beginning of the operation.

On the network side, no significant performance impact was observed. The packet round trip time between the HMI and OPC in both directions reminded mostly constant before and after the EFS was enabled.

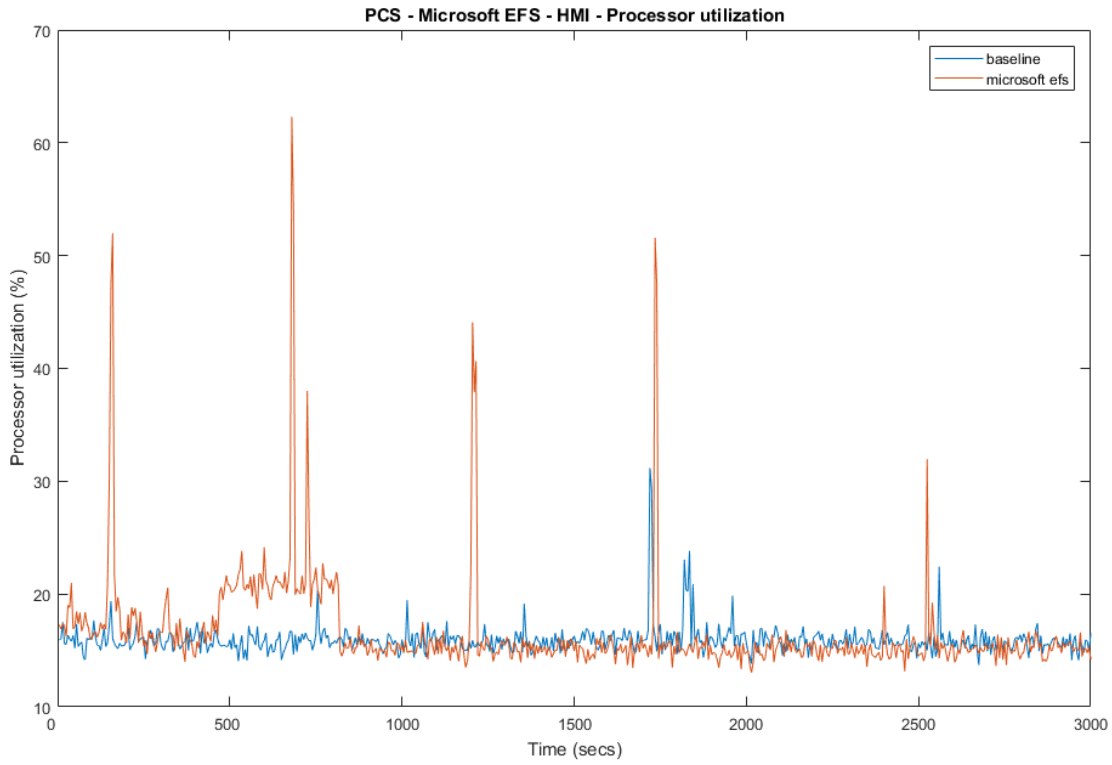


Figure 4-29 HMI computer processor utilization with EFS enable (red) and without EFS enable (blue)

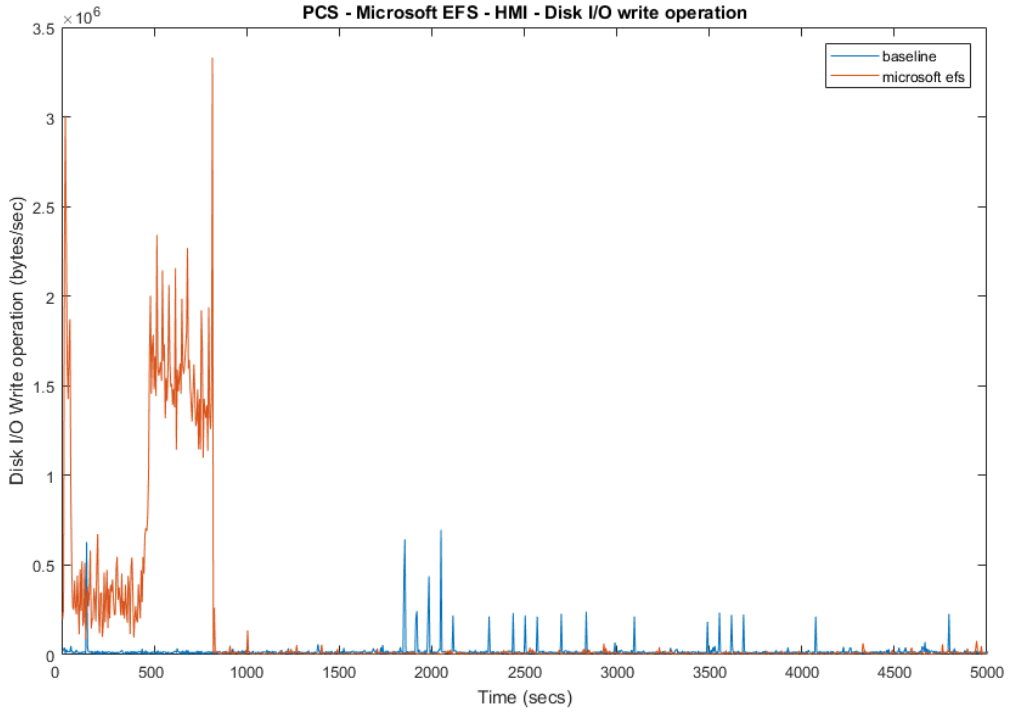


Figure 4-30 HMI computer disk write operation with EFS enable (red) and without EFS enable (blue)

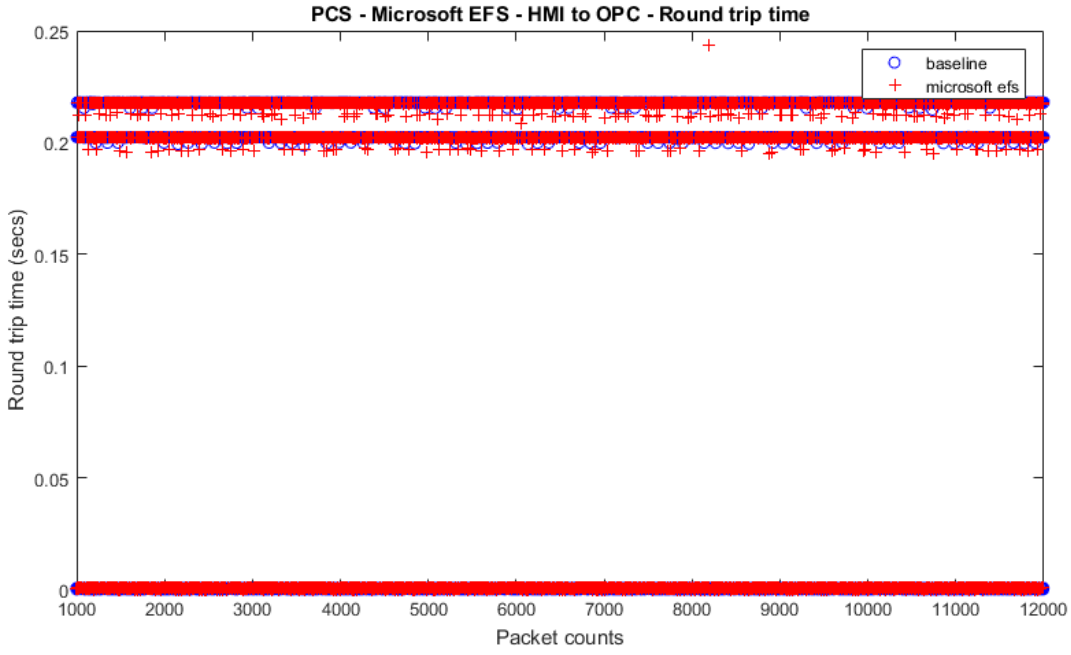
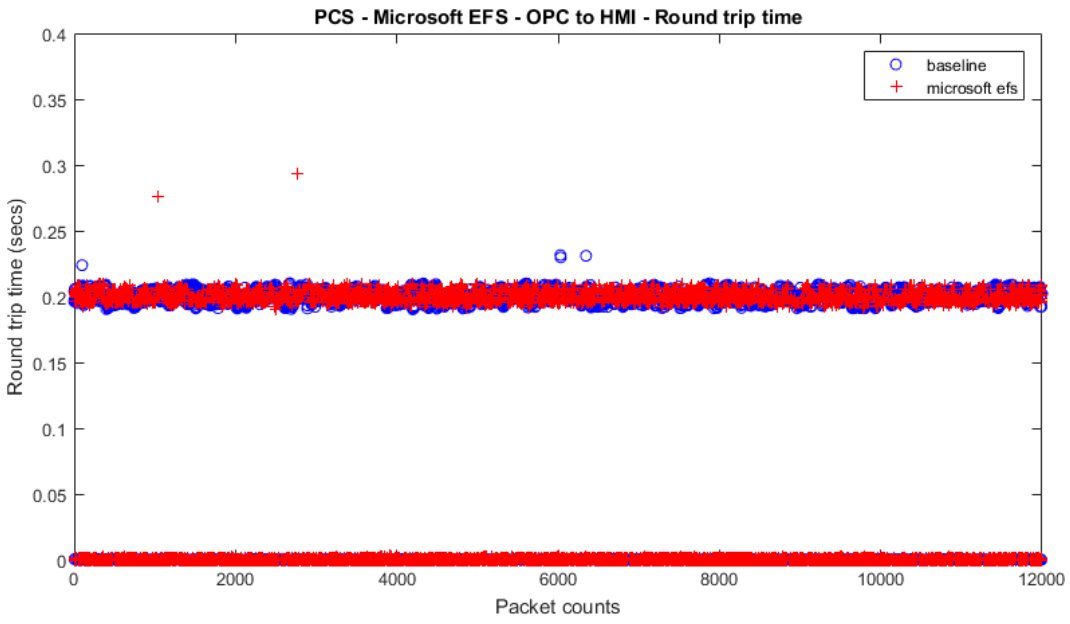


Figure 4-31 Packet round trip time from HMI to OPC with EFS enable (red) and without EFS enable (blue)

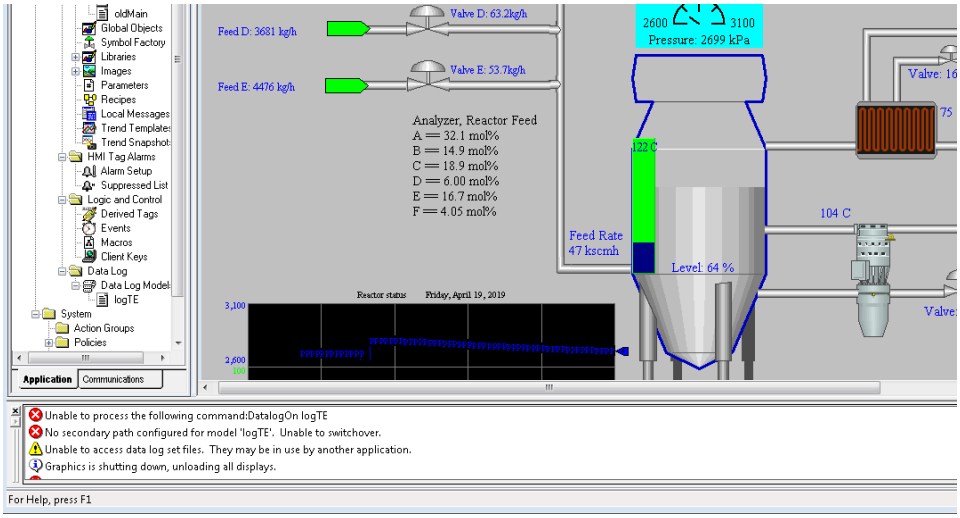


4897

4898 **Figure 4-32 Packet round trip time from OPC to HMI with EFS enable (red) and without EFS enable (blue)**

4899 The HMI application was not able to access the data log files and new data from operation was
4900 not logged. The HMI flagged an error/warning message to the operator.

4901 Care should be taken for encrypting application specific files or folders. There is performance
4902 impact to the manufacturing process in the form of losing the ability to log data files in the HMI.



4903

4904 **Figure 4-33 HMI screen with warning message "Unable to access data log set files"**

4905

4.14.7 Link to Entire Performance Measurement Data Set

File Encryption KPI data

File Encryption measurement data

4.15 GTB Inspector

4.15.1 Technical Solution Overview

GTB Inspector by GTB Technologies is a DLP solution that has been evaluated in our lab environment for low baseline manufacturing profile. GTB Inspector's built in ability to detect, log, and block network traffic trying to leave premise. Inspector detects and blocks FTP, Email, HTTP, HTTPS (SSL/TLS), Finger Printed files, USB protection, and other configured exfiltration methods. GTB Inspector is the main component that analyzes all network traffic and depending on the configuration Bridge (In-Line), Monitoring (OOL), TAP, Transparent Proxy (TPROXY), and Load Balancing if required. GTB Central Console which is the device Inspector reports back to, so there is always a log of violation that occurred. Central Console allows for groups and escalation paths depending on the alerting required.

GTB is configured within the corporate network. This option was chosen to ensure we could get the best protection for the entire environment.

All DLP products have a high cost to implement, but GTB Technologies provides a product that can grow as your company does.

Once installed and configured system requires little maintenance.

Install time within the lab was approximately 16 hours for configuration, but for simple data capture setup took about an hour.

4.15.2 Technical Capabilities Provided by Solution

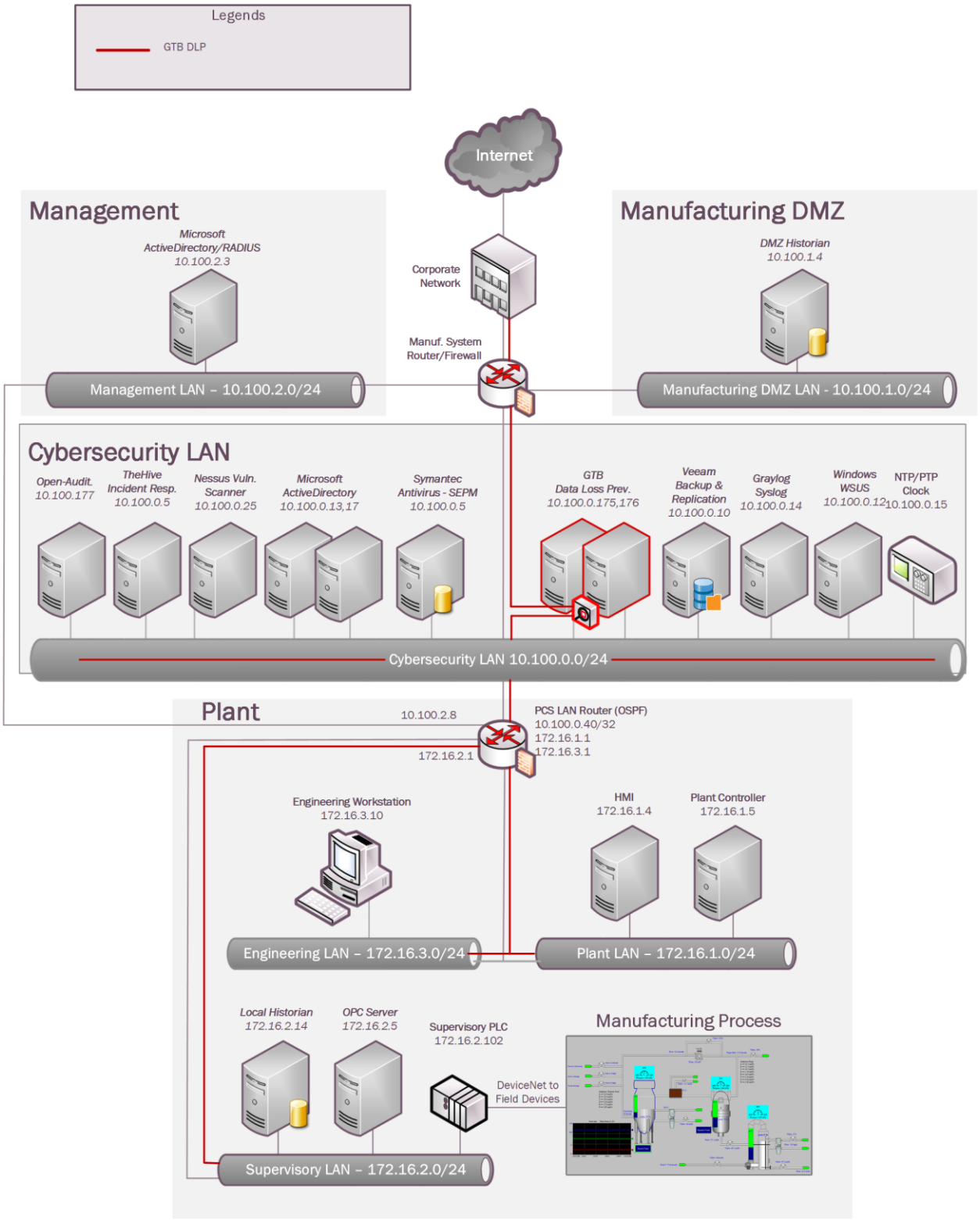
GTB Inspector provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Data Loss Prevention

4.15.3 Subcategories Addressed by Implementing Solution

PR.DS-5

4.15.4 Architecture Map of Where Solution was Implemented



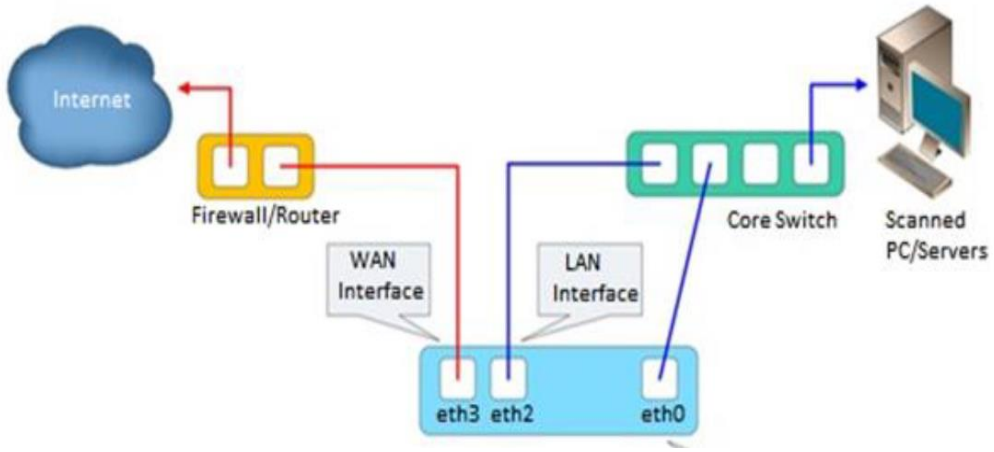
4.15.5 Installation Instructions and Configurations

Steps for installing GTB Central Console and Inspector

- Both products are virtual machines and downloadable from https://gttb.com/downloads/ select desired product for download.
- Once downloaded extract each zip file to its own folder.
- Inside newly created folders there'll be a "**installation guide"** along with the extracted files for each product.
- See attached PDF for current "**system requirements"** for each component being installed.

GTB DLP Installation Requirements for a G

- Currently **"GTB Inspector"** network configuration is enabled in **"Bridge [Inline]"** mode. This diagram is within **"installation guide" GTB Inspector DLP, installation methods. Displayed is Bridge [Inline] mode which monitors.**



Hyper-V Install Configuration

- Create two virtual machines **(See below for current specification of our environment)**
- GTB Inspector (VM #1)
  - VHDX -- D:\Hyper-V\GTB InspectorVirtual Hard Disks\GTB Inspector.vhdx
  - Memory – 16GB (16384MB)
  - Processor – 4 CPU
  - Network Adapter
    - **"vswitch_TestBed_LAN"** Management Port
      - Management port IP is (10.100.0.175)
    - **"Eth2 for GTB Inspector"** Connects to Monitor Port 1 on Tap Device
      - **"Eth3 for GTB Inspector"** Connects to Monitor Port 2 on Tap Device
- GTB Central Console (VM #2)

- VHDX -- D:\Hyper-V\GTB Central Console\Virtual Hard Disks\GTB Central Console.vhdx
- Memory – 16GB (16384MB)
- Processor – 4 CPU
- Network Adapter
  - **"vswitch_TestBed_LAN"** Management Port / Connection
    - Management Port / Connection IP is (10.100.0.176)

Install Instructions for Each Virtual Machine and any additional configuration

- **Inspector**
  - See install guide for most updated instructions, or attachment below. **Changes made within our environment are included below.**
  - Each network connection was installed and rebooted to ensure they were assigned correct name / location, and if not, this command can be used to rename the network to reflect and needed changes. */usr/local/gtb/libexec/manage_nics -i ethX –o ethX* **(This syntax is included within installation guide)**
  - **IP Address (10.100.0.175)**
  - **Hostname = gtbinspector / gtpinspector.lan.lab**
  - Created DNS A record for **"gtbinspector"** along with reverse lookup
  - **Configured LDAP integration with Active Directory (10.100.0.17)**
  - **UPN is required for username**
  - **Configured email**
    - SMTP Server Hostname **(postmark.nist.gov)**
    - Send email from **(**GTBInspector@nist.gov**)**
    - SMTP Server Port **(25)**
  - Check and ensure LAN and WAN interfaces are configured for eth2 **(WAN)** eth3 **(LAN)**
    - Configuration tab, Network, #-3 and #-4


GTB Inspector Installation Guide.pdf

- **Central Control**
  - See install guide for most updated instructions or attachment below. **Changes made within our environment are included below.**
  - **IP Address (10.100.0.176)**
  - **Hostname = gtbcc / gtbcc.lan.lab**
  - Created DNS A record for **"gtbcc"** along with reverse lookup
  - **Configured LDAP integration with Active Directory (10.100.0.17)**
  - **UPN is required for username**
  - **Configured email**
    - SMTP Server Hostname **(postmark.nist.gov)**
    - Send email from **(**GTBInspector@nist.gov**)**

- SMTP Server Port **(25)**

GTB Central Console Installation Guide.pdf

- **Install information for VMware**
  - **Install**
    - Installed a separate physical machine with vSphere (10.100.0.180) for testing since problems were observed with Hyper-V ability to block rule violations with HTTP/HTTPS traffic.
    - Configured two network cards in vSphere for pass thru access. This was completed to give the virtual machine access to physical network cards to eliminating possible configuration issues being observed in Hyper-V. (Will try to confirm if possible still exist with Hyper-V since new release from GTB has been released)
    - GTB's Inspector (10.100.0.181) is currently at release 15.4 and contains an option under **"Configuration → Network"** labeled (Failover Mode). In our environment this option is set to **"NO"** since we don't have a bypass card installed. This setting allows all web traffic to be filter via scanning engine.

14	Failover mode	No	Select "Yes" to enable failover mode of the Bypass Network Card in Bridge and TPROXY. Select "No" to enable fail closed mode.

    - Email filtering is designed to use **"MTA"** from Inspector and then forward along to intended recipient after been scanning for any rule violations.
    - Added GTTB Certificate to **"Default Domain Policy"** so any machine within the domain will update with the required Trusted Certificate Authority so as not to get a warning message. **(Confirmed working)**

    - **Lesson learned:**
      - Microsoft Hyper-V solution detects and logs traffic, however even when configured for blocking, only detection occurs. Support has indicated that this is since we're not using a bypass network card stated earlier with a physical box.

    - **Performance Impact:**
      - This tool has not been configured and ran against ICS enclaves currently, so there has been no performance impact that were aware of.

Specific configuration steps for GTB's Inspector and Central Console

*This section contains information for configuration within our environment. If scanning email for content violation, you'll need to configure email clients to point **SMTP** to **10.100.0.175** (Inspector - MTA) for email scanning. For additional configuration information please see vendors Administrator Guides which are included in download package from vendor.*

Inspector

Generating and applying License:

- **Generating**
  - Click on middle top web page once logged into Inspector
    - 

    - You will now be directed to a page that allows you to download, email, or upload a license file.
    - License files should be emailed to support@gttb.com . Support will reply with an updated file to be uploaded.
- **When to generate a new license file**
  - Anytime a network change effects the **MAC (Media Access Control)** address for Inspector you'll need to generate a new license key an email support@gttb.com. Before emailing change the extension from **".dat"** to **".txt"**. Example: **Inspector** – "***7-31-2018-sysinfo_inspector.dat to 7-31-2018-sysinfo_inspector.txt***". This change may be required if your email provider blocks **".dat"** file extension.
- **Configuration Setting**
  - Login into GTB Inspector web page and click **"Configuration"** tab.
    

  - All setting are accessible via **"Groups"** located on left side of webpage.
  - Central Console = **"gtbcc.lan.lab"**

5060

- **Network = Screenshot below**

Network

1	Inspector location	GTBInspector.lan.lab	The location or hostname the Inspector appliance.
2	Deployment mode	TPROXY	Deployment mode of the Inspector: "OOL" for Out-of-Line, "BRIDGE" for Inline, "TAP" for a Tap connection, "TPROXY" for Transparent Proxy.
3	LAN interface	eth2	LAN interface (ie. eth0, eth1, eth2, or eth3) where the network traffic is coming from. It is being used in all Inspector modes.
4	WAN interface	eth3	WAN interface (ie. eth0, eth1, eth2, or eth3) where the network traffic is coming to. It is being used in TAP, BRIDGE, and TPROXY modes.
5	OOL LAN	10.100.0.0/24, 172.16.3.0/24	List of source IP addresses, subnets or MAC addresses separated by commas which are inspected in the OOL mode.
6	OOL WAN		List of destination IP addresses, subnets or MAC addresses separated by commas which are inspected in the OOL mode. An empty entry accepts all WAN packets.
7	TPROXY LAN	10.100.0.0/20,192.168.0.0 /20,172.16.0.0/20	List of source IP addresses or subnets separated by commas which HTTP/HTTPS traffic is being inspected in the TPROXY mode.
8	TPROXY source exceptions	10.100.0.14, 10.100.0.11	List of source IP addresses or subnets which are not inspected in the TPROXY mode. Each object is delimited by comma or new line.
9	TPROXY destined exceptions		List of destination IP addresses or subnets which are not inspected in the TPROXY mode. Each object is delimited by comma or new line.
10	TPROXY IP address	10.100.0.175	IP address of TPROXY NIC device.
11	TPROXY netmask	255.255.255.0	Subnet mask of TPROXY NIC device.
12	TPROXY gateway	10.100.0.1	Default gateway of TPROXY NIC device.
13	TPROXY routing	10.100.0.0/24 via 10.100.0.1 dev eth0 192.168.0.0/20 via 10.100.0.1 dev eth0 172.16.0.0/20 via 10.100.0.1 dev eth0	Static routing rules each on a separate line. Example: 192.168.0.0/24 via 191.168.0.1 dev eth0. Where 192.168.0.0/24 is destination host/subnet, 191.168.0.1 is a gateway, eth0 is a NIC device of the Inspector.
14	Failover mode	No	Select "Yes" to enable failover mode of the Bypass Network Card in Bridge and TPROXY. Select "No" to enable fail closed mode.
15	OOL/TAP blocking	Yes	Select "Yes" to enable blocking in OOL/TAP modes.
16	Blocking interface	eth2	Network interface name for sending TCP Reset or FIN packets in "TAP" mode (ie. eth0, eth1, eth2, or eth3).
17	DNS servers	10.100.0.17, 10.100.0.13	DNS servers IP addresses separated by commas.
18	Network Overload Protection	No	Enable skipping stream inspection (BRIDGE mode only) due to excessive network traffic.
19	Network MTU	9000	The maximum transmission unit size for inspection ports (LAN and WAN), this can be up to 16110.
20	CRC checking	No	Select "Yes" to perform a CRC check of every network packet. Normally, should be set to "No".

5061
5062

- **Emails Alerts = Screenshot below**

Email Alerts

1	Security Respondents	wesley.downard@nist.gov,neeraj.shah@nist.gov	Default Security Respondents - list of email addresses separated by commas.
2	Special Case Security Respondents		Format: [Policy: list of email addresses separated by commas]. Example: PCI: demo@gttb.com
3	MD5 Recipients		Email address receiving MD5 of triggered events.
4	System Administrator Email	wesley.downard@nist.gov,neeraj.shah@nist.gov	System Administrator email address(es) separated by commas.
5	Notify about system errors by email	Yes	Select "Yes" to notify System Administrator about system errors by email.
6	Send Emails From	GTBInspector-ICSLab-220-A230@nist.gov	Email address, appears as the source of the email notification.
7	SMTP Server Hostname	postmark.nist.gov	The IP address or domain name (FQDN) of the SMTP server. This address is required in order for the Inspector to send email notifications.
8	SMTP Server Port	25	The SMTP server port number. Typically, it is port 25.
9	Use SSL/TLS	No	Select "Yes" to use SSL/TLS encrypted connection.
10	Email Username		Authenticated Email Username.
11	Email Password		Authenticated Email Password.
12	Time between Alerts	60	Minimum interval in seconds, between alert emails.
13	Enable HTTP Block Response	Yes	Select "Yes" to return an alert page to a web browser when HTTP request is blocked.
14	HTTP Response Message	http://testpage.gtbtechnologies.com:	Response message in HTML or redirect URL returned when the HTTP session is blocked.

5064
5065
5066

- **LDAP Intergration = Screenshot below**

LDAP Integration

1	LDAP Server Hostname	10.100.0.17	IP address or hostname of the corporate LDAP server.
2	LDAP Server Port	389	LDAP server port.
3	LDAP Username (bind DN)	gttbldap@lan.lab	Example: Domain\Username (for MS Active Directory), cn=Admin,o=MyOrganization (for Novell eDirectory or OpenLDAP).
4	LDAP Password	******	LDAP password.
5	LDAP SSL	No	Select "Yes" to use SSL connection to the LDAP server.
6	LDAP Cache Refresh Period	1800	Period in seconds used for LDAP objects cache periodic refreshes. Zero means no periodic refreshes.
7	Hostnames Cache Refresh Period	3600	Period in seconds used for hostnames cache periodic refreshes. Zero means no periodic refreshes.
8	NRH UDP Port	2222	UDP port for receiving reports from Name Resolution Helpers (the device acts as server).
9	Cache Persistence Timeout	450	User names cache persistence timeout in seconds. If the system is stopped for more than timeout specified, cache becomes obsolete and is dropped. Zero means "never obsoleted".

5068

5069 ○ **Mail Transfer Agent = Screenshot below**

Mail Transfer Agent			
1	List Of Allowed Hosts	*	Allowed hosts for email processing. Insert hostnames or IP addresses in separate rows. Insert * to accept emails from any host. A blank field means emails are rejected from any host.
2	Route Emails	Yes	Select "Yes" to have MTA route all emails to the next email hops listed in the "Domain Routing Rules" field.
3	Email Username		Authenticated next email hop Username. Example: demo@gttb.com.
4	Email Password		Authenticated next email hop User Password.
5	Domain Routing Rules	* 129.6.16.94	This entry contains routing rules per email domain on separate lines. Each rule consists of a domain pattern and a list of hostnames to which MTA will attempt to relay emails for this pattern. Use a colon to separate hostnames. Use double colon to specify a port number. Example: *.com 192.168.0.1:192.168.0.100, *.net 192.168.1.1::2525
6	Excluded domains		Emails destined to these domains will be passed without inspection. Domains should be colon delimited and without spaces. Example: gmail.com:gttb.com
7	Bcc domain inspection		List of email domains for inspection only (without routing). Domains should be colon delimited and without spaces. Example: gmail.com:gttb.com
8	MTA Listening Ports		List of listening TCP port numbers separated with colons. Default is 25. Example: 25:465
9	Email Size Limit	20	Maximum allowed email size in MBytes which is accepted for delivery and inspection. Value "0" means unlimited size.
10	Alert on Queue Above	4	System will alert Administrator hourly, when the number of email messages in the MTA queue is above this value. Set 0 to disable it.
11	Backup Emails	None	Enable email backup system.
12	Reject Email on fail	No	Select "Yes" to enable email rejection when inspection fails.

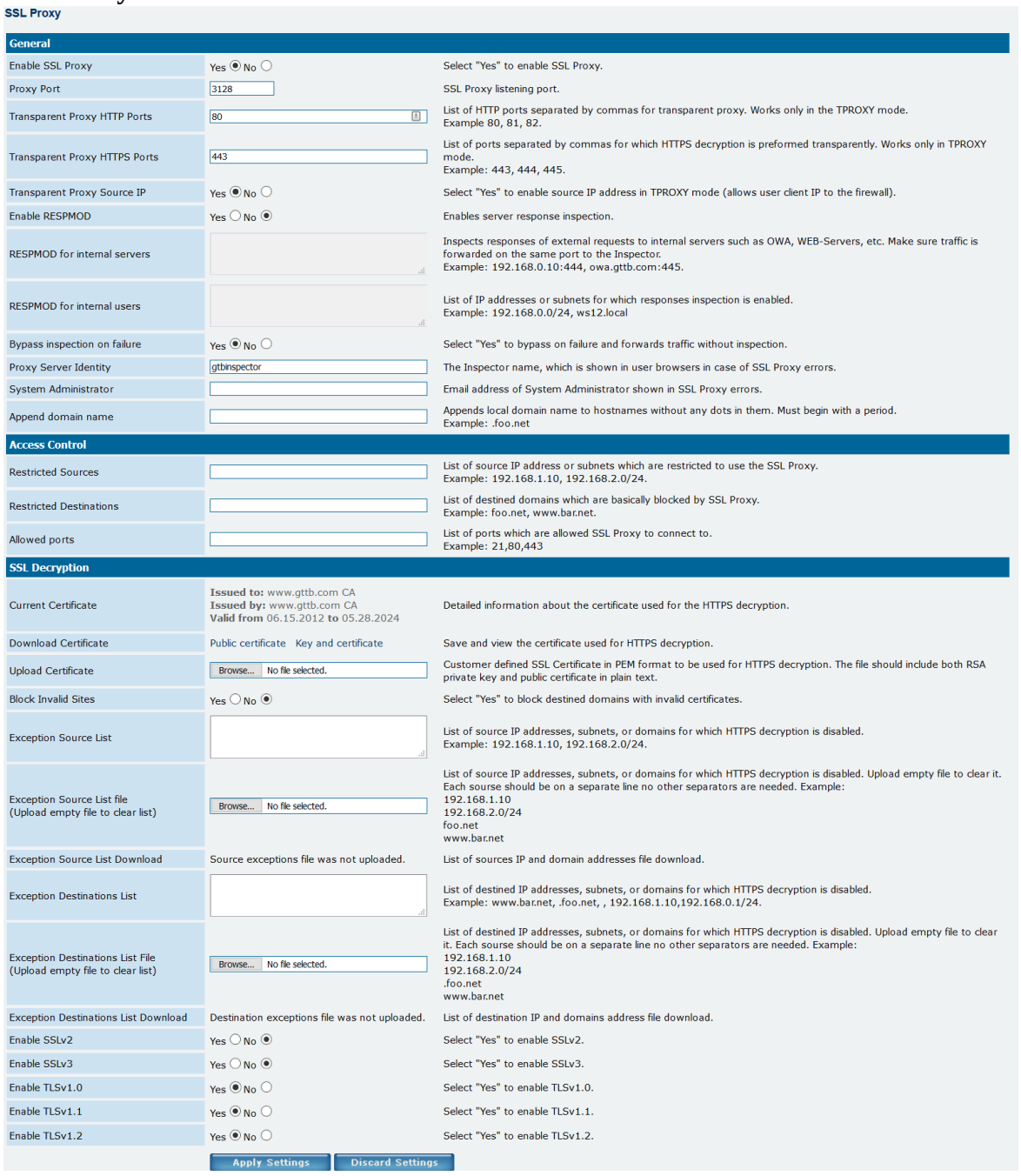
5070
5071

5072 ○ **SIEM = Screenshot below**

SIEM			
1	SIEM Receiver Hostname	10.100.0.27	IP address or hostname of the corporate SIEM receivers separated by commas.
2	Log Content	Yes	Select "Yes" to include security events triggers into the SIEM message.
3	Arcsight CEF	Yes	Select "Yes" to use Arcsight Common Event Format in the SIEM messages.

5073

5074 ○ **SSL Proxy = Screeshot below**



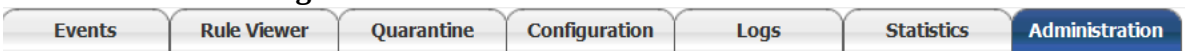
SSL Proxy

General		
Enable SSL Proxy	Yes (●) No ( )	Select "Yes" to enable SSL Proxy.
Proxy Port	3128	SSL Proxy listening port.
Transparent Proxy HTTP Ports	80	List of HTTP ports separated by commas for transparent proxy. Works only in the TPROXY mode. Example 80, 81, 82.
Transparent Proxy HTTPS Ports	443	List of ports separated by commas for which HTTPS decryption is preformed transparently. Works only in TPROXY mode. Example: 443, 444, 445.
Transparent Proxy Source IP	Yes (●) No ( )	Select "Yes" to enable source IP address in TPROXY mode (allows user client IP to the firewall).
Enable RESPMOD	Yes ( ) No (●)	Enables server response inspection.
RESPMOD for internal servers		Inspects responses of external requests to internal servers such as OWA, WEB-Servers, etc. Make sure traffic is forwarded on the same port to the Inspector. Example: 192.168.0.10:444, owa.gttb.com:445.
RESPMOD for internal users		List of IP addresses or subnets for which responses inspection is enabled. Example: 192.168.0.0/24, ws12.local
Bypass inspection on failure	Yes (●) No ( )	Select "Yes" to bypass on failure and forwards traffic without inspection.
Proxy Server Identity	gtbinspector	The Inspector name, which is shown in user browsers in case of SSL Proxy errors.
System Administrator		Email address of System Administrator shown in SSL Proxy errors.
Append domain name		Appends local domain name to hostnames without any dots in them. Must begin with a period. Example: .foo.net
Access Control		
Restricted Sources		List of source IP address or subnets which are restricted to use the SSL Proxy. Example: 192.168.1.10, 192.168.2.0/24.
Restricted Destinations		List of destined domains which are basically blocked by SSL Proxy. Example: foo.net, www.bar.net.
Allowed ports		List of ports which are allowed SSL Proxy to connect to. Example: 21,80,443
SSL Decryption		
Current Certificate	**Issued to:** www.gttb.com CA **Issued by:** www.gttb.com CA **Valid from** 06.15.2012 **to** 05.28.2024	Detailed information about the certificate used for the HTTPS decryption.
Download Certificate	Public certificate Key and certificate	Save and view the certificate used for HTTPS decryption.
Upload Certificate	Browse... No file selected.	Customer defined SSL Certificate in PEM format to be used for HTTPS decryption. The file should include both RSA private key and public certificate in plain text.
Block Invalid Sites	Yes ( ) No (●)	Select "Yes" to block destined domains with invalid certificates.
Exception Source List		List of source IP addresses, subnets, or domains for which HTTPS decryption is disabled. Example: 192.168.1.10, 192.168.2.0/24.
Exception Source List file (Upload empty file to clear list)	Browse... No file selected.	List of source IP addresses, subnets, or domains for which HTTPS decryption is disabled. Upload empty file to clear it. Each sourse should be on a separate line no other separators are needed. Example: 192.168.1.10 192.168.2.0/24 foo.net www.bar.net
Exception Source List Download	Source exceptions file was not uploaded.	List of sources IP and domain addresses file download.
Exception Destinations List		List of destined IP addresses, subnets, or domains for which HTTPS decryption is disabled. Example: www.bar.net, .foo.net, , 192.168.1.10,192.168.0.1/24.
Exception Destinations List File (Upload empty file to clear list)	Browse... No file selected.	List of destined IP addresses, subnets, or domains for which HTTPS decryption is disabled. Upload empty file to clear it. Each sourse should be on a separate line no other separators are needed. Example: 192.168.1.10 192.168.2.0/24 .foo.net www.bar.net
Exception Destinations List Download	Destination exceptions file was not uploaded.	List of destination IP and domains address file download.
Enable SSLv2	Yes ( ) No (●)	Select "Yes" to enable SSLv2.
Enable SSLv3	Yes ( ) No (●)	Select "Yes" to enable SSLv3.
Enable TLSv1.0	Yes (●) No ( )	Select "Yes" to enable TLSv1.0.
Enable TLSv1.1	Yes (●) No ( )	Select "Yes" to enable TLSv1.1.
Enable TLSv1.2	Yes (●) No ( )	Select "Yes" to enable TLSv1.2.
	Apply Settings Discard Settings	

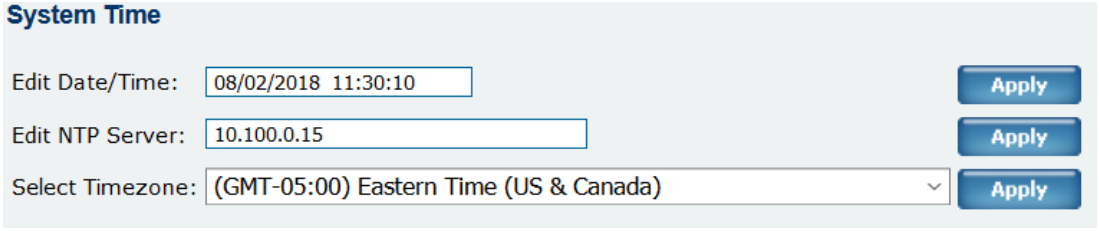
5075

5076

- **Administration setting**



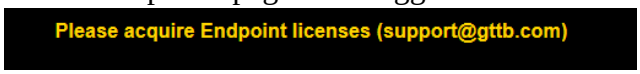
  - Licensing = Used for download and uploading license information.
  - Health Check = Ability to perform **"Self-Test"** to check Inspector install health.
  - Account Manager = Used to add new personal who will be administrating Inspector or responding to alerts for further investigation.
  - **System Time = Screenshot below**

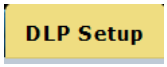


Central Console

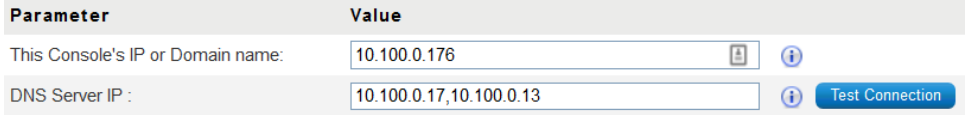
Generating and applying License:

- **Generating**
  - Click on middle top web page once logged into Central Console



    - You will now be directed to a page that will allow you to download, email, or upload a license file.
    - License files should be emailed to support@gttb.com . Support will reply with an updated file to be uploaded.
- **When to generate a new license file**
  - Anytime a network change effects the **MAC (Media Access Control)** address for Central Console you'll need to generate a new license key and email it to support@gttb.com. Before emailing change the extension from **".dat" to ".txt"**. Example: **Central Console - 7-31-2018-sysinfo_cc.dat to 7-31-2018-sysinfo_cc.txt**. This change may be required if your email provider blocks **".dat"** file extension.
- **System settings**
  - Click on **"DLP Setup"** tab 

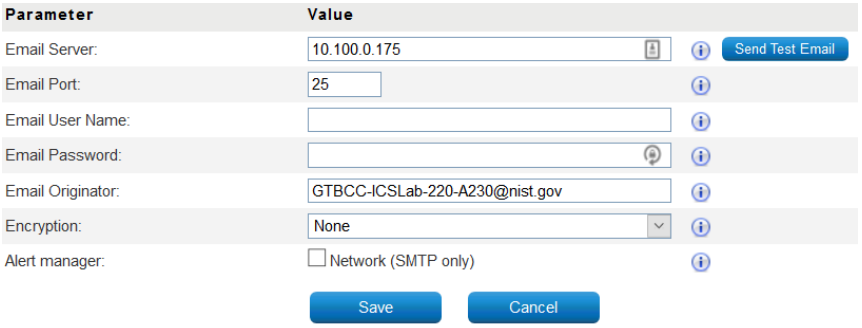
  - **Network (Located under Categories)**
    - Enter required information. See below for screenshot



    - Click save to continue.

- **LDAP**
  - Enter information for screenshot below. This user has been created and only has Domain User right. Check for password in database.

  - User name = gttblab@lan.lab
  - Password = check database
  - LDAP Server = 10.100.0.17
- **Email and alerts**
  - Enter information from screenshot below



  - Email Server = 10.100.0.175
  - Email Originator = GTBCC-ICSLab-220-A230@nist.gov
  - Click save
- **Data and Time**
  - NTP Server = 10.100.0.15 (Click set time to sync)
  - Time Zone = Eastern Time (US and Canada) (Click Apply to save)
  - Click Save

Other settings under **DLP Setup → System** aren't currently configured. These setting will be updated an included when these features are enabled.

Lesson learned: If integrating with Active Directory using LDAP it's recommended to use Secure LDAP to ensure user name and password are not sent in plaintext.

How ACL rules are created for use with GTB DLP Inspector.

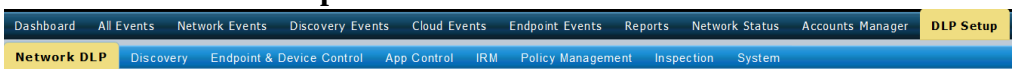
GTB DLP Inspector views data as it passes thru the device and responds based on configured rules.

GTB Central Console is the portal were all policy rules and other settings are configured.

ACL Rules:

- Login into to Central Console via web browser (E.g. 10.100.0.176).

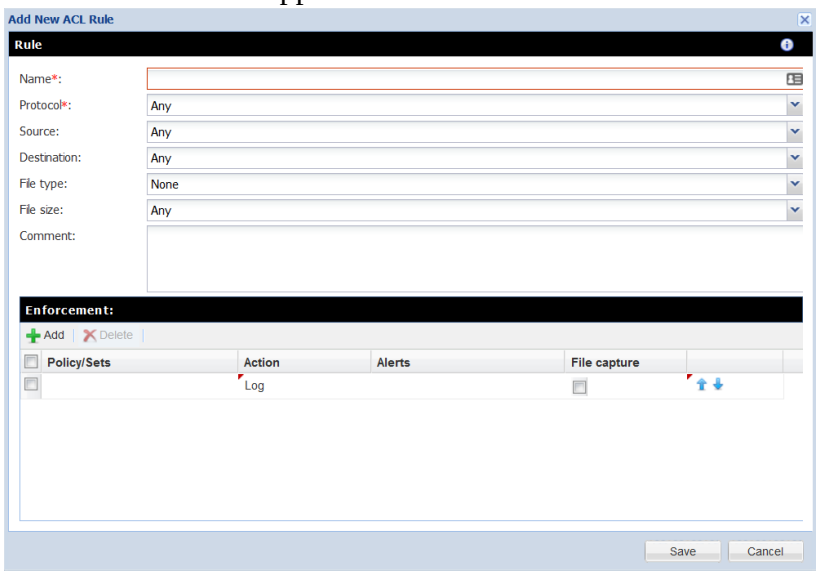
- Now click on **DLP-Setup→Network DLP** to access rules.



- Now, look to the left of window under categories and select your Inspector installation.

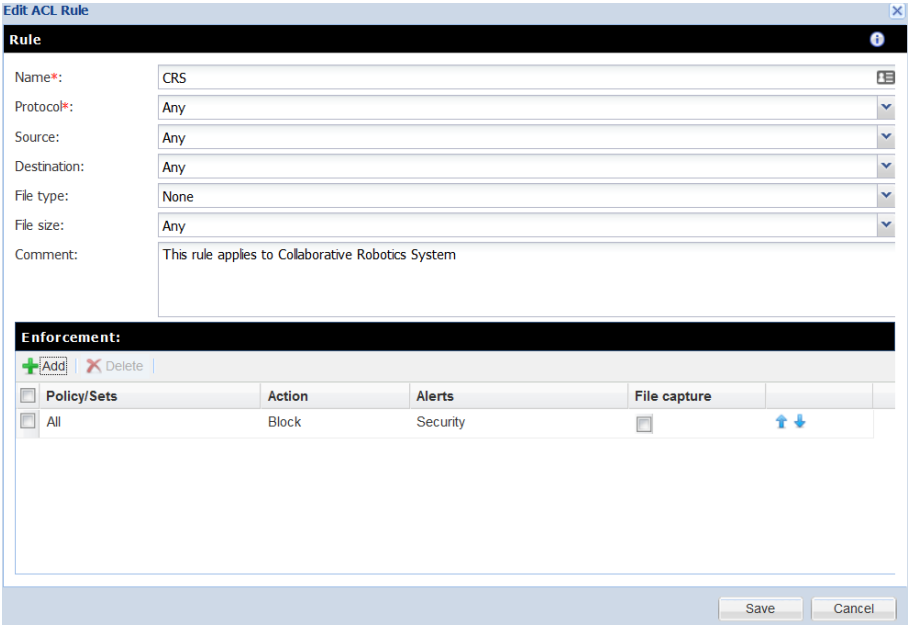
- Once selected you will see on the right current **ACL** Rules being applied.
- Click Add button. 

- A new window will appear titled **"Add New ACL Rule"**

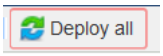


- Now type in a name for the new rule being created.
- Change Protocol to desire setting. This can be left to **"ANY"** which will look at all protocols passes thru the Inspector (*This may cause a performance impact on you Inspector installation depending on the number of clients within your organization*).
- **Source:** Choices are → **Any, IP Address, Hostname, Hostname (Custom), and Group (User/Computer)**.
- **Destination:** Choices are → **Any, IP Address, Hostname, Hostname (Custom), and Group (User/Computer)**.
- **File type:** Choices are → **None, All Files, Encrypted, and Extension**.
- **File Size:** Choices are → **Any,** and **Not more than**.

- **Comments:** Give a description of the rule being applied then click **Add** button.



- Once Add has been clicked you'll have an option to select a **"Policy/Sets"** to enforce. Default policies that are enforce are (Credit Card Number **CCN** and Social Security Numbers **SSN)**.
- Next, select the action to be taken. There are four choices, **Log**, **Block**, **S-Block**, and **Pass**.
- Now select if you would like additional personal to be notification upon rule violations.
- Finally, place a check in **File Capture** if you want to retain a copy of the offending data.
- Click **Save** to complete.
- Last step is to click on **Deploy all** button. This sends newly created policy to Inspector. This button will have a red blinking box around it indicating required action.



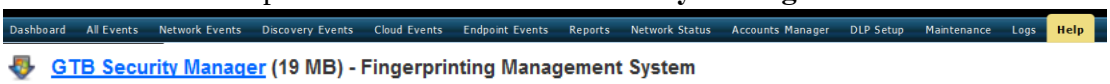
Useful Information:

- Once a new rule has been created double click on that rule to adjust the ordering from top to bottom by click the **UP** or **Down** arrows towards the right.
- Remember rules work from **Top → Down**, so think about ordering process. If unsure move the rule all the way to the top and then click **Deploy all** again.

5174 **How to Fingerprint Files using GTB Security Manager for DLP Protection**

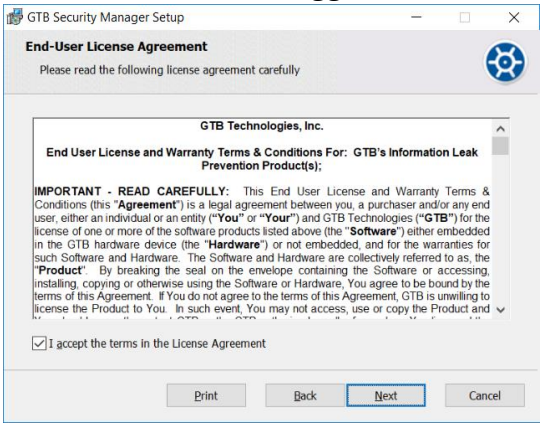
5175 **Download:**

5176 • First download "**GTB Security Manager"** by clicking on **Help** tab within Central
5177 Console server web portal then select "**GTB Security Manager"** link to start download.

5178 

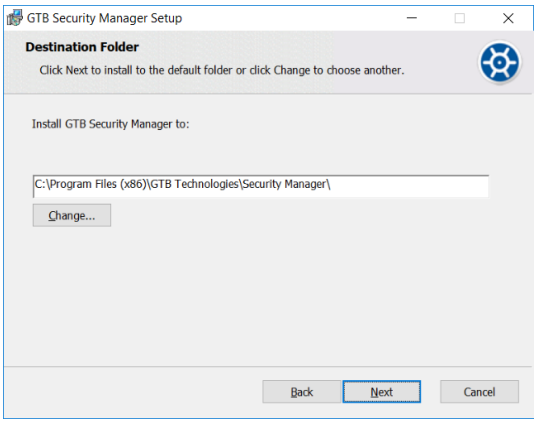
5179
5180 • Select location to save file being downloaded.
5181 • Double click to start install for **"GTBSecurityManager_15.3.0.msi"** from location
5182 where file was saved to (version number might be different than one listed above).
5183 • Once first screen appears click on **"Next"** to continue.

5184
5185 • Select Yes to License Aggreement and click **"Next"** to continue.



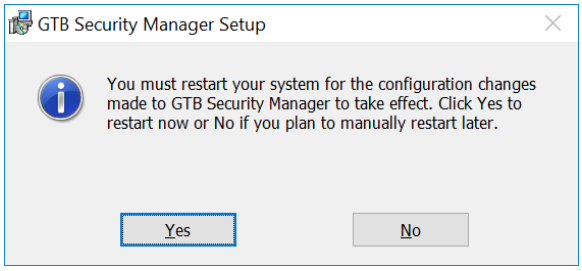
5186

- Leave Destination Folder as default and Click **"Next"**



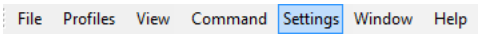
- Click **"Install"** to continue.

- When prompted by **User Access Control (UAC)** enter administrator password to continue install.
- If prompted to close Open Applications, select either option. Reboot is required if second option is selected.
- Click **"OK"** to continue.
- Once install has completed click **"Finish"** to complete install.
- If prompted to reboot, select **"Yes"**. MAKE SURE TO SAVE ALL OPEN FILES BEFORE SELECTING **"YES"**

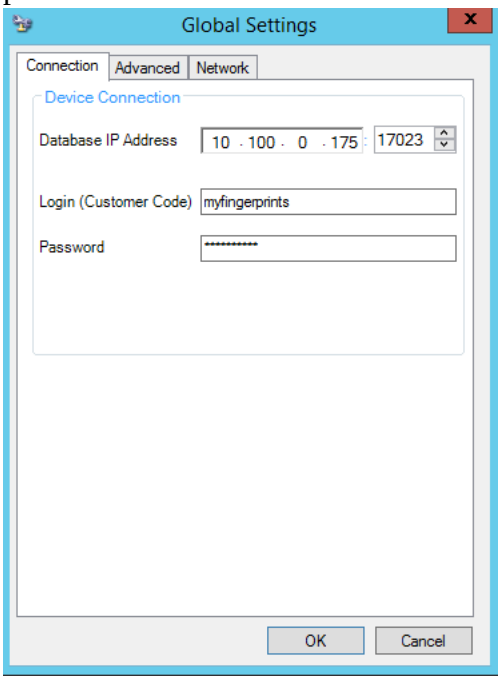


- Once machine has completed rebooting open **"GTB Security Manager"** by right click and selecting **"Run as administrator"**
- When prompted enter administrator password for application to start.

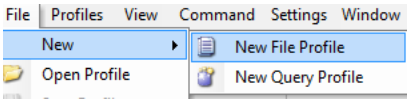
- Once "**GTB Security Manager"** has opened, click on setting button on menu bar.



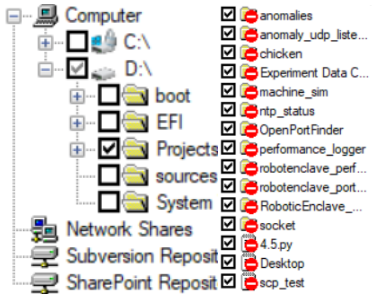
- Now enter the IP Address of where **"Central Console"** is installed. Login and password are already populated with default credentials from vendor. Both can be changed. See foot notes for additonal steps required to change Fingerprint Inspections login an password.



- Once IP Address has been enter click **"OK"** to save changes.
- Now, click on **File** from menu bar and select **New → New File Profile**

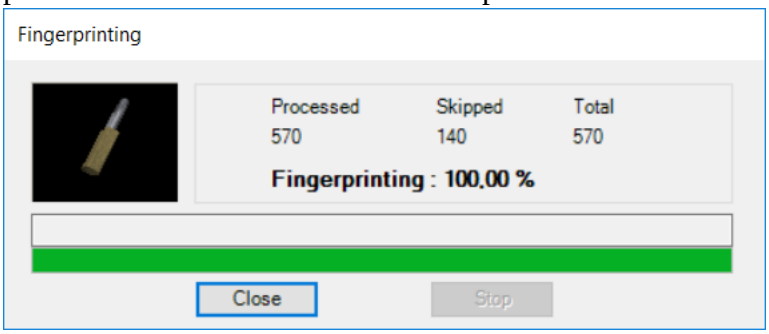


- A new window will appear allowing the ability to select files to be added. Files can be copied to **Local Machine**, or accessed from a **Network Share**, **Subversion Repositories,** or **SharePoint Respositories.**
- Select the folder, or files that need fingerprinting. Once a folder is selected all files within selected folder will recive a check mark indicating which files will be fingerprinted.

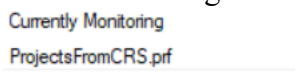


- Now click on floppy disk icon to save. 
- Select location to save newly created profile.

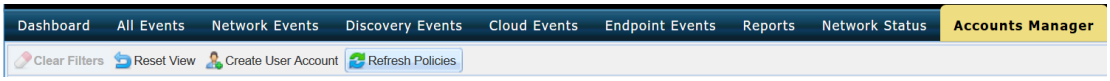
- Now the profile has been saved click the **padlock** icon to start fingerprinting process (Depending on the number of files being fingerprinted this can take a few minutes).
- To view the process see the Output screen that will display what files have been processed and there status. Once completed click **Close**



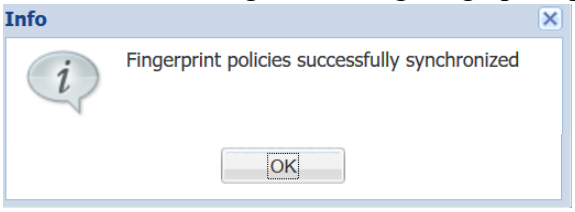
- Now look to the right side window for a tab labeled **"Profiles"** if this is missing click on **"View"** from menu bar and select **"Profiles Window"**. Click on Profile tab and a slide out appears show all the Profiles that can be monitored.
- Now select the Profile that was created earlier and right click, then select **Start Monitoring**.
- Once monitoring is enabled it'll appears under **"Currently Monitoring"** under help.



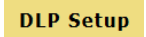
- Files that were included in fingerprinting profile will now have **ACL rules applied from Network DLP section from Central Console**.
- Login to **Central Console** and navigate to **Account Manager** Tab and click Refesh Polices.

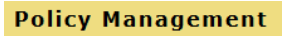


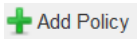
You'll see a message indicating Fingerprint polices successfully synchronized.



How to add policy to GTB Central Console for detecting fingerprinted files

- Login to Central Console
- Click on DLP Setup tab. 

- Now select Policy Management tab. 

- Now double click on Default to launch a new window.
- Click Add Policy. 

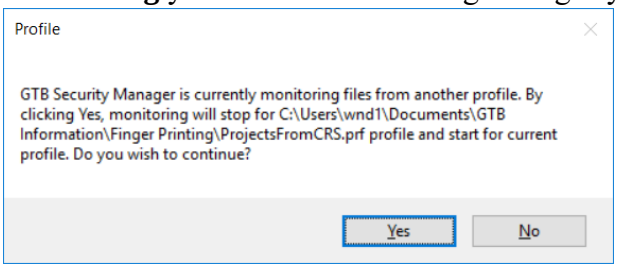
- Click drop down and select File. 

- Now click save button for setting to be applied.

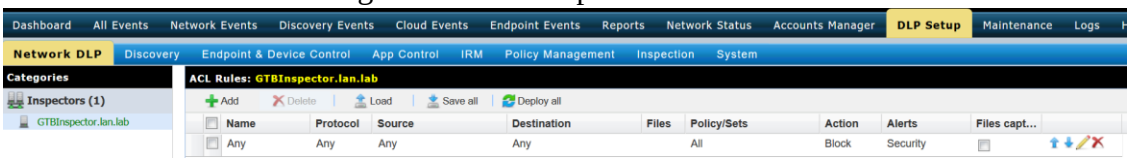
All fingerprinted files from above steps will automatically be added to default Network DLP policy applied ACL. New Default values are **"SSN, CCN, and File"**

Additional Information for Fingerprinting:

- Recommended to configured **GTB Security Manager** to connect to IP address of DLP Inspector.
- Fingerprint only allows for one active Profile at a time. If another profile is set to **Start Monitoring** you'll receive a warning asking if you'd like to disable the active profile.



- Recommendation would be to install **GTB Security Manager** on a machine that can be the central repositoiry for all fingerprinted files. Creating a large folder were the files can placed into for fingerprinting. Files don't have to remain in saved location once the profile has been fingerprinted and uploaded to **Central Console**. Access to fingerprinted files is only required when changes are made to profile containing said files.
- Although only one profile is able to monitored at a time you are able to define multiple Polices within that profile. This is useful since when a fingerprint violation is triggered it will be tagged with the Defined Policy name, which allows for easier usability.
- Fingerprinted files follow **ACL Rules:** created within **Central Console** under **DLP Setup → Network DLP**. Rules are processed in order from top to bottom. This means the first rule with a matching violation takes precedence over rules below.



4.15.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the installation of GTB into the PCS due to its location within the network topology. No manufacturing process components across the boundary on a regular basis while the system is operational.

4.15.7 Link to Entire Performance Measurement Data Set

N/A

4.16 Graylog

4.16.1 Technical Solution Overview

Graylog is an open source log management tool. It can collect, parse and enrich logs, wire data, and event data from any data source. Graylog also provides centralized configuration management for 3rd party collectors such as beats, fluentd and nxlog. The processing pipelines allow for greater flexibility in routing, blacklisting, modifying and enriching messages in real-time as they enter Graylog. It has a powerful search syntax to help query exactly what we are looking for. With Graylog one can even create dashboards to visualize metrics and observe trends in one central location.[28]

Points to consider

- Open source product with good community support
- Easy to setup and customize. Support log collection from any OS platform.
- It is packaged for major Linux distributions, has a VM ready for use and Docker images are also available.
- The dashboard part, even if though well integrated and useful, lacks many features and visualizations contained in other elastic search tools such as Kibana (like aggregations).

4.16.2 Technical Capabilities Provided by Solution

Graylog provides components of the following Technical Capabilities described in Section 6 of Volume 1:

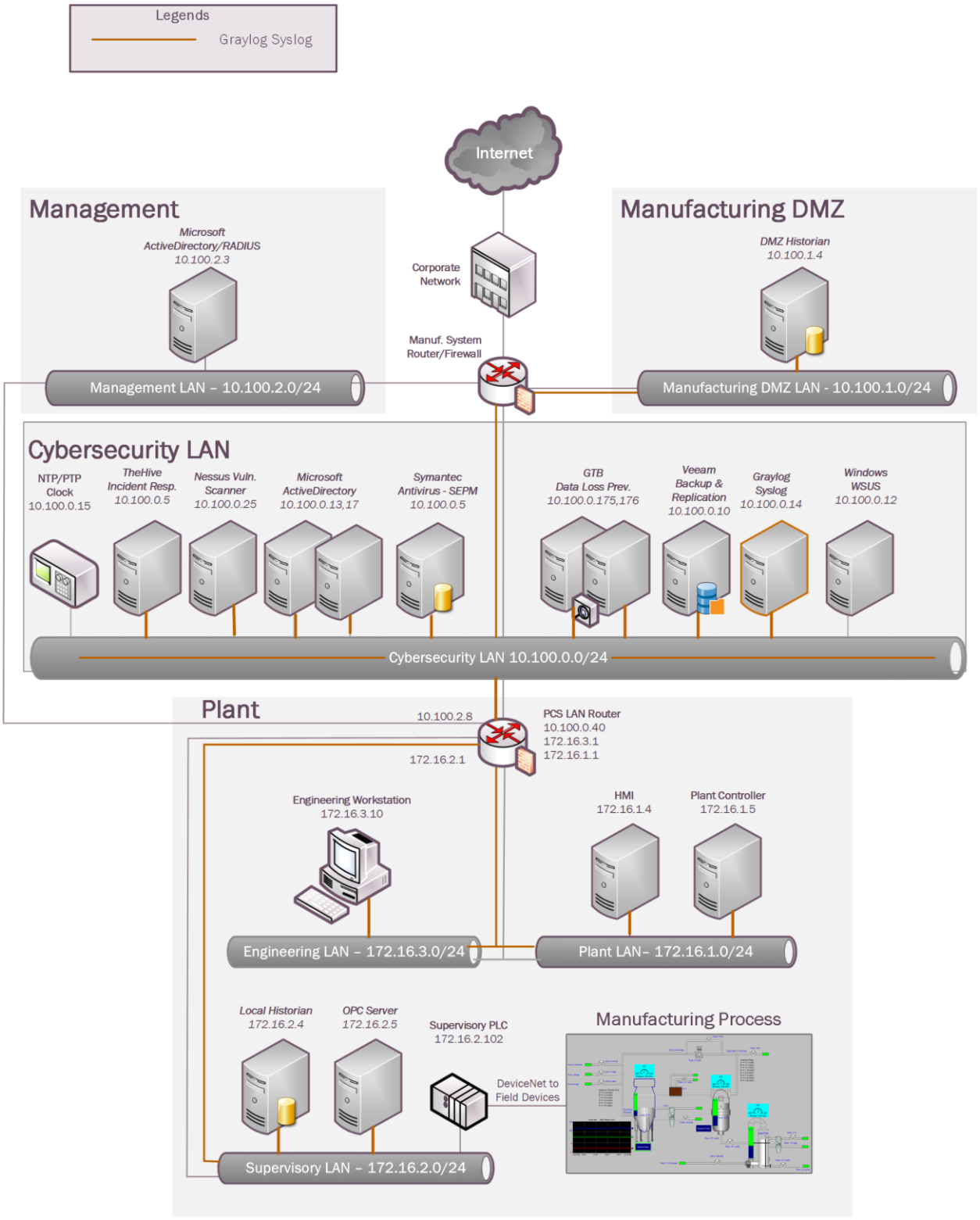
- Network Monitoring
- Event Logging
- Forensics

4.16.3 Subcategories Addressed by Implementing Solution

PR.DS-4, PR.PT-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-6, DE.DP-3, RS.AN-3

[28] Graylog Documentation http://docs.graylog.org/en/3.0/

4.16.4 Architecture Map of Where Solution was Implemented



4.16.5 Installation Instructions and Configurations

Details of the solutions implemented:

Name	Version	Daily volume of logs	Server
Graylog Enterprise	2.4.6	< 5GB per day	Ubuntu 14

Setup:

- Download the installation package from the Graylog website (https://www.graylog.org/). Graylog can be installed on any flavor of Linux. In addition, Graylog also provides a preconfigured virtual machine for **non-production** environments. This virtual machine template (OVA) file was used in our environment.
- The OVA file was deployed on a Microsoft Hyper-V host server in our Cybersecurity LAN network.
- The Graylog server at a minimum requires UDP port 514 which is the default syslog port to be opened. Accordingly, UDP 514 was permitted in the firewall rules. Additional ports such as UDP 5415 and 12202 are also used if configuring other features of Graylog as described in the documentation.
- Upon deploying the OVA file, the virtual machine will default to a DHCP IP address. Login to the system to assign it a static IP address as per below shown instructions.

Assign a static IP

Per default the appliance make use of DHCP to setup the network. If you want to access Graylog under a static IP please follow these instructions:

```
$ sudo ifdown eth0
```

Edit the file `/etc/network/interfaces` like this (just the important lines):

```
auto eth0
  iface eth0 inet static
  address <static IP address>
  netmask <netmask>
  gateway <default gateway>
  pre-up sleep 2
```

Activate the new IP and reconfigure Graylog to make use of it:

```
$ sudo ifup eth0
$ sudo graylog-ctl reconfigure
```

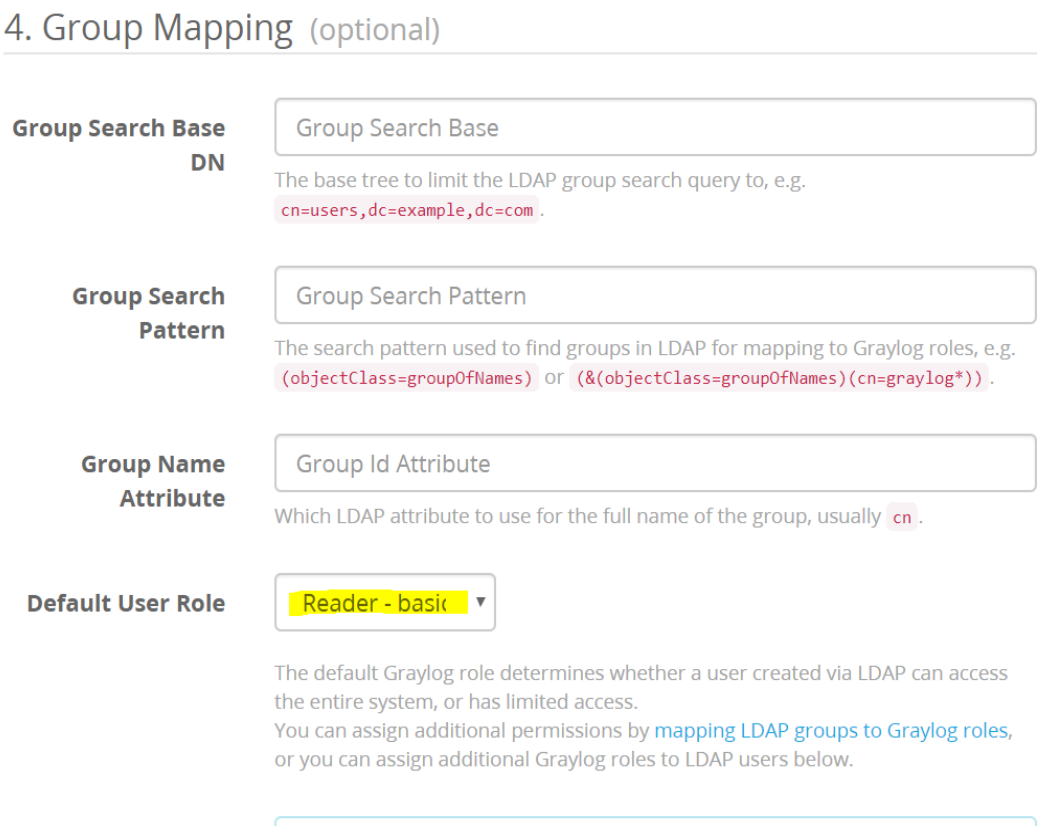
Wait some time until all services are restarted and running again. Afterwards you should be able to access Graylog with the new IP.

- Login to the Web Interface using the default credentials and change the admin password.

- Active Directory (AD)-integration is supported in Graylog. To configure, on the Top Menu Bar, Click on **System** >> **Authentication**. On the Authentication Management page, click on **LDAP / Active Directory** and fill out the AD server details**.** Detailed instructions can be found in product documentation.[29]

    - Note: Any AD domain user that's added is assigned "**Reader**" access by default. This can be changed by configuring **Group Mapping** options in the same page. Change the Default User Role depending on your requirement. Adding permissions can be assigning by clicking on **LDAP Group Mapping** button on the same page

[29] Configuring External Authentication in Graylog
http://docs.graylog.org/en/2.3/pages/users_and_roles/external_auth.html?highlight=ldap



Configuration:

Syslog from Windows servers:

- NXLOG (https://nxlog.co/) was used to forward logs from the Windows hosts in the Process Control System. The free community edition of NXLOG was installed on each windows host. In addition, it was also installed on Active Directory servers in Cyber-security LAN network.

- Once NXLOG is installed, edit the nxlog.conf file located at **C:\Program Files (x86)\nxlog\conf** directory as per whichever category of events you want to forward to your Graylog server. Detailed instructions on NXLOG configuration can be found on its website.[30] Below is a sample nxlog.conf from one of the Windows hosts in the Process Control system

[30] https://nxlog.co/documentation/nxlog-user-guide/

```
## Please set the ROOT to the folder your nxlog was installed into,
## otherwise it will not start.

#define ROOT C:\Program Files\nxlog
define ROOT C:\Program Files (x86)\nxlog

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log

<Extension _syslog>
  Module     xm_syslog
</Extension>

<Input in>
Module     im_msvistalog
ReadFromLast True
Query   <QueryList>\
          <Query Id="0">\
          <Select Path="System">*[System[(EventID=1074)]]</Select>\
  <Select Path="Application">*[System[(EventID=1034)]]</Select>\
          <Select Path="Security">*[System[(EventID=4625)]]</Select>\
          <Select Path="Security">*[System[(EventID=4689)] and
EventData[Data[@Name='ProcessName'] and (Data='C:\Program Files (x86)\Common
Files\Rockwell\RsvcHost.exe')]]</Select>\
          <Select Path='Microsoft-Windows-TerminalServices-
LocalSessionManager/Operational'>*</Select>\
  <Select Path="Veeam Agent">*[System[(EventID=190)]]</Select>\
          <Select Path="FTDiag">*[System[(EventID=1001)]]</Select>\
   </Query>\
    </QueryList>
</Input>

<Output out>
  Module     om_udp
  Host       10.100.0.14
  Port       514
  Exec       to_syslog_bsd();
</Output>
<Route 1>
  Path       in => out
```

As per the screenshot above, we have configured it to forward the below types of events

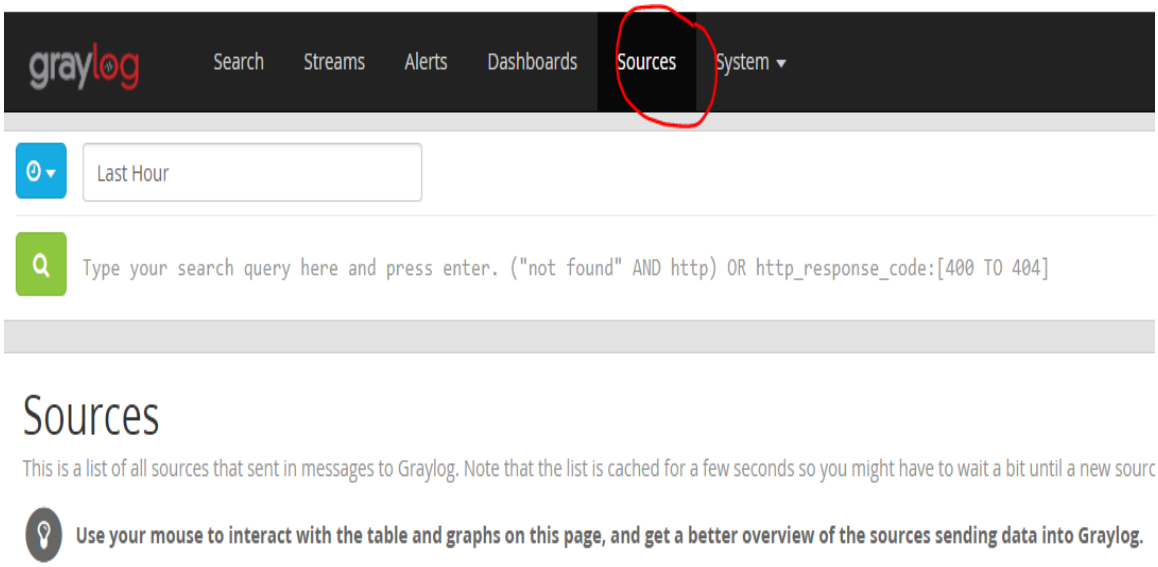
- Event ID 1074 from "System" category to notify us when system gets rebooted

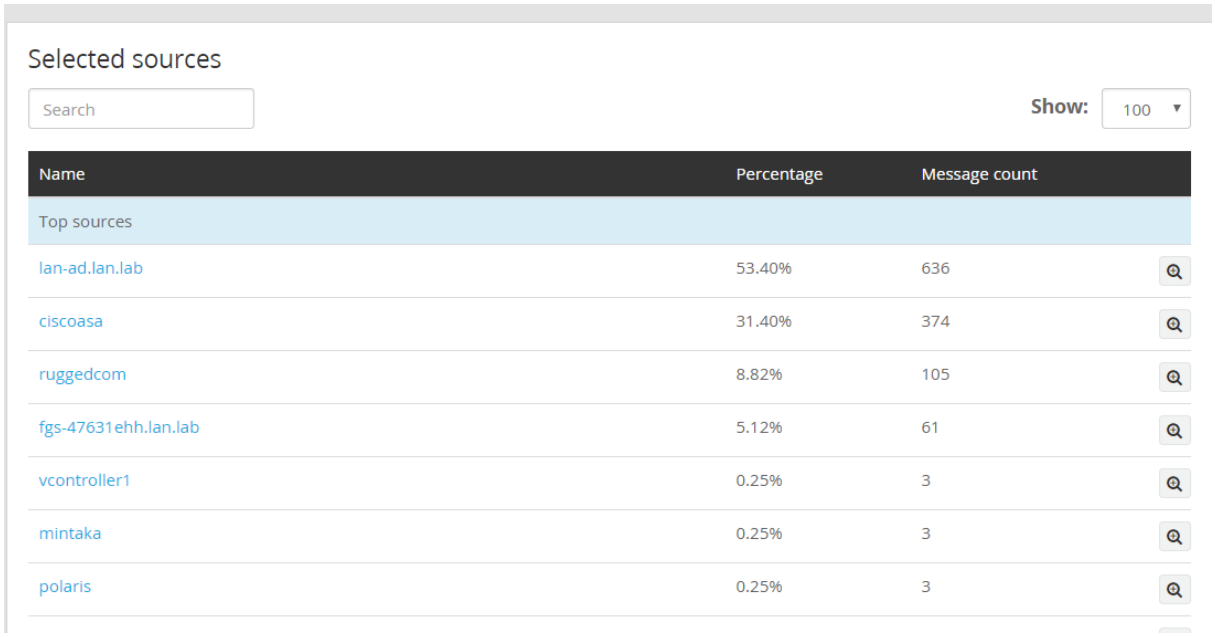
- Event ID 1034 from "Application" category
- Event ID 4625 from "Security" category
- Event ID 4689 from "Security" category and ProcessName= to notify us when the process for Rockwell Automation software stops.
- All events [*] from "*'Microsoft-Windows-TerminalServices-LocalSessionManager*" category to notify us when a user logs in or logs out of the system.
- Event ID 190 from Veeam category to notify us for backup completion messages
- Event ID 1001 from FTDiag category which is a custom event ID generated by Factory Talk Administration Software where there is an authentication failure.

You can add other categories like "**Application**" or "**System**" should you need to collect those events as well. Ensure to balance out the type of events you are sending from your host. Too much noise will eventually make it difficult to search for meaningful logs in Graylog.

Save the nxlog.conf once edited and restart the **NXLOG** windows service. The device will now begin sending syslog (events) to the Graylog server. If the service fails to start, please check the syntax of your nxlog.conf file for any blank spaces or missing parenthesis. Nxlog.conf file is very **sensitive** to proper indentation.

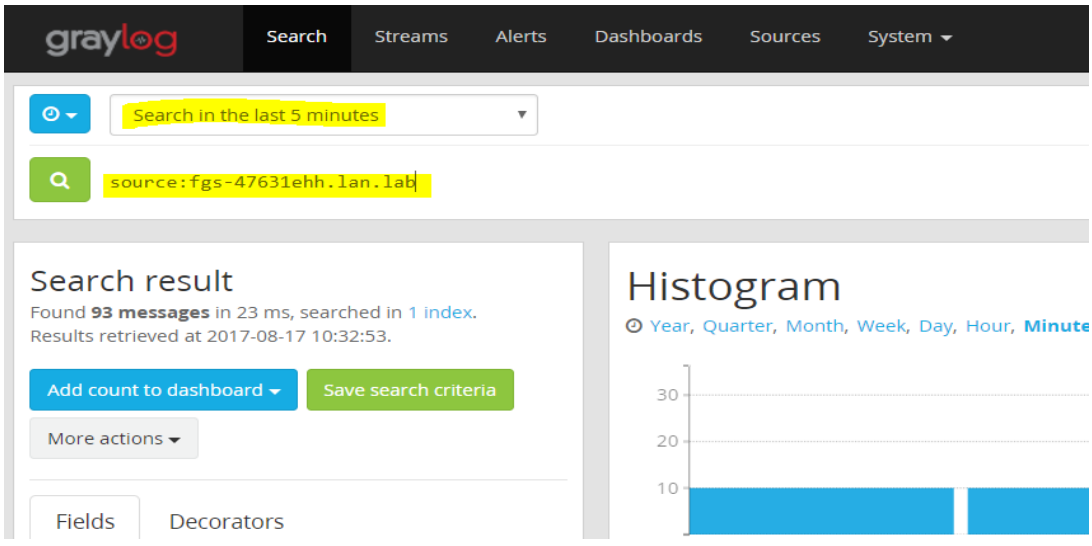
- Login to Graylog Web UI and you should start seeing the events from these windows hosts. Click on "**Sources**" in the Top menu bar to verify if the windows host shows up under the list of "Selected sources". Any device which you configure to send syslog data should begin showing up here under "**Selected Sources**" assuming your configuration is correct. If you don't see your device in here, verify the nxlog config and network connectivity between the end device and Graylog server.





- Search for events from a host by entering a search query and selecting the appropriate time interval in the home page.

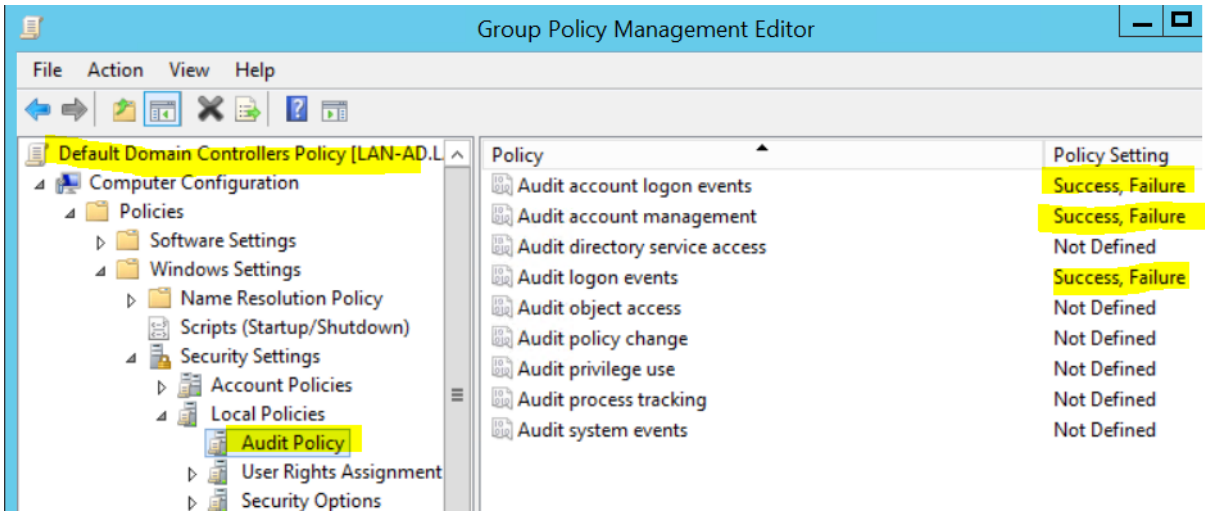
  For example: To search for events by hostname, enter *"source: <windows hostname>"* (without quotes) in the Search *box* as shown below



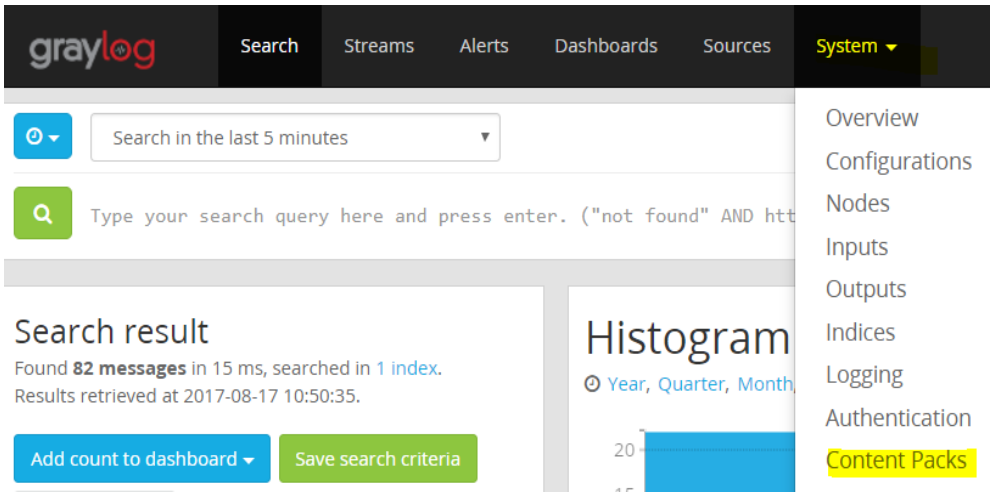
Syslog from Active Directory Domain Controllers

- The **nxlog.conf** configuration remains same on the Domain Controllers as that for a member server except the PORT number to send the data on. In addition, there is a **Content** pack available at Graylog Marketplace, which if installed can parse Active Directory events and generate useful graphs. This content pack requires a different **UDP Port (5414)**. Accordingly, this port was used in the nxlog.conf of the Domain Controllers instead of the default 514. The AD content pack can be downloaded from: https://marketplace.graylog.org/addons/750b88ea-67f7-47b1-9a6c-cbbc828d9e25

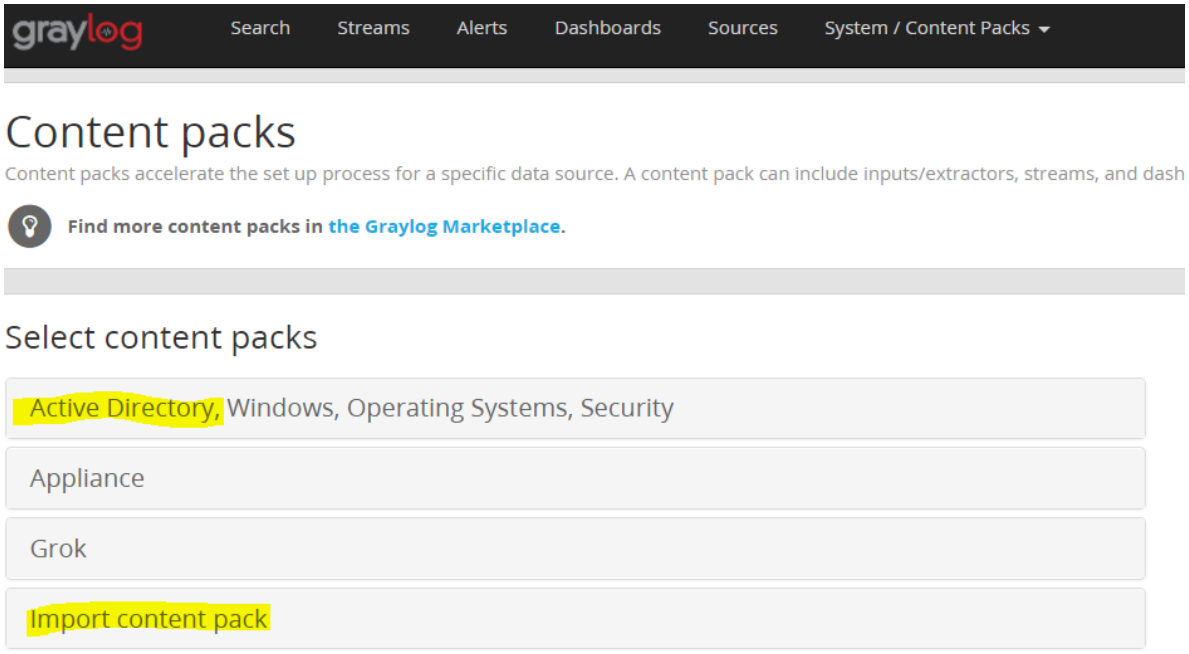
- Ensure to first enable **Auditing** on Domain Controllers (as mentioned in the Requirements section of the Content pack) prior to importing this content pack. This can be done using the "**Default Domain Controllers Policy**" in the Group Policy Management Console on the Domain Controller.



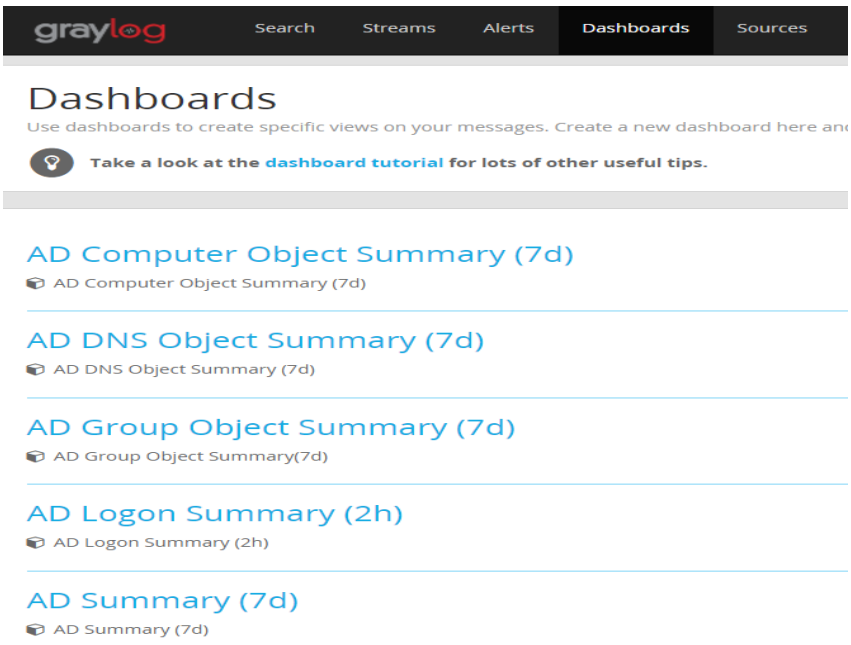
- Next, login to the Graylog Web UI. Click on "System" >> "Content Packs"



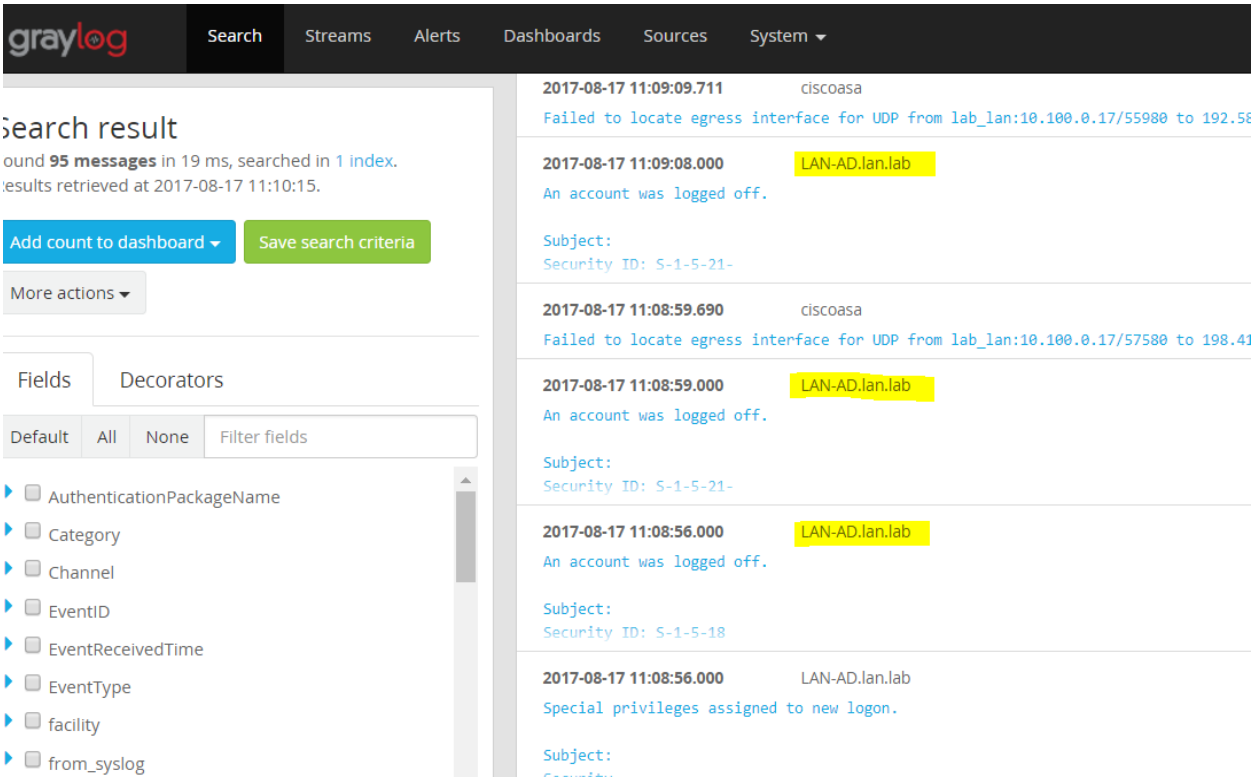
- Download the Active Directory Content pack. Next, click on "**import content packs**" to import it. Once import is completed you should see "**Active Directory**" under "Select Content packs". This is the pack we just imported.



- Click on "**Dashboards**" to view the new graphs of the AD user and group activities. The graphs will begin populating data assuming the AD server is successfully sending over the events to Graylog server.



- On the main dashboard look for events from the AD server. Use the search query as explained in previous steps to look for events using the server hostname.



- **Note**: Likewise, there are lot of useful Content packs and plugins available at Graylog Marketplace for vendor specific technologies / devices such as Cisco, Microsoft DNS, Bro IDS, Cacti, Symantec etc. Download and install each as per the infrastructure in your environment.

Syslog from Boundary Firewall/Network Devices:

- All network devices such as switches and boundary routers from Process Control system were configured to send their syslog data to the Graylog server. There is a device specific setting in each network device to log to a Syslog server. This can be done either via Web UI or CLI of the device.

  The below commands were used on the Boundary Router of the system which is an Allen Bradley Stratix firewall.

  - Enable
  - configure terminal
  - logging enable
  - logging 10.100.0.14

  (Optional) To limit the messages sent based on priority level, enter:

  - logging trap informational
  - end
  - wr mem

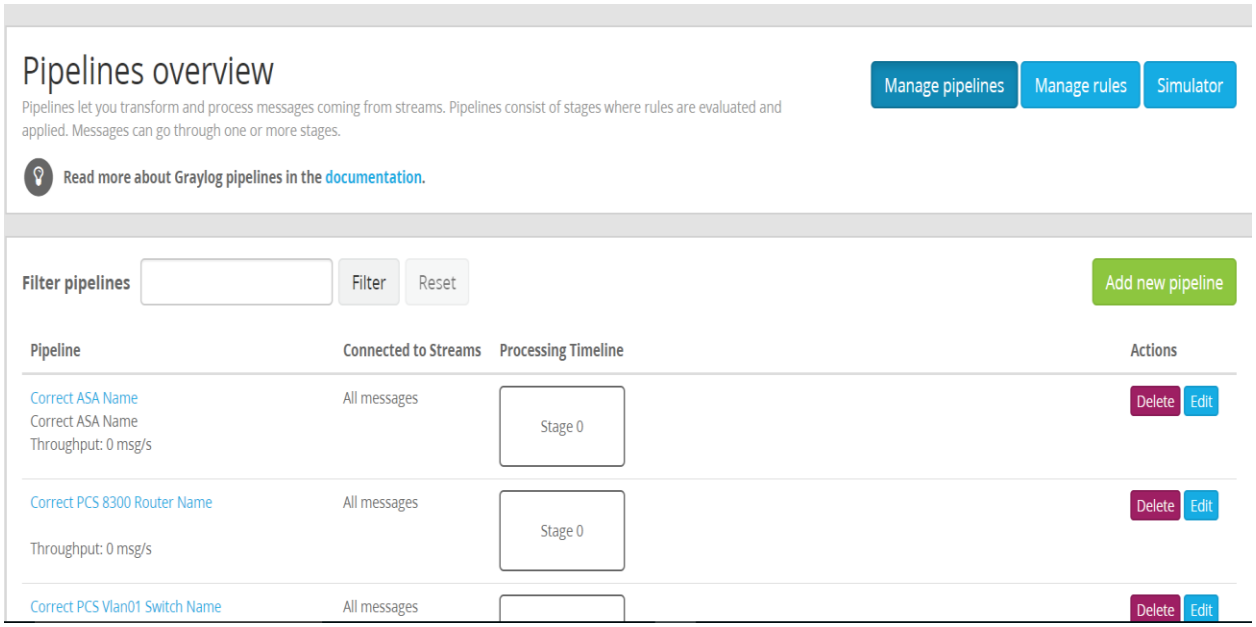
- It was observed that these messages however ended up in Graylog under the device's **IP address** as the **Source** instead of its hostname. This an expected behavior as different vendor devices log in different formats.

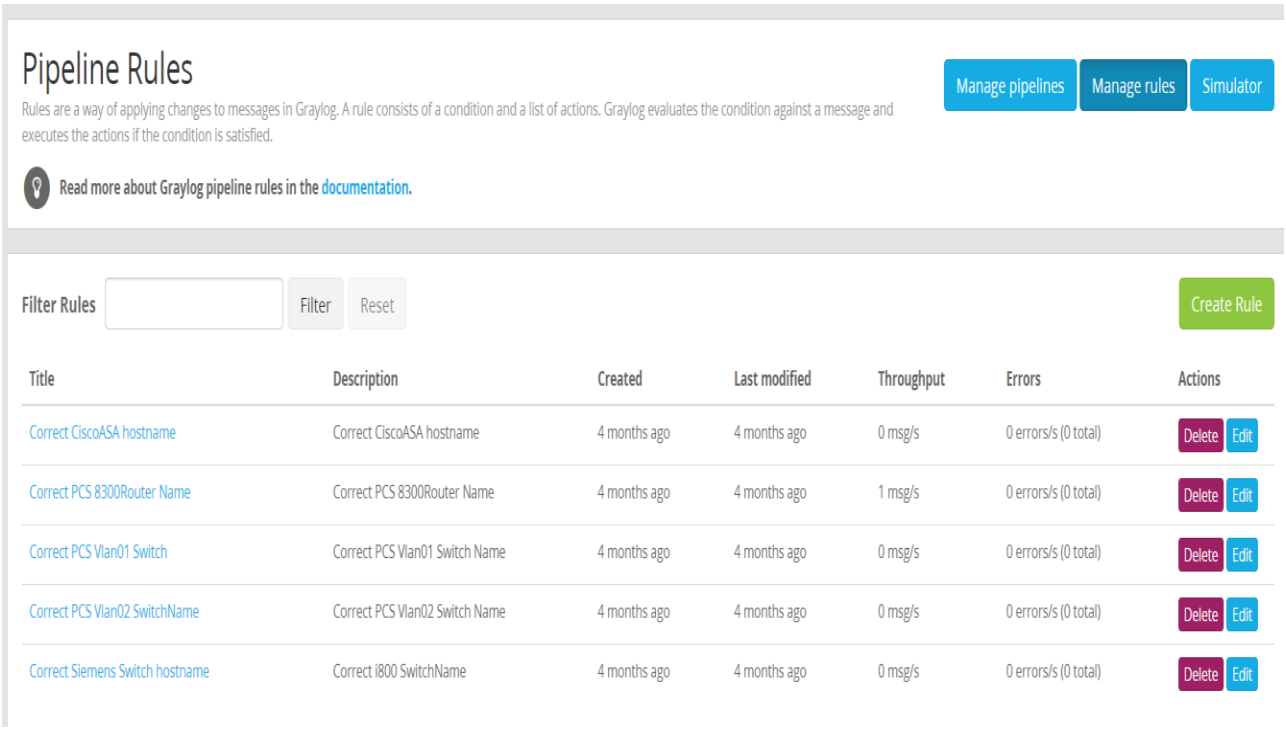
  To overcome this, Graylog offers native features such as Pipelines, Rules, Grok Patterns and Lookup Tables to get around this. Their documentation offers details on creating these http://docs.graylog.org/en/2.4/pages/pipelines.html
  Additional guidance on creating pipelines can be found at https://jalogisch.de/2018/working-with-cisco-asa-nexus-on-graylog/

Configuring Pipelines /Rules for Network devices:

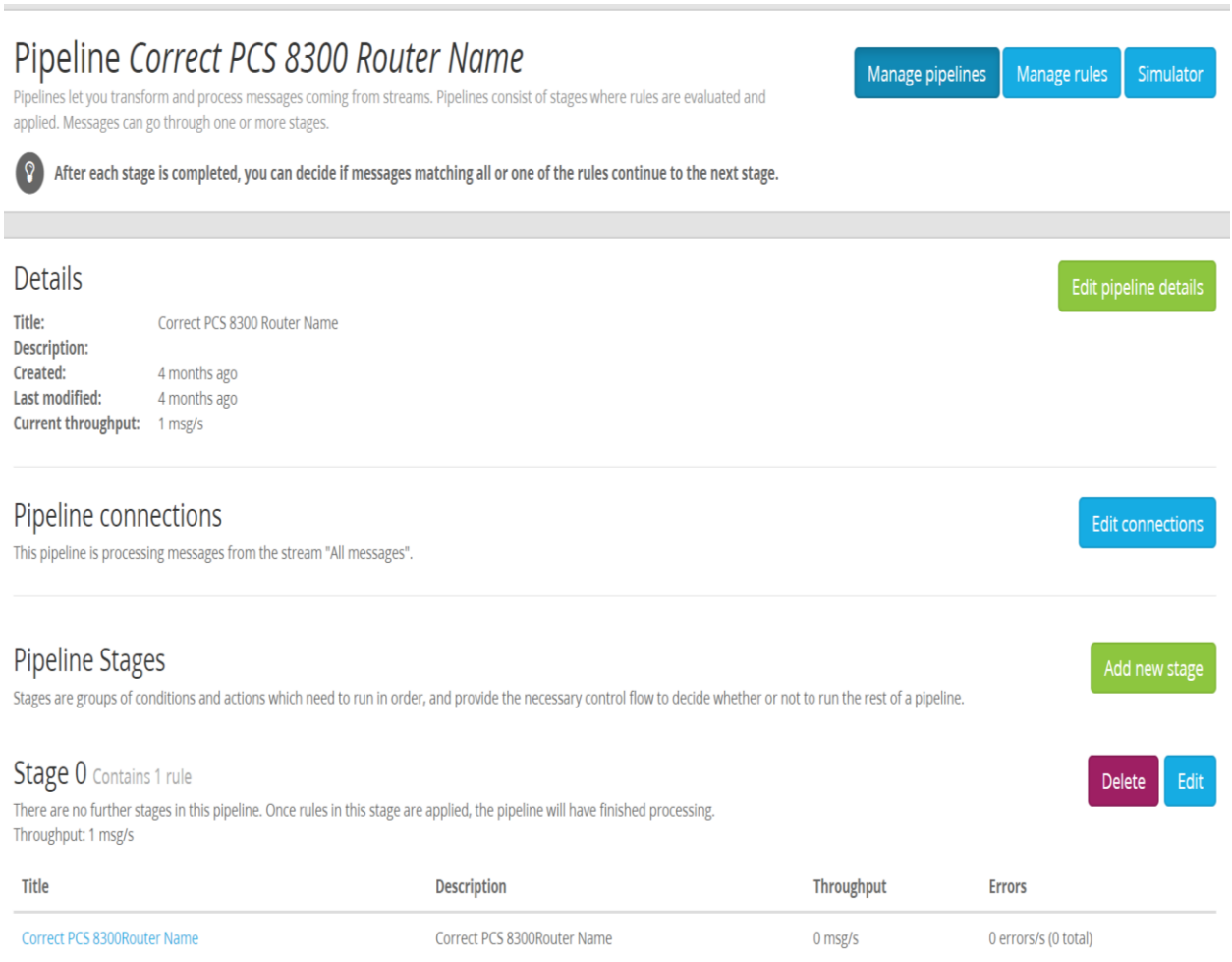
- The following screenshots show some pipelines and rules that were created.

  Pipelines can be created by clicking on **System/Pipelines** >> **Pipelines** option in the TOP Menu bar

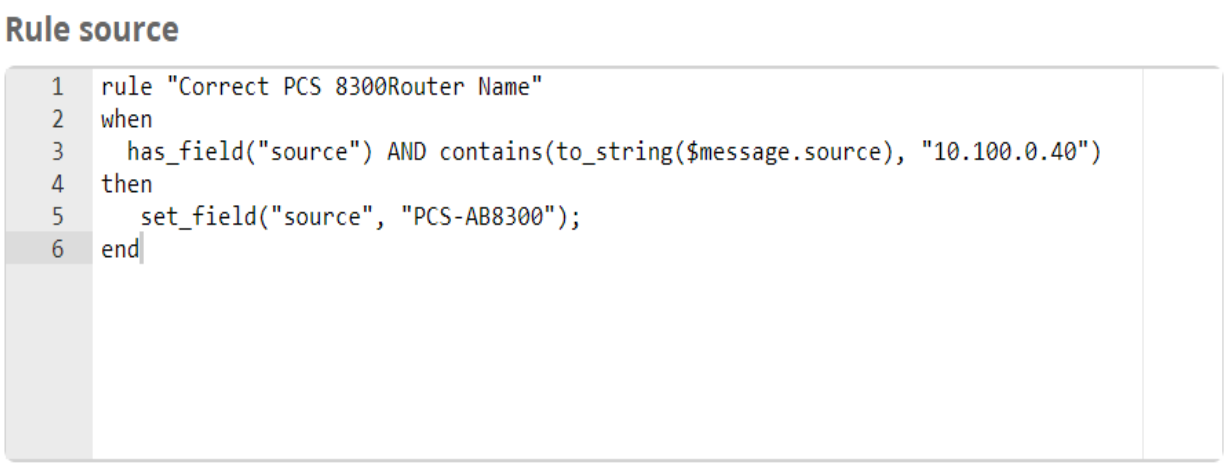




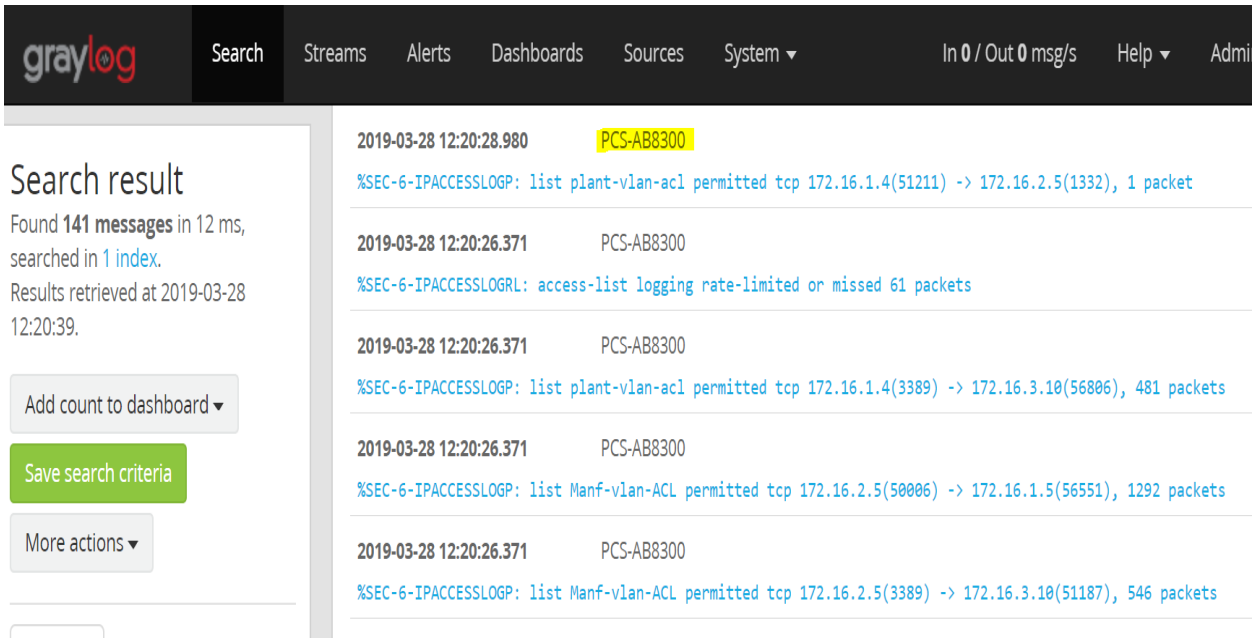
- The following screenshots show details of one such pipeline "**Correct PCS 8300 Router Name**" and its corresponding rule "**Correct PCS 8300 Router Name**" that was created to make the Allen Bradley Boundary Router display its hostname correctly.



Rule: Click on "**Manage Rule**" to create a rule to associate with the pipeline.

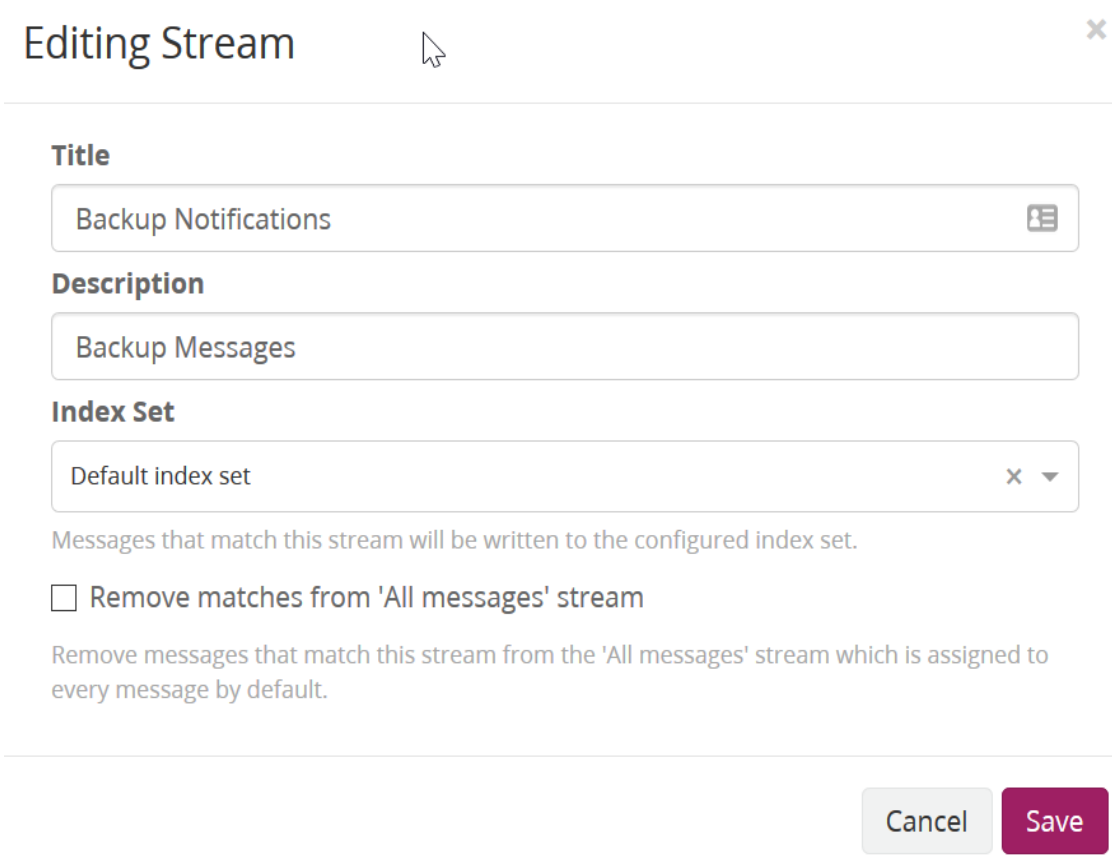


- End Result in the "Search" pane now shows the hostname "PCS-AB8300" as configured in the Rule.



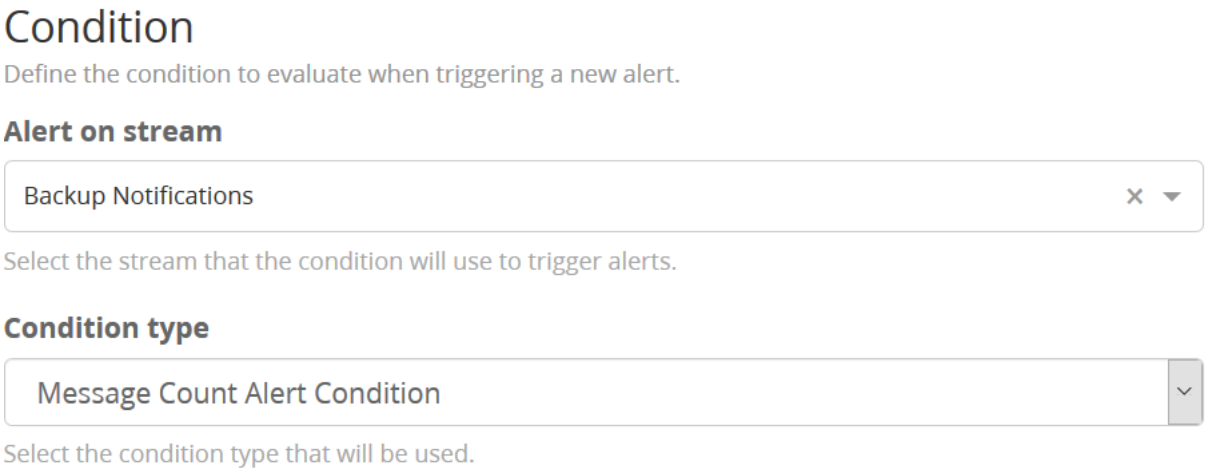
Configuring Email Notifications for Alert conditions:

- You can create email alerts for any custom events, alert condition as per your requirement. Below process show how our Graylog was configured to send out email notifications, for any Veeam backup events that it received from the Windows clients. Follow this process to define your custom alert conditions
- There are multiple configuration settings required for email notification to work – Creating a **stream**, adding an **alert condition** and creating a **notification**.
- To create a stream, click on **Streams** on the Top-Menu >> **Create a Stream** >> Enter Title, Description, and Index Set which should default to "**Default index set**"
- Click **Save** to save the changes



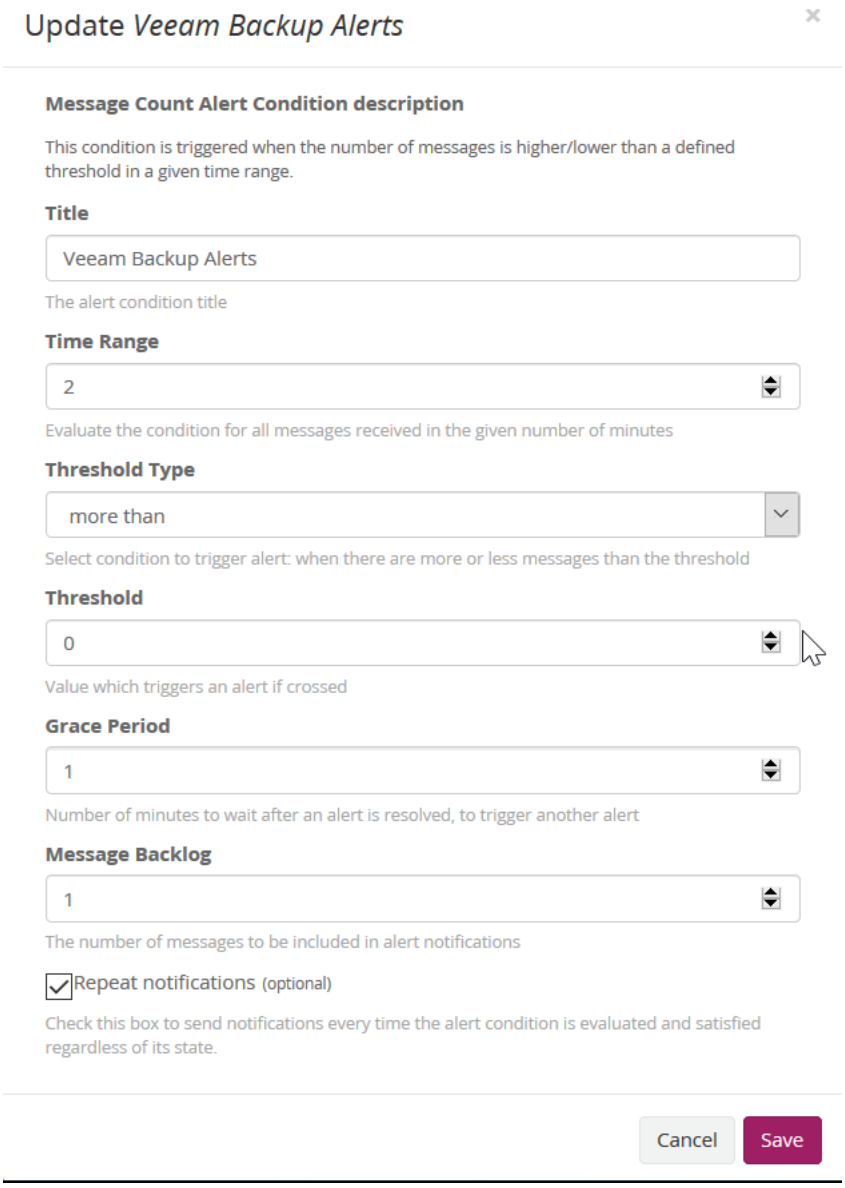
- Next, click on "**Alerts**" options on the top menu >> Click on **Manage conditions** >> Click on  to define a condition.

- Click drop menu under "**Alert on Stream**" and select the stream created earlier. Click on "**Condition Type**" menu drop down and select "**Message Count Alert Condition"**



- Click "**Add Alert Condition"**. Once window appears fill out the required information.

- Click **Save** to complete (See below for example of current Message Count Alert Condition).



- Now create a **notification**.
  - Click on "**Manage notifications**" blue button in upper right-hand corner.
  - Click green button for "**Add new notification**"
  - Under "**Notify on Stream"** select notification created earlier from drop down menu.
  - Under "Notification type" select "Email Alert Callback" from drop down menu.
  - Click "Add alert notification" button
  - Title: "Veeam Backup Alerts"

- Email Subject: “Successfull Veeam Backup source: ${foreach backlog message}${message.source}${end}” without the quotes, see below for screen shot of current callback wording.
- Sender: < sender address >
- E-mail Body: “This can be adjusted as required”

```
Alert Description: ${check_result.resultDescription}
Date: ${check_result.triggeredAt}
Stream ID: ${stream.id}
Stream title: ${stream.title}
Stream description: ${stream.description}
Alert Condition Title: ${alertCondition.title}

${if backlog}Last messages accounting for this alert:
${foreach backlog message}${message}

${end}${else}<No backlog>
${end}
```

- User Receivers: “Select a Graylog user if desired”
- Email Receivers: “Enter email address for individuals receiving these alerts”
- Click **Save**

- Test new Streams / Alerts / Notifications to ensure they are configured correctly.

4.16.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the use of the Graylog due to its typical installation and usage location (i.e., external to the manufacturing system).

4.16.7 Link to Entire Performance Measurement Data Set

N/A

4.17 DBAN

4.17.1 Technical Solution Overview

DBAN is a free open source data wiping utility allowing the ability to sanitize hard drives to ensure data is not left behind when drives are beginning decommissioned and prepared for removal from on-premise. DBAN and other hard drive sanitization tools only work with spinning hard drives, SSD hard drives and other flash media refer to vendors for specific directions for sanitizing media before removing from company control.

4.17.2 Technical Capabilities Provided by Solution

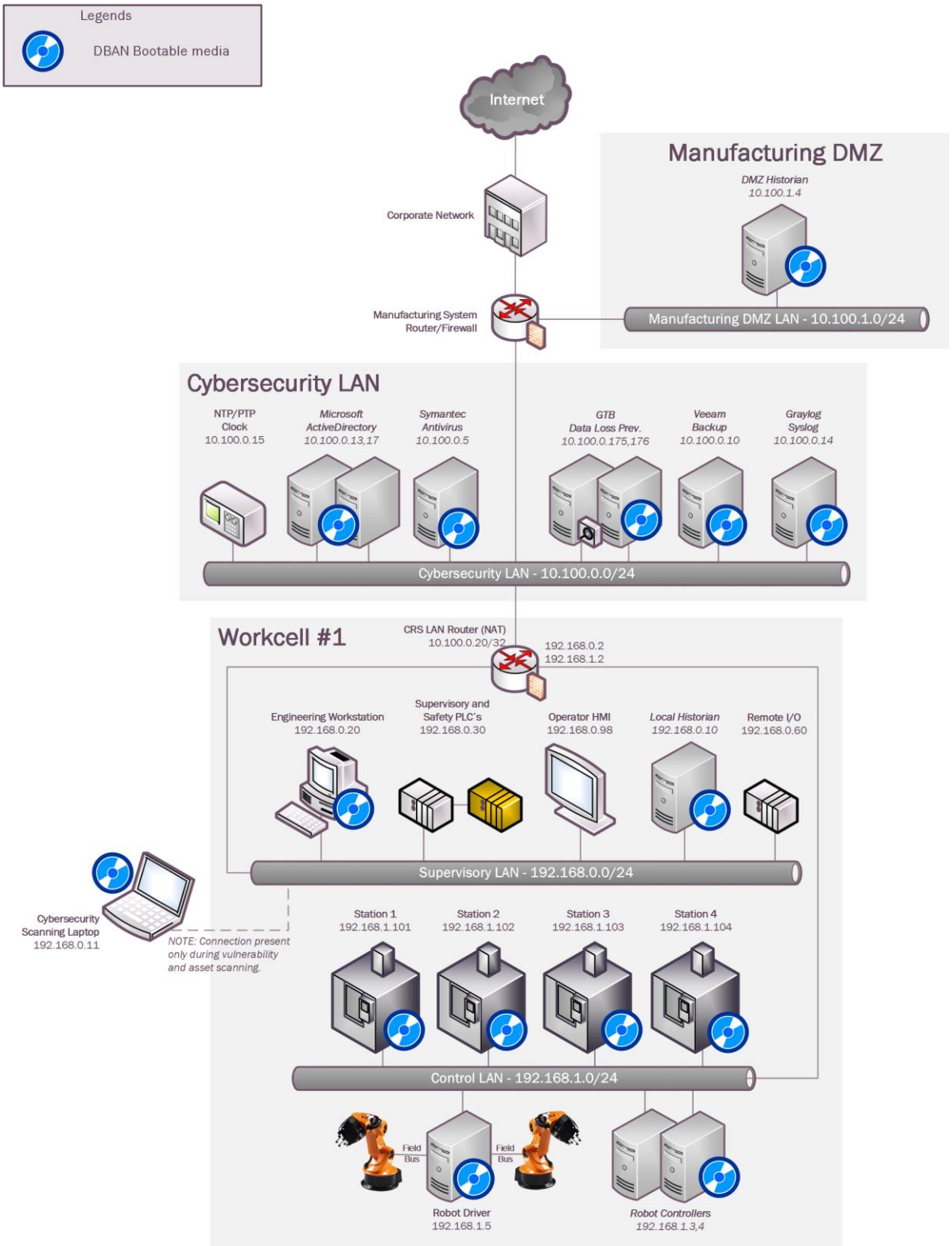
DBAN provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Media Sanitization

4.17.3 Subcategories Addressed by Implementing Solution

PR.DS-3, PR.IP-6

4.17.4 Architecture Map of Where Solution was Implemented



4.17.5 Installation Instructions and Configurations

Instructions for installing DBAN and use

Download:

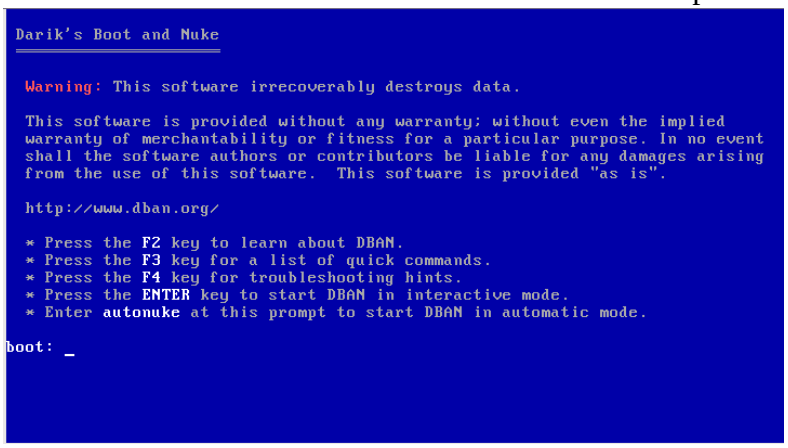
DBAN can be downloaded from https://dban.org

Click download link which redirects the page and a pop will appear to start download process for ISO image file **"dban-2.3.0_i586.iso".**

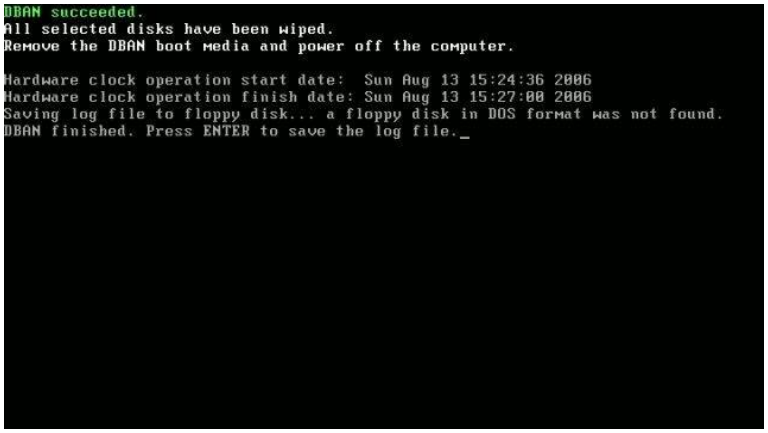
Download ISO file and burn to CD/DVD, or USB drive using widely available ISO bootable utilities.

Instructions:

1. Once ISO has been burned to bootable media go to device requiring sanitization.
2. Power on machine and boot from USB or CD/DVD depending on the install option from earlier steps above. **(Change Boot order in BIOS if no option for Boot Menu is available during machine power-up)**
3. Once machine has booted from media select desire option for media sanitization.



4. Select option to continue. Default sanitization mode is "**short DoD 5520.22-M**", but this can be changed depending on the level your security program indicates.
5. Follow menu options to start wiping process.
6. Once the wipe has completed, you will see a screen like the image below.



7. Once sanitization has completed, remove hard drive from device and label wiped ready for disposal.

Lesson Learned and things to know:

Not all hard drives are able to be wiped clean using this sanitization method. Media that is either SSD or flash memory is written differently than spinning drives, so follow SSD/Flash media vendors' recommendations for proper media sanitization for all non-spinning hard drives.

4.17.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the use of DBAN due to its typical installation and usage location (i.e., external to the manufacturing system).

4.17.7 Link to Entire Performance Measurement Data Set

N/A

4.18 Network Segmentation and Segregation

4.18.1 Technical Solution Overview

Network segmentation and segregation solutions enable a manufacturer to separate the manufacturing system network from other networks (e.g., corporate networks, guest networks), segment the internal manufacturing system network into smaller networks, and control the communication between specific hosts and services.

Each Router's native capabilities were leveraged to implemented network segmentation.

4.18.2 Technical Capabilities Provided by Solution

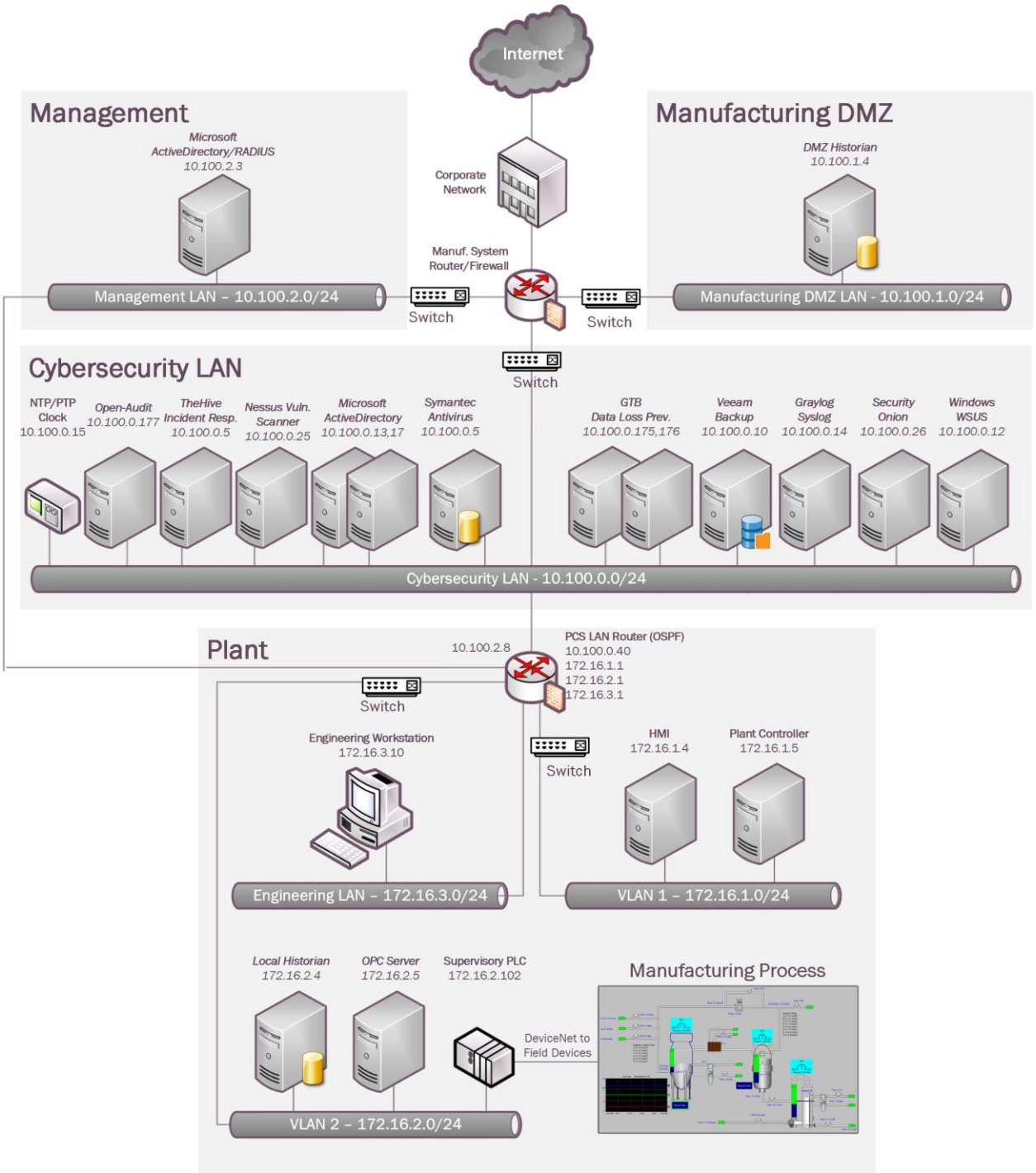
Network Segmentation and Segregation provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Network Segmentation and Segregation

4.18.3 Subcategories Addressed by Implementing Solution

PR.AC-5

4.18.4 Architecture Map of Where Solution was Implemented



4.18.5 Installation Instructions and Configurations

The following devices were involved in implementing Network Segmentation

Device	Details	Location
Cisco-ASA 5512	NGFW, running Firepower Services FTD 6.2.3	Manufacturing System
Allen Bradley Stratix 8300	Firewall, Router	Work cell

- **Segmentation in the Cybersecurity LAN**:

Following is a list of interfaces created on the Boundary Router/Firewall – Cisco ASA of the Cybersecurity LAN network

Interface	IP address of Interface	Subnet	Description
GE 0/0	129.6.66.x	129.x.x.x/x	Uplink to Corporate
GE 0/1	10.100.0.1	10.100.1.0/24	Cybersecurity LAN
GE 0/2	129.6.1.x	129.x.x.x/x	VPN users
GE 0/3	10.100.2.1	10.100.2.0/24	Management LAN
GE 0/4	10.100.1.1	10.100.0.0/24	Manufacturing DMZ LAN

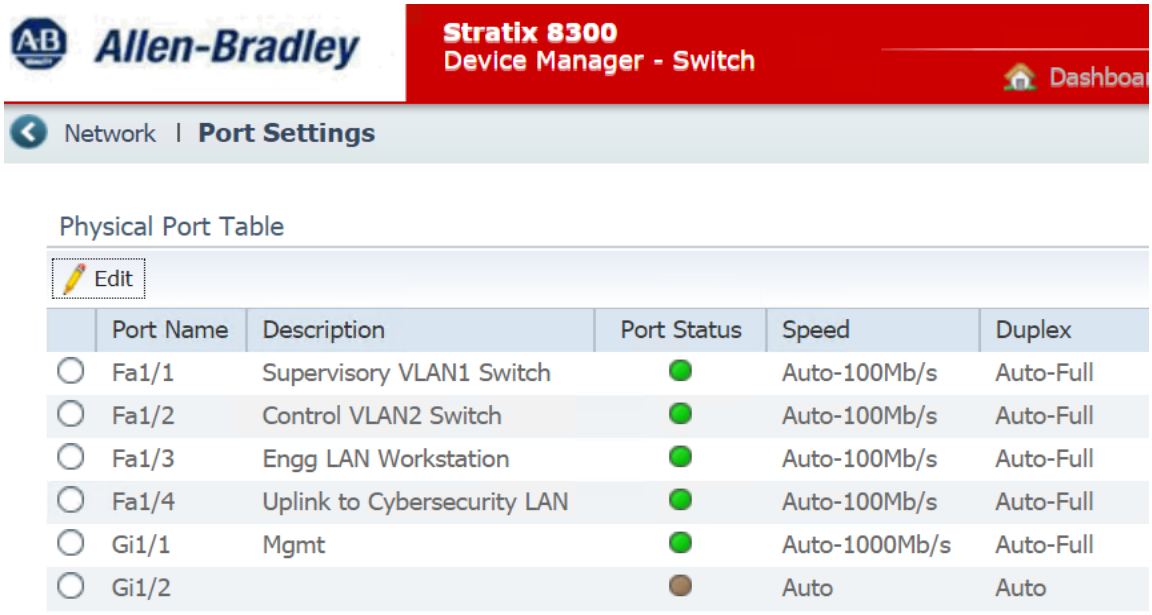
- **Segmentation in the Plant:**

- The Work Cell consists of the following network devices.

Type	Description
Allen Bradley Stratix 8300	Boundary protection Firewall, Router
Allen Bradley Stratix 5700	Layer-2 Switch for the Control Network
Allen Bradley Stratix 5700	Layer-2 Switch for the Supervisory Network

- Following is a list of interfaces created on the Boundary Router – Allen Bradley 8300

Interface	IP address of Interface	Subnet	Description
Fa 1/1	172.16.1.1	172.16.1.0/24	Supervisory Vlan1
Fa 1/2	172.16.2.1	172.16.2.0/24	Control Vlan1
Fa 1/3	172.16.3.1	172.16.3.0/24	Engineering LAN
Fa 1/4	10.100.0.40		Uplink to Cybersecurity LAN
Gi 1/1	10.100.2.8		Management interface



- One of the Stratix 5700 switches was connected to the Fa1/1 interface of the 8300 Router and used for the Supervisory (Vlan1) sub-network. Devices connected to this switch were assigned an IP address from the 172.16.1.0/24 subnet

- The other Stratix 5700 switch was connected to the Fa 1/2 interface of the Router and used for the Plant (Vlan2) sub- network. Devices connected to this switch were assigned an IP address from the 172.16.2.0/24 subnet.

4.18.6 Highlighted Performance Impacts

No performance measurement experiments were performed for network segmentation and segregation due to it being implemented on the PCS before the Manufacturing Profile implementation was initiated.

4.18.7 Link to Entire Performance Measurement Data Set

N/A

4.19 Network Boundary Protection

4.19.1 Technical Solution Overview

Boundary Protection devices are implemented to monitor and control connections and communications at the external boundary and key internal boundaries within the organization. Boundary protection mechanisms include for example, Routers, Firewalls, Gateways, Data diodes separating system components into logically separate networks and sub networks.

4.19.2 Technical Capabilities Provided by Solution

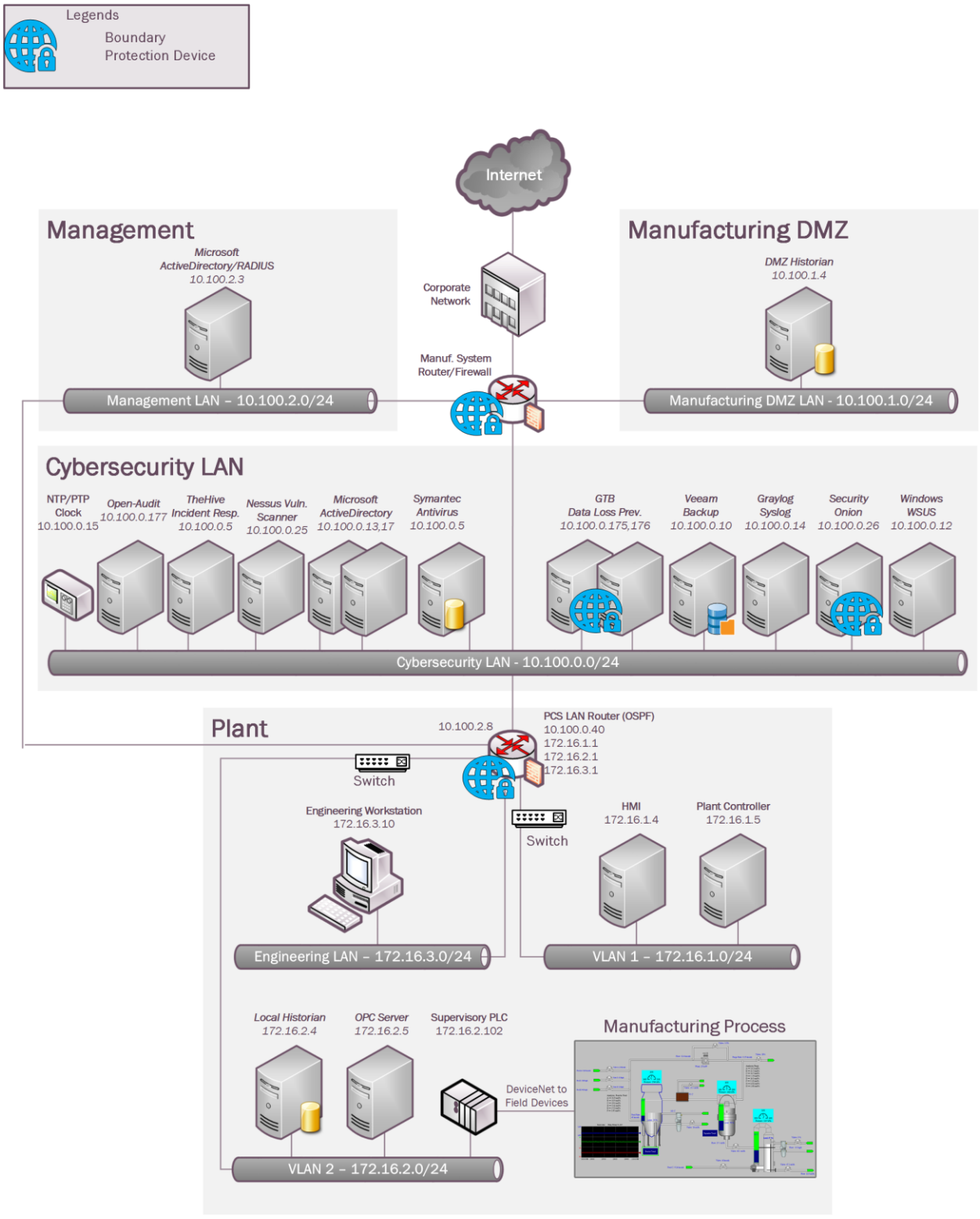
Network Boundary Protection provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Network Boundary Protection

4.19.3 Subcategories Addressed by Implementing Solution

PR.AC-5, PR.PT-4, DE.CM-1

4.19.4 Architecture Map of Where Solution was Implemented



4.19.5 Installation Instructions and Configurations

Setup:

The following devices were implemented for Boundary protection in the PCS System

Device	Details	Location
Cisco-ASA 5512	NGFW, running Firepower Services FTD 6.2.3	Manufacturing System
Allen Bradley Stratix 8300	Firewall, Router	Work cell
GTB Inspector	Data Loss Prevention (DLP) virtual appliance	Cybersecurity LAN
Security Onion	Running Snort, BRO IDS	Cybersecurity LAN

- **Configuration on Cisco-ASA**:

The following features, settings were enabled on the ASA firewall

- Network Segmentation
- ACL Rules
- NAT policy for Internet access
- Snort Inspection
- DMZ network

Network Segmentation

Separate network interfaces were configured for the different network segments as listed below

- Inside Interface (Network: 10.100.0.0/24)
- DMZ Interface (Network: 10.100.1.0/24)
- Outside Interface (Network:129.6.91.x/24, Uplink to NIST Corporate for Internet)
- Public interface (Network:129.6.1.x/24 For VPN Users)

Access Control List (ACL) rules

The following rules were put in place on the ASA with a default Action to **Block all traffic**.

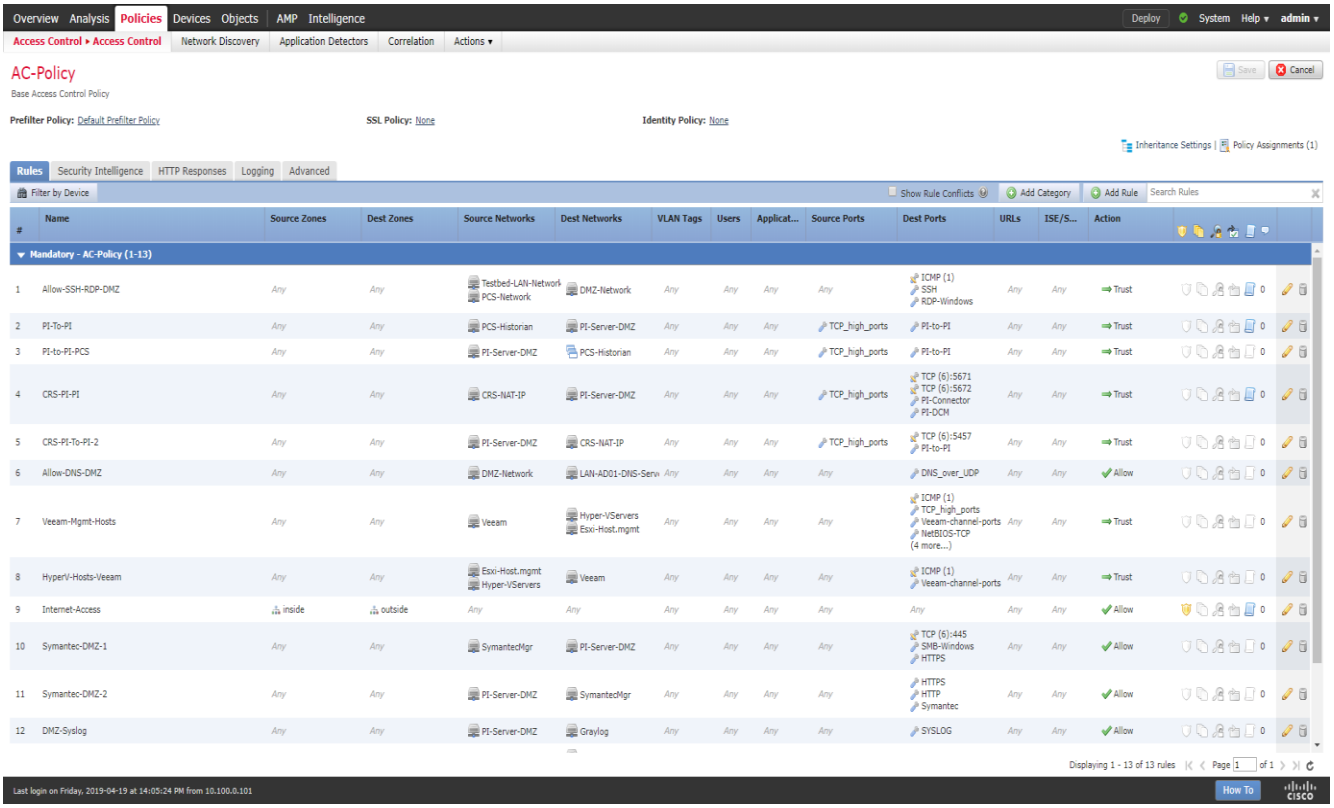
5668

Source	Source Port	Destination	Dest Ports	Protocol	Action
10.100.0.0/24, 172.16.0.0/22	Any	DMZ network	SSH,RDP,ICMP	TCP	Trust
PCS-Historian (172.16.2.14)	TCP_High_Ports	DMZ-Historian	5450	TCP	Trust
DMZ Historian	TCP_High_Ports	PCS-Historian	5450	TCP	Trust
CRS-NAT (10.100.0.20)	TCP_High_Ports	DMZ-Historian	5450, 5460, 5671, 5672	TCP	Trust
DMZ Historian	TCP_High_Ports	CRS-NAT (10.100.0.20)	5457, 5450	TCP	Trust
DMZ Historian	Any	Active Directory (10.100.0.17)	53	UDP	Allow
Veeam Server	Any	Hyper-V Host servers, Esxi Host Server	NETBIOS, ICMP, HTTPS, 445, TCP_High_ports, 2500-5000, 6160-6163	TCP	Trust
Hyper-V Host Servers, Esxi Host Server	Any	Veeam Server	ICMP, 2500-5000	TCP	Trust
inside_interface	Any	outside_interface	Any	Any	Allow
DMZ Historian	Any	Symantec Server	SMB (445), HTTPS	TCP	Trust
Symantec Server	Any	DMZ Historian	HTTP, HTTPS, 8014	TCP	Trust
DMZ Historian	Any	Graylog Server	514	UDP	Trust
VPN_Pool (192.168.100.10 - .20)	Any	PCS-HMI-Server, PCS-Workstation	3389	TCP	Allow

5669

5670

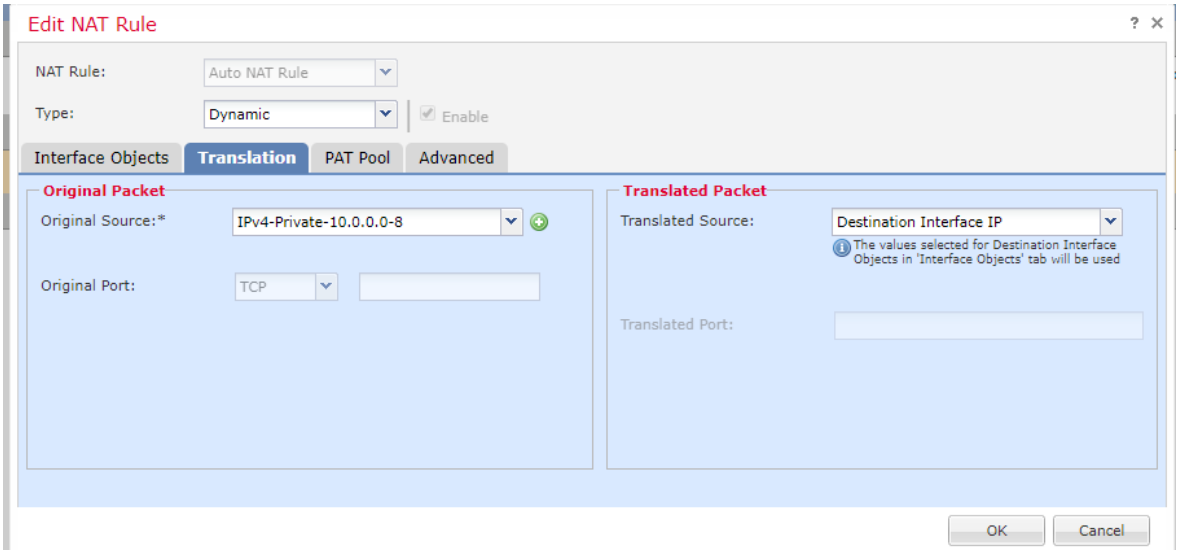
5671



NAT Policy

- A Dynamic NAT policy was configured to allow internet access.

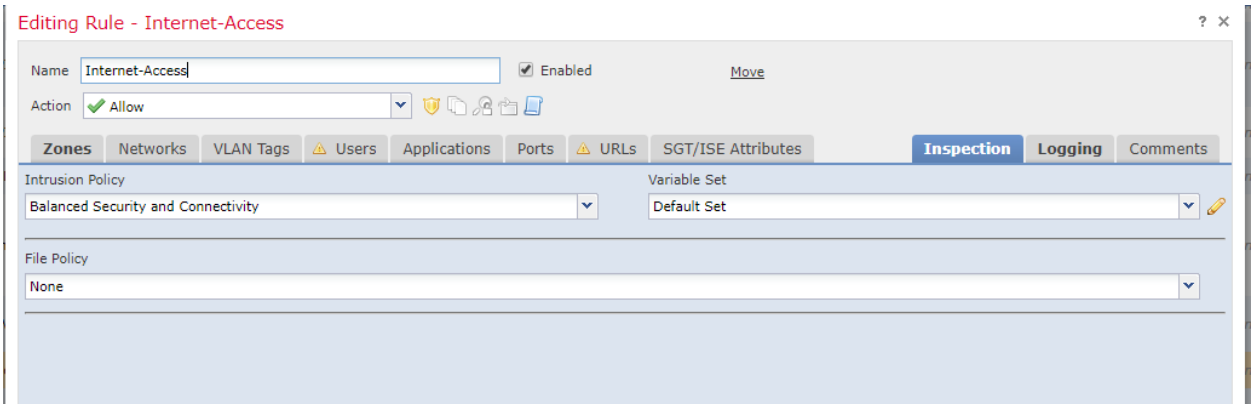
Type of NAT rule	Auto NAT [1]
Source Interface	inside
Destination Interface	outside
Original sources	10.100.0.0/8
Translated Source	Destination Interface IP
Options	Translate DNS Replies that match this Rule: False



Snort Inspection

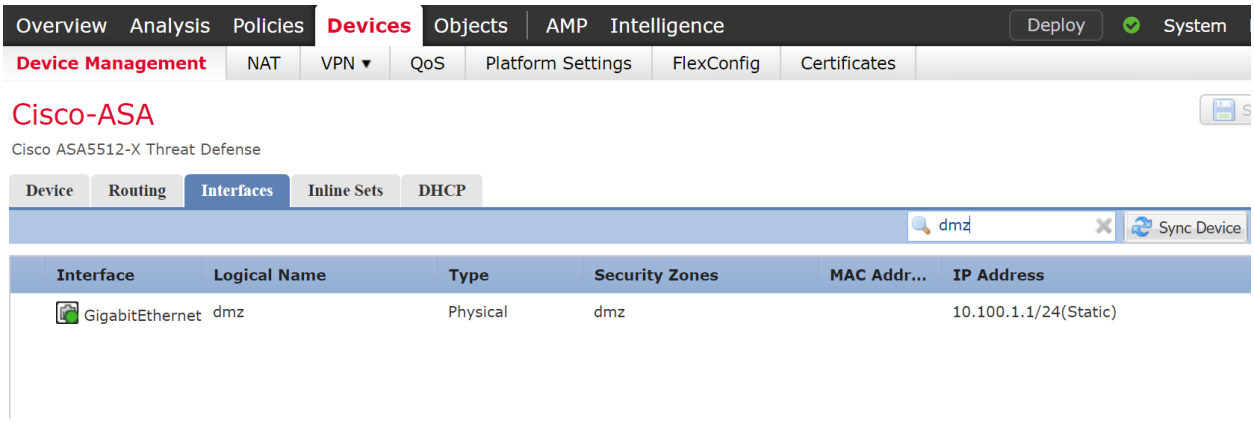
- Snort Inspection was enabled on the following ACL rules

Name of the ACL	Intrusion Policy
Allow-DNS-DMZ	Balanced connectivity and security
Internet-Access rule	Balanced connectivity and security
VPN-Rule	Balanced connectivity and security



5683 **DMZ Network**

5684 A Separate interface was setup for the Manufacturing DMZ LAN Network for hosting the **DMZ**
5685 **Historian** server.



5686

5687 • **Configuration of Allen Bradley Firewall:**

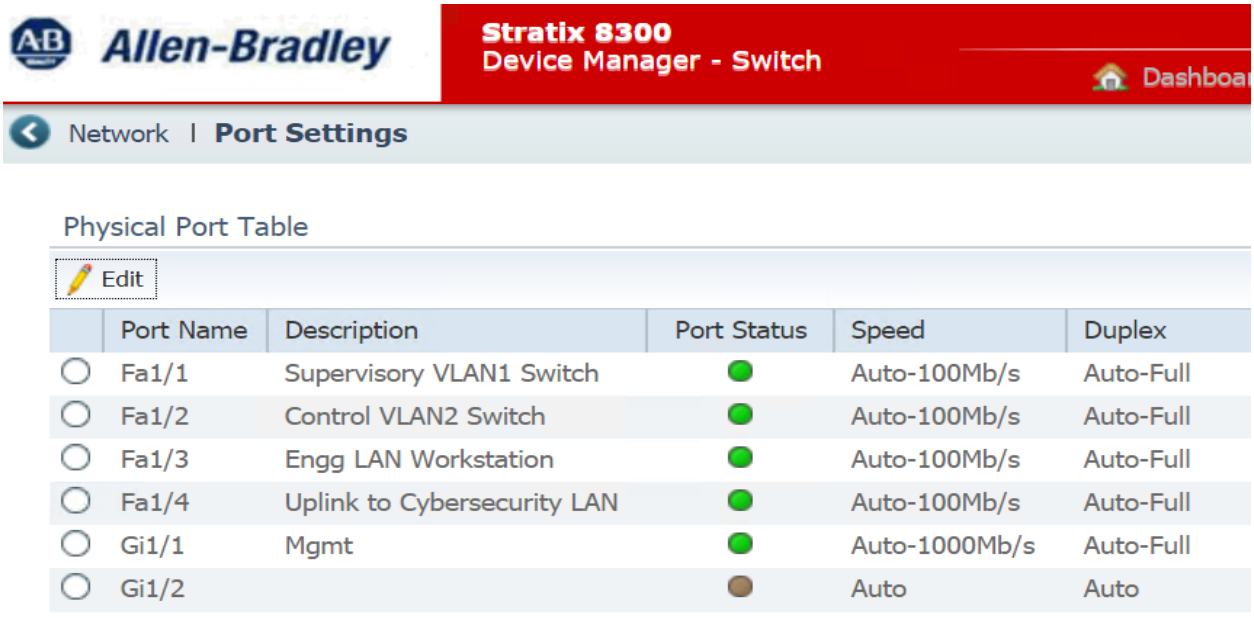
5688 The following features, settings were enabled on this firewall

5689 • Network Segmentation
5690 • ACL Rules

5691 **Network Segmentation**

5692 Separate network interfaces were configured for the different network segments as listed below

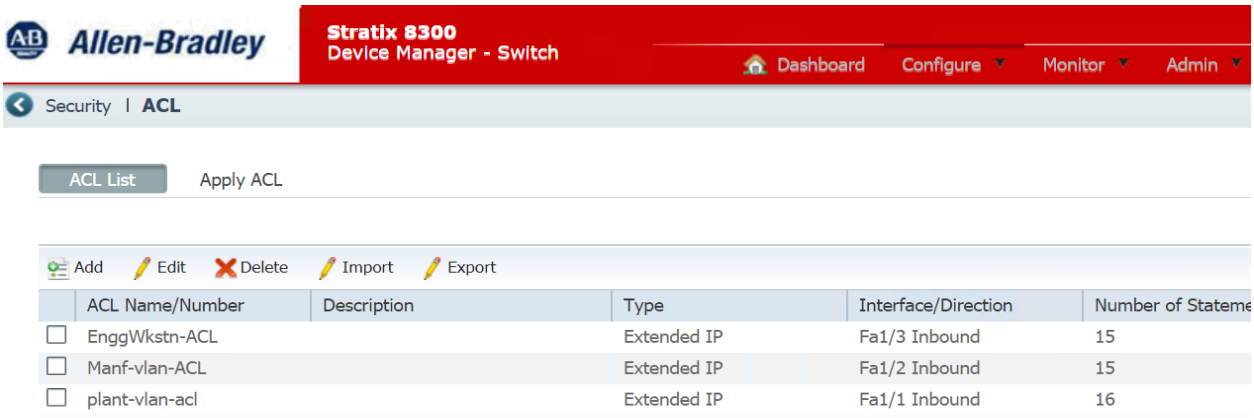
5693 • Supervisory VLAN1 (Network: 172.16.1.0/24)
5694 • Control VLAN2 Interface (Network: 172.16.2.0.0/24)
5695 • Engineering LAN (Network: 172.16.3.0/24)
5696 • Uplink (IP:10.100.0.40, Uplink to Cybersecurity LAN)
5697 • Management interface (IP:10.100.2.8)



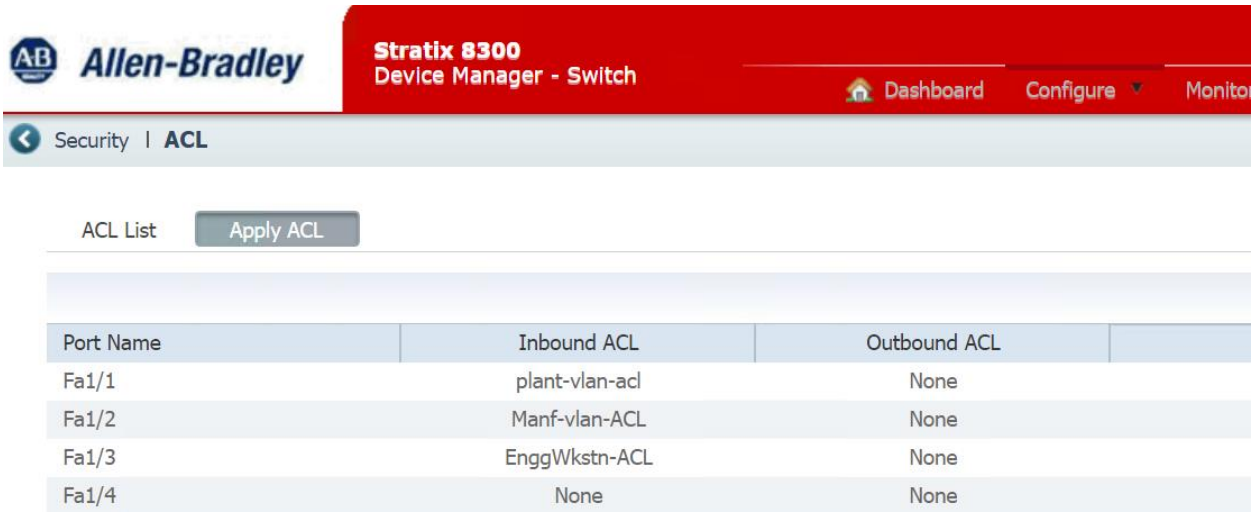
5698

5699 **Access Control List (ACL) rules**

5700 Three ACLs of Extended type were created as shown below. Each one was associated to a
5701 specific network interface as an Inbound ACL



5702



5703

```
ip access-list extended EnggWkstn-ACL
 permit ip host 172.16.3.10 10.100.0.0 0.0.0.255
 permit tcp host 172.16.3.10 172.16.1.0 0.0.0.15 eq 3389
 permit tcp host 172.16.3.10 172.16.2.0 0.0.0.15 eq 3389
 permit icmp host 172.16.3.10 any
 permit tcp host 172.16.3.10 host 172.16.2.102 eq 44818
 permit ip host 172.16.3.10 host 172.16.3.1
 permit ip host 172.16.3.10 host 172.16.2.2
 permit ip host 172.16.3.10 host 172.16.1.3
 permit tcp host 172.16.3.10 host 10.100.1.4 eq 3389
 permit tcp host 172.16.3.10 host 129.6.1.2 eq ftp
 permit tcp host 172.16.3.10 host 129.6.1.2 eq 22
 permit tcp host 172.16.3.10 host 129.6.1.2 eq www
 permit tcp host 172.16.3.10 host 172.16.2.102
 permit tcp 192.168.100.0 0.0.0.255 host 172.16.3.10 eq 3389
 permit tcp host 172.16.3.10 host 192.168.100.10 gt 49000
```

5704

5705

```
ip access-list extended Manf-vlan-ACL
 permit ip 172.16.2.0 0.0.0.15 172.16.1.0 0.0.0.15 log
 permit icmp 172.16.2.0 0.0.0.255 any log
 permit tcp 172.16.2.0 0.0.0.255 host 172.16.3.10 gt 49000 log
 permit ip 172.16.2.0 0.0.0.255 host 10.100.0.5 log
 permit ip 172.16.2.0 0.0.0.255 host 10.100.0.10 log
 permit ip 172.16.2.0 0.0.0.255 host 10.100.0.13 log
 permit ip 172.16.2.0 0.0.0.255 host 10.100.0.17 log
 permit ip 172.16.2.0 0.0.0.255 host 10.100.0.25 log
 permit ip 172.16.2.0 0.0.0.255 host 10.100.0.177 log
 permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.234 log
 permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.12 eq www log
 permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.12 eq 443 log
 permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.12 eq 8530 log
 permit udp 172.16.2.0 0.0.0.255 host 10.100.0.14 eq syslog log
 permit tcp host 172.16.2.14 host 10.100.1.4 gt 49000 log
```

```
ip access-list extended plant-vlan-acl
 permit ip 172.16.1.0 0.0.0.15 172.16.2.0 0.0.0.15 log
 permit icmp 172.16.1.0 0.0.0.255 any log
 permit tcp 172.16.1.0 0.0.0.255 host 172.16.3.10 gt 49000 log
 permit ip 172.16.1.0 0.0.0.255 host 10.100.0.5 log
 permit ip 172.16.1.0 0.0.0.255 host 10.100.0.10 log
 permit ip 172.16.1.0 0.0.0.255 host 10.100.0.13 log
 permit ip 172.16.1.0 0.0.0.255 host 10.100.0.17 log
 permit ip 172.16.1.0 0.0.0.255 host 10.100.0.25 log
 permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.234 log
 permit udp 172.16.1.0 0.0.0.255 host 10.100.0.14 eq syslog log
 permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.12 eq www log
 permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.12 eq 443 log
 permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.12 eq 8530 log
 permit ip 172.16.1.0 0.0.0.255 host 10.100.0.177 log
 permit tcp 192.168.100.0 0.0.0.255 host 172.16.1.4 eq 3389 log
 permit tcp host 172.16.1.4 192.168.100.0 0.0.0.255 gt 49000 log
```

- **Configuration of GTB Inspector:**

Refer to Section 4.15 for details.

- **Configuration of Security Onion:**

Refer to Section 4.7 for details

4.19.6 Highlighted Performance Impacts

The following performance measurement experiment was performed for the network boundary protection while the manufacturing system was operational:

Experiment PL004.1- Firewall rules are activated at the PCS boundary router

There was no significant performance impact observed when firewall rules were activated. For example, the packet round trip time between the HMI and OPC remained mostly constant before and after the firewall rules were activated.

Care needs to be used for implementation of the rules and a thorough understanding of the system is important. A misconfigured firewall rule can block a legitimate connection and cause system failure.

In the PCS system implementation, a thorough analysis on network connections was performed to identify all the legitimate connections in order to implement the firewall rules. Some network connections are legitimate but not obvious or only stayed connected for a short amount of time. Validation test was performed to ensure all the legitimate network connections for normal operation are allowed. The implementation and validation test was completed during a planned system down time.

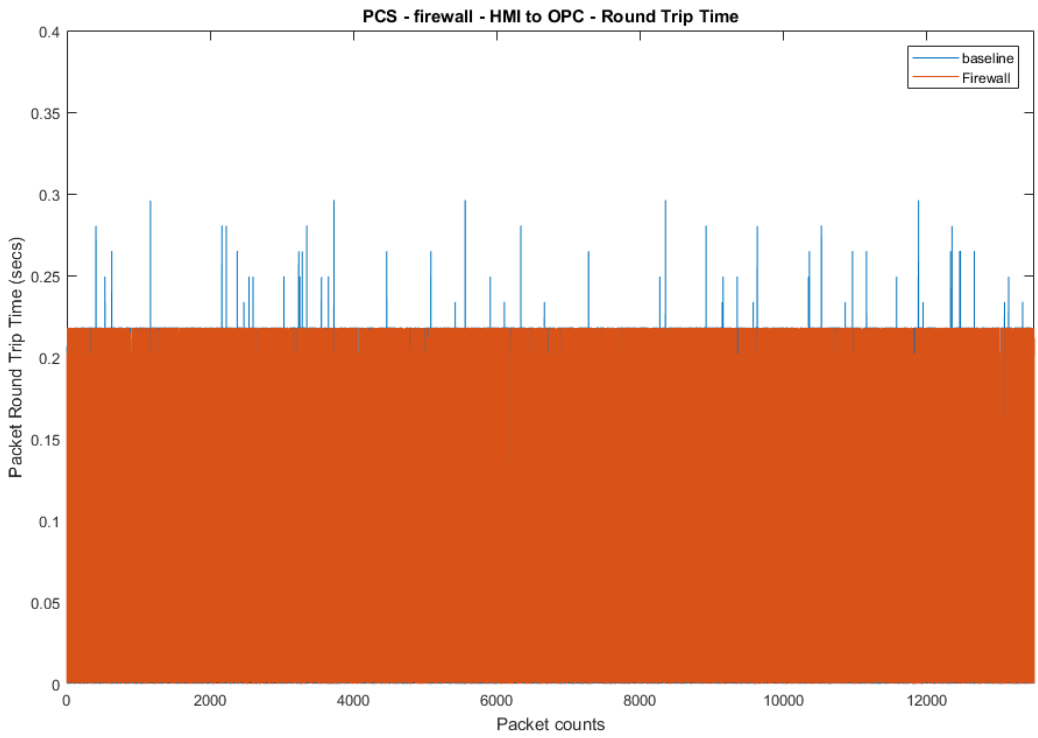
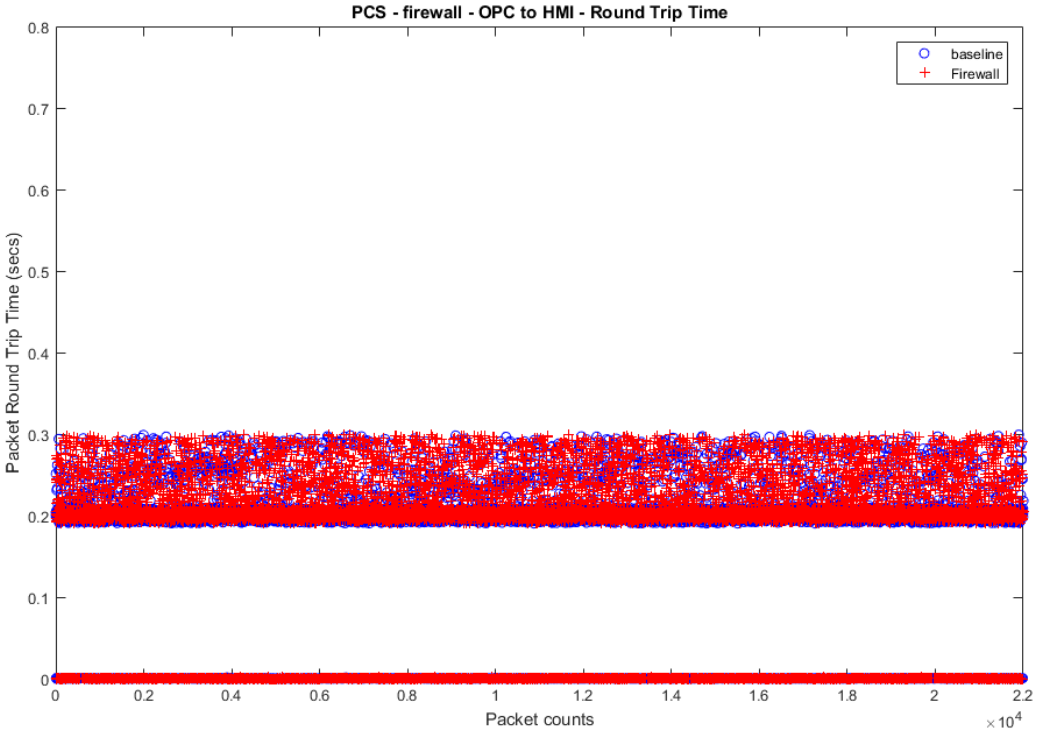


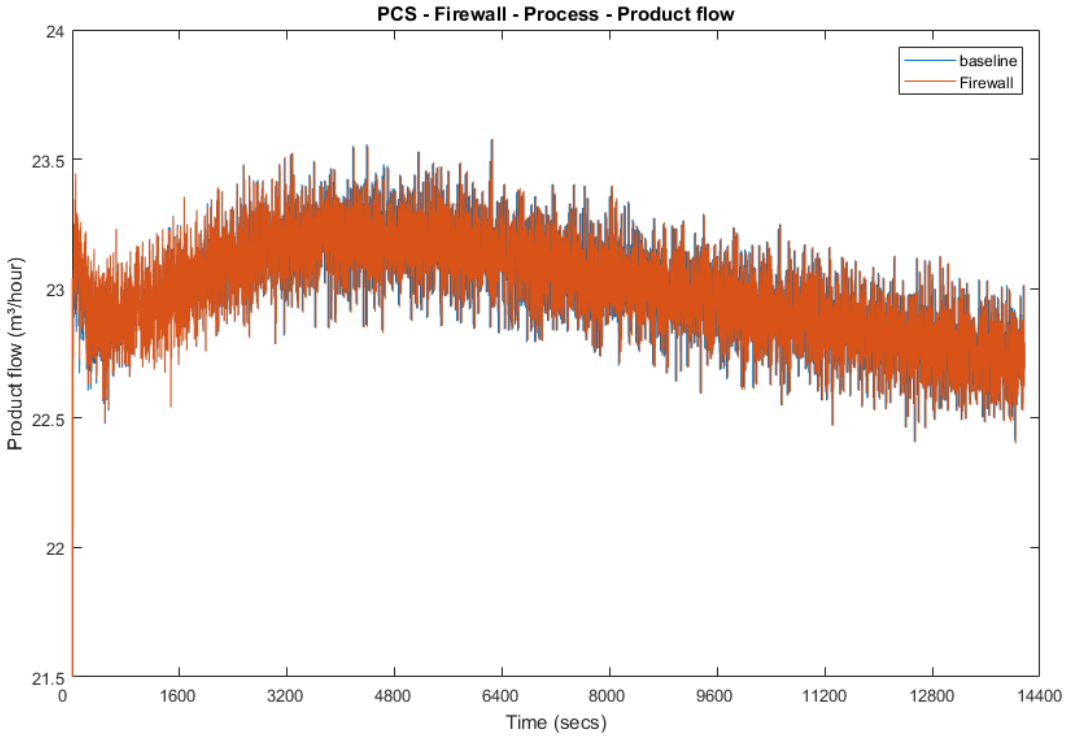
Figure 4-35 Packet round trip time from HMI to OPC before and after firewall rules were activated



5730

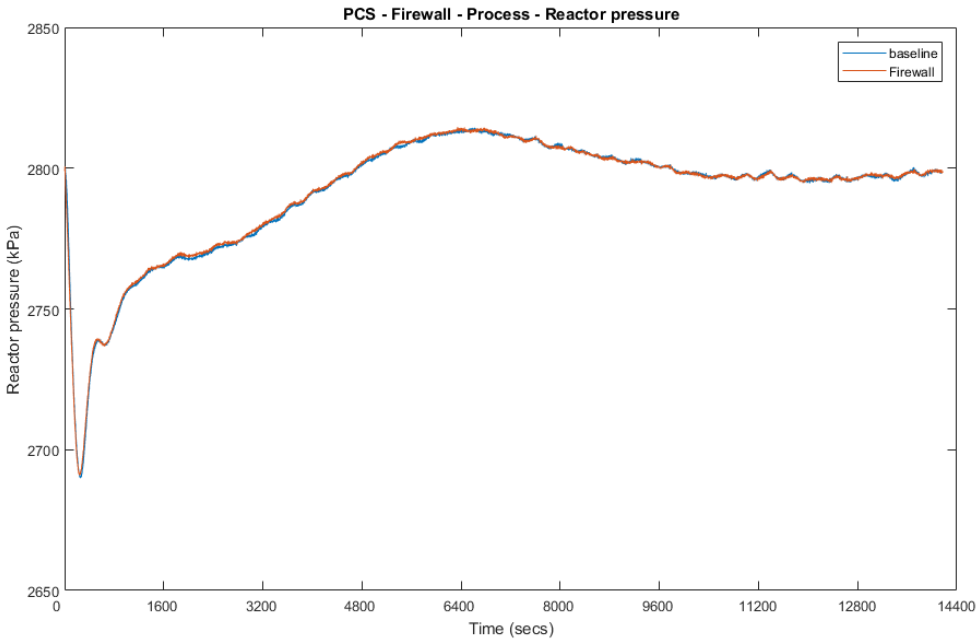
5731 **Figure 4-36 Packet round trip time from OPC to HMI before and after firewall rules were activated**

5732



5733

5734 **Figure 4-37 Manufacturing process product flow rate before and after firewall rules were activated**



5735

5736 **Figure 4-38 Manufacturing process reactor pressure before and after firewall rules were activated**

5737

5738 ### 4.19.7 Link to Entire Performance Measurement Data Set

5739 **Firewall KPI data**

5740 **Firewall measurement data**

5741

5742

4.20 Managed Network Interfaces

4.20.1 Technical Solution Overview

Managing network interfaces controls what network devices are plugged into switches within manufacturing system, along with physical labeling connections to help with system identification and classification. Required actions will be performed directly on the exterior of the switch. Switch port in use will be labeled logically within switch console itself, along with the corresponding network cable for easy identification. All cable should be labeled/identified at the switch and at the opposite end of the network cable. Switch Port Security should be configured to restrict access to only allowed preconfigured Media Access Control (MAC) addresses devices.

Minimal cost for labeling. Effort of implement is high, but not difficult. The effort will be spent taking the required time to accurately identify cabling connections.

Most switches have built in Port security. Since this technical control is built into switches there is no additional cost for implementation. Configuration for Port security is well documented and easily configured

4.20.2 Technical Capabilities Provided by Solution

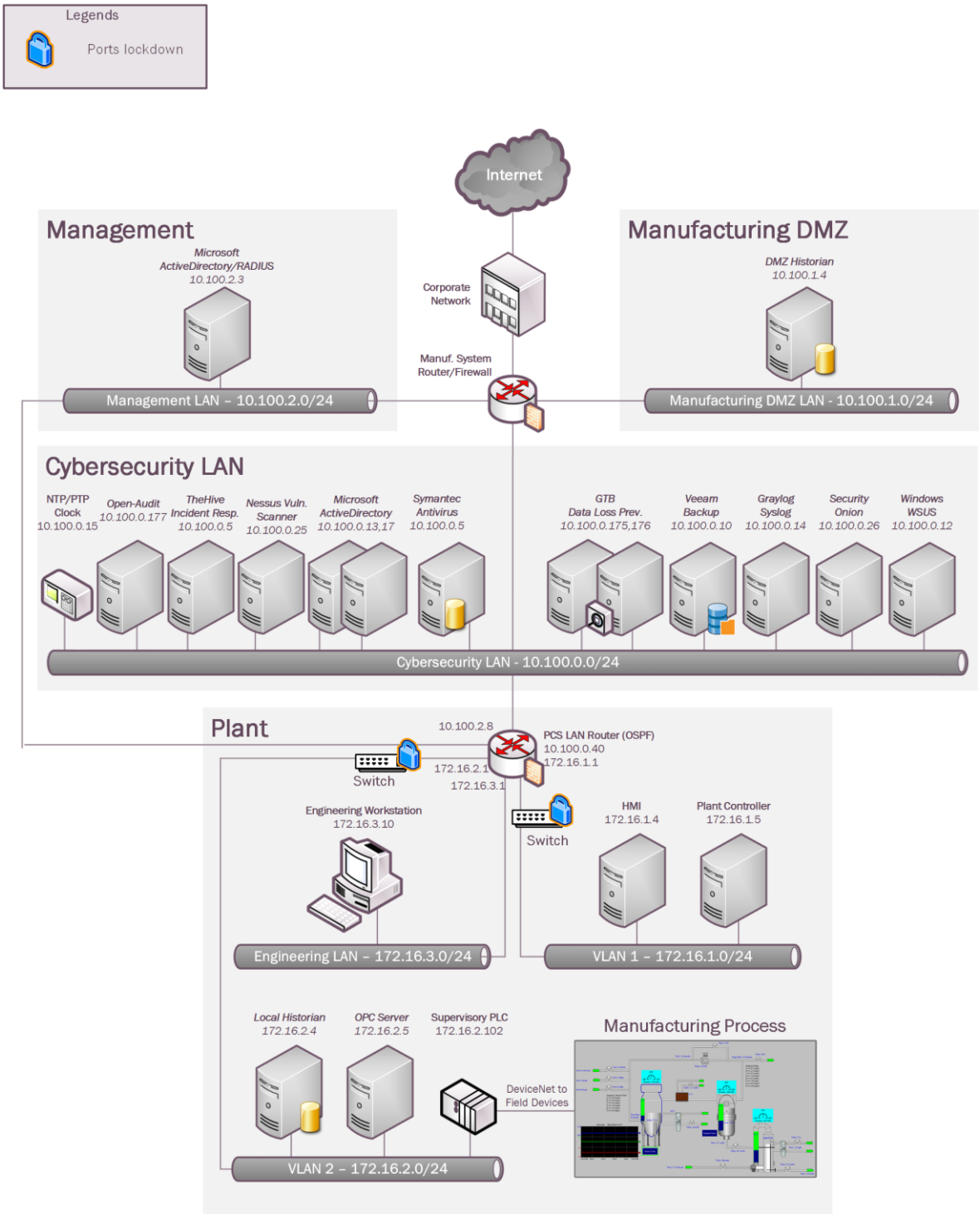
Managed Network Interfaces provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Managed Network Interfaces

4.20.3 Subcategories Addressed by Implementing Solution

PR.AC-5

4.20.4 Architecture Map of Where Solution was Implemented



4.20.5 Installation Instructions and Configurations

Managing Network Interface Instructions

Overview:

Port labeling provides ability for others to understand and know what network devices belong where. Managing your switches with correct labeling and classification makes troubleshooting simpler along with improving cybersecurity.

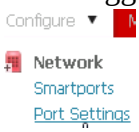
Labeling ports within switch:

Router/Switches within PCS: Allen-Bradley

Stratix 8300 (Router) 172.16.3.1

Stratix 5700 (Switch) Vlan1 172.16.1.3, Vlan2 172.16.2.2

- Login to switch/router via web browser. https://x.x.x.x
- Once logged in click on Configure→Port Settings



- Select port that will be labeled and click edit.
- A window will appear, now type into box next to Description and enter desired label. Description | Engg Workstation
- Click OK to save change and exit.

Same steps apply to Switches/Router within Process Control

Port Security Configuration for Process Control Enclave

Overview:

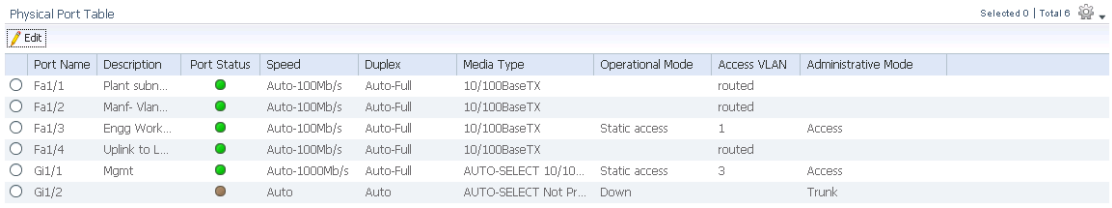
Port security prevents unauthorized devices from being plugged into a network switch while trying to obtaining sensitive information, which could be used for mapping out network connections for possible data exfiltration. When an unauthorized device is plugged into a protected port a warning message is logged and sent to a syslog server if supported by switch vendor.

Process Control Enclave:

- Enclave contains two different switches/routers.
  - Allen Bradley Router (8300)
  - Allen Bradley Switch (5700)

Allen Bradley Router 8300: Has multiple ports which are individual configurable depending on desired network topology.

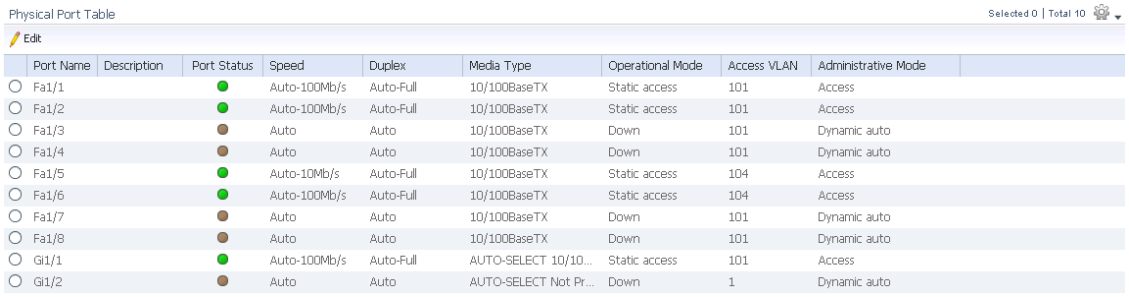
- Ports Fa1/1, Fa1/2, Fa1/3**(Port Security Enabled)**, Fa1/4, Gi1/1 = Enabled
- Port Gi1/2 = Disabled



- Enabling port security for connection are only allowed when configuring a switching port. If a port has been configured for routing port security cannot be enabled.

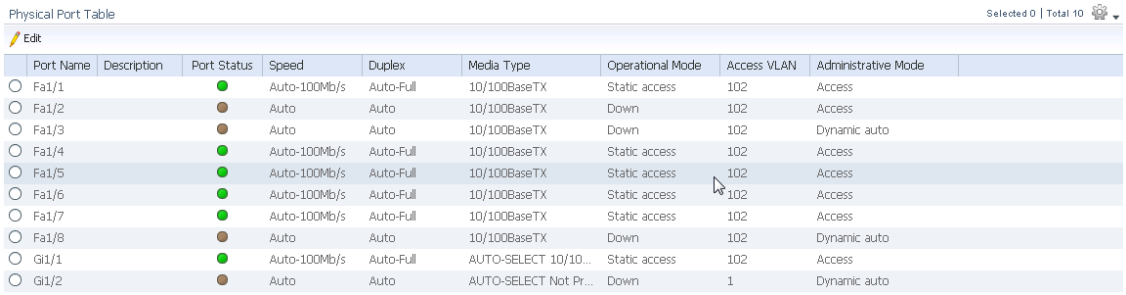
Allen Bradley 5700 (172.16.1.3): Layer 2 switch (Vlan1)

- Ports Fa1/1, Fa1/2, Fa1/5, Fa1/6, Gi1/1 are all configured for switching.
- Ports Fa1/3, Fa1/4, Fa1/7, Fa1/8, Gi1/2 are currently disabled.



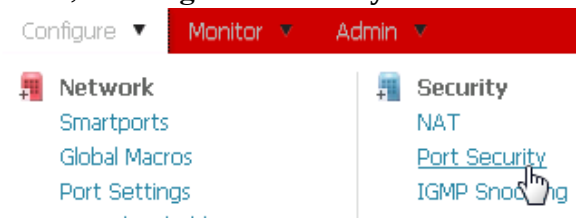
Allen Bradley 5700 (172.16.2.2): Layer 2 switch (Vlan2)

- Ports Fa1/1, Fa1/4, Fa1/5, Fa1/6, Fa1/7, Gi1/1 are all configured for switching.
- Ports Fa1/2, Fa1/3, Fa1/8, Gi1/2 are currently disabled.

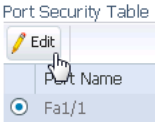


5815 **Enable Port Security (Allen Bradley 5700 and 8300, switch ports only)**

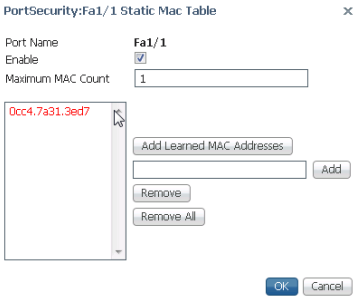
5816 • Login into Allen Bradley device via web browser.
5817 • Click, **"Configure→Security→Port Security"**



5818



5819 • Select desired port requiring security and click **"Edit"** button.
5820 • Place a check in box next to **"Enable"** and then click **"Add Learned MAC Addresses"**
5821 or add the Addresses manually.

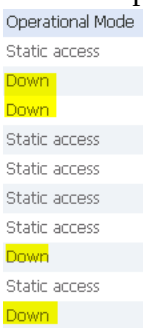


5822
5823 • Once MAC addresses have been added click **"OK"** to save changes.
5824 • If more than one MAC addresses are required to be added change **"Maximum MAC**
5825 **Count"** to the required MACs being assigned to this port.

5826

5827 **Disable unused ports**

5828 • While on the homepage select **"Configure→Port Settings"**
5829 • Find all Operational Mode labeled as down to identify ports being disabled.



5830
5831 • Now select on of the down ports and click on **"Edit"**
5832 • Once **"Edit Physical Port"** window appears remove check for enable from
5833 Administrative and click OK.

5834 • Port now is disabled. Any device plugged into this port or other disabled ports will not
5835 work.

5836 **Lessons Learned**

5837 • A Router don't allow Port Security via MAC on a routed port. This is because a routed
5838 port uses IP Address and not MAC Addresses.
5839 • When enabling Port Security turn on one port at a time to limit changes within the
5840 environment.

5841 Snippet from Allen Bradley Vlan1 Switch Running-Config File

```
interface FastEthernet1/1
 switchport access vlan 101
 switchport mode access
 switchport port-security mac-address 0cc4.7a31.3ed7
 switchport port-security
!
interface FastEthernet1/2
 switchport access vlan 101
 switchport mode access
 switchport port-security mac-address 0cc4.7a31.4447
 switchport port-security
!
interface FastEthernet1/3
 switchport access vlan 101
 shutdown
!
interface FastEthernet1/4
 switchport access vlan 101
 shutdown
!
interface FastEthernet1/5
 switchport access vlan 104
 switchport mode access
 switchport port-security mac-address 0cc4.7a32.b300
 switchport port-security
!
interface FastEthernet1/6
 switchport access vlan 104
 switchport mode access
 switchport port-security mac-address 001d.9cbf.78b3
 switchport port-security
!
interface FastEthernet1/7
 switchport access vlan 101
 shutdown
!
interface FastEthernet1/8
 switchport access vlan 101
 shutdown
!
```

5842

```
interface GigabitEthernet1/1
 switchport access vlan 101
 switchport mode access
 switchport port-security mac-address e490.693b.c2c6
 switchport port-security
!
interface GigabitEthernet1/2
 shutdown
interface FastEthernet1/1
 switchport access vlan 102
 switchport mode access
 switchport port-security mac-address 0cc4.7a32.b301
 switchport port-security
!
interface FastEthernet1/2
 switchport access vlan 102
 switchport mode access
 shutdown
!
interface FastEthernet1/3
 switchport access vlan 102
 shutdown
!
interface FastEthernet1/4
 switchport access vlan 102
 switchport mode access
 switchport port-security mac-address fcaa.147a.aa42
 switchport port-security
!
interface FastEthernet1/5
 switchport access vlan 102
 switchport mode access
 switchport port-security mac-address 001d.9cc9.6d42
 switchport port-security
!
interface FastEthernet1/6
 switchport access vlan 102
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address 0800.27ae.9958
 switchport port-security mac-address 0cc4.7a31.44bd
 switchport port-security
!
interface FastEthernet1/7
 switchport access vlan 102
 switchport mode access
 switchport port-security mac-address 0060.3520.c156
 switchport port-security
!
interface FastEthernet1/8
 switchport access vlan 102
 shutdown
```

5843

```
interface GigabitEthernet1/1
 switchport access vlan 102
 switchport mode access
 switchport port-security mac-address e490.693b.c2c7
 switchport port-security
!
interface GigabitEthernet1/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
```

Snippet from the Allen Bradley Boundary Router Running-Configuration file

```
interface FastEthernet1/3
 description Engg LAN Workstation
 switchport mode access
 switchport port-security mac-address 40a8.f03d.48ae
 switchport port-security
 ip access-group EnggWkstn-ACL in
```

4.20.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the managed network interfaces due to their implementation method (i.e., manually disable unused network interfaces in configuration).

4.20.7 Link to Entire Performance Measurement Data Set

N/A

4.21 Time Synchronization

4.21.1 Technical Solution Overview

Ability to have all devices sync from a reliable time source. Time synchronization is vital for system logins, event tracking and all other time sensitive events occurring with a manufacturing system.

No additional cost since services are included.

Ease of use simple

Effort and time required = minimal

4.21.2 Technical Capabilities Provided by Solution

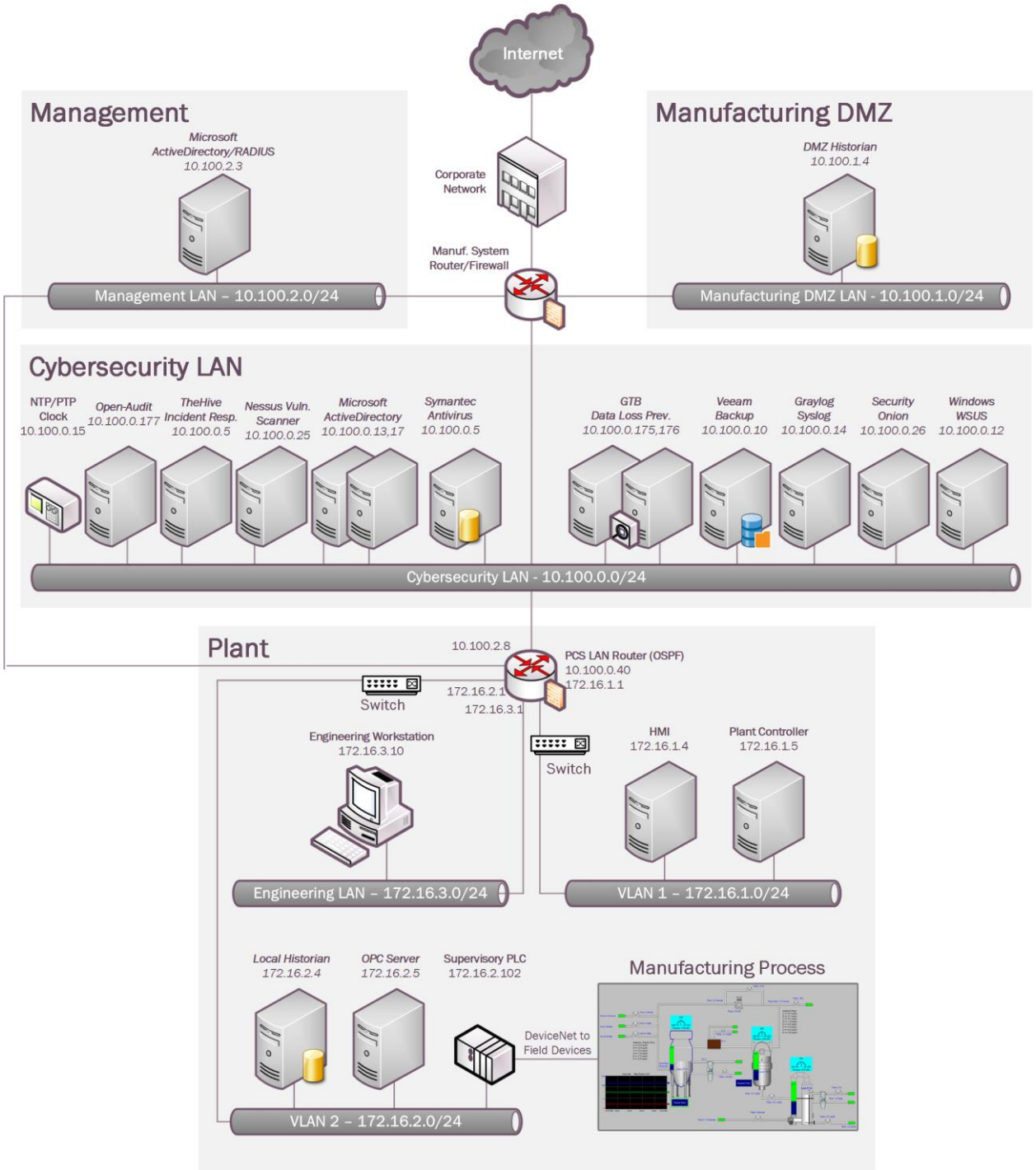
Time Synchronization provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Time Synchronization

4.21.3 Subcategories Addressed by Implementing Solution

PR.PT-1

4.21.4 Architecture Map of Where Solution was Implemented



4.21.5 Installation Instructions and Configurations

Details of the NTP server implemented:

Name	IP address	Purpose
Meinberg M9000 Lantime	10.100.0.15	NTP/PTP Clock

Computers:

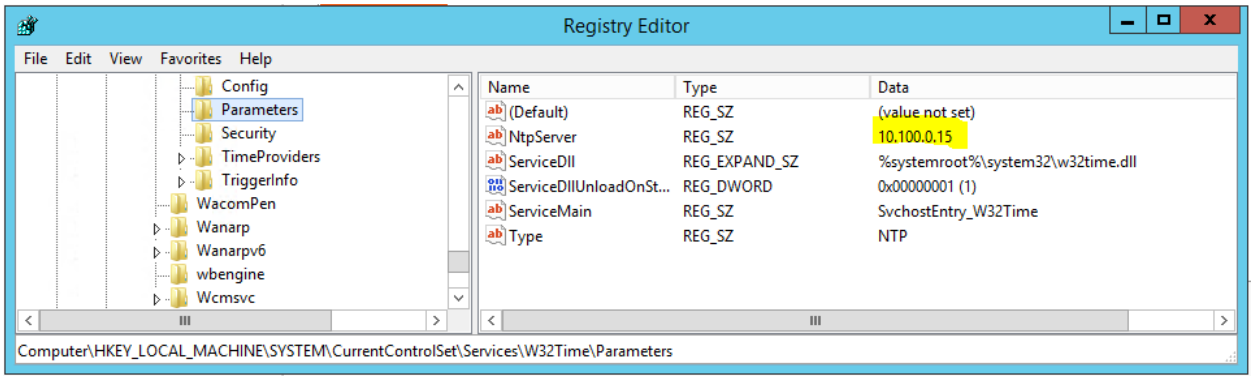
All windows computers within process control environment for Westman are joined to a domain. Domain joined machines automatically update their time by contacting local domain controller.

Domain Controller:

Domain controller obtains time from Meinberg Lantime M900 device. W32tm.exe is used to configure Windows Time service settings. Change the following registry key on the Domain Controller to have w32Time sync its time from an external source IP address.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\NtpServer

The image below shows our Domain Controller pointing to the IP address of Meinberg LAN Time clock



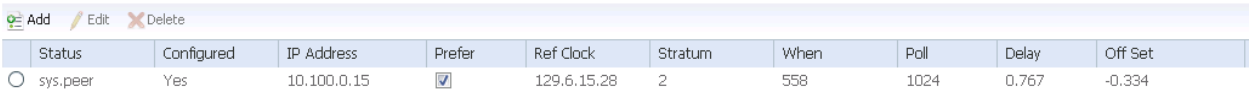
Other Devices:

All other devices within manufacturing system contact Meinberg Lantime M900 using NTP to sync time.

Allen Bradley Boundary Router:

- Login to the web UI by browsing to https://172.16.3.1
- Click on Configure →NTP

- Click Add button to add new time server.



- Save change
- Logout

Switches:

- Steps for switches **Vlan1 (172.16.1.3)** and **Vlan2 (172.16.2.2)** are the same as above.

Lesson Learned: The master time reference selected should be as close to your physical location as possible. This should reduce the Off Set.

4.21.6 Highlighted Performance Impacts

No performance measurement experiments were performed for time synchronization due to its installation in the system before the Manufacturing Profile implementation was initiated.

4.21.7 Link to Entire Performance Measurement Data Set

N/A

4.22 System Use Monitoring

4.22.1 Technical Solution Overview

System use monitor is accomplished by multiple tools to protect manufacturing system environment from harmful actives using data loss protection, auditing and syslog server for monitoring, store and auditing. Each tool provides a different level required to protect the manufacturing system.

Implementation effort is moderate requiring understand of Linux and Windows systems, along with virtual machine experience. Time required to install and configure all components 10 to 20 hours depending on skill level.

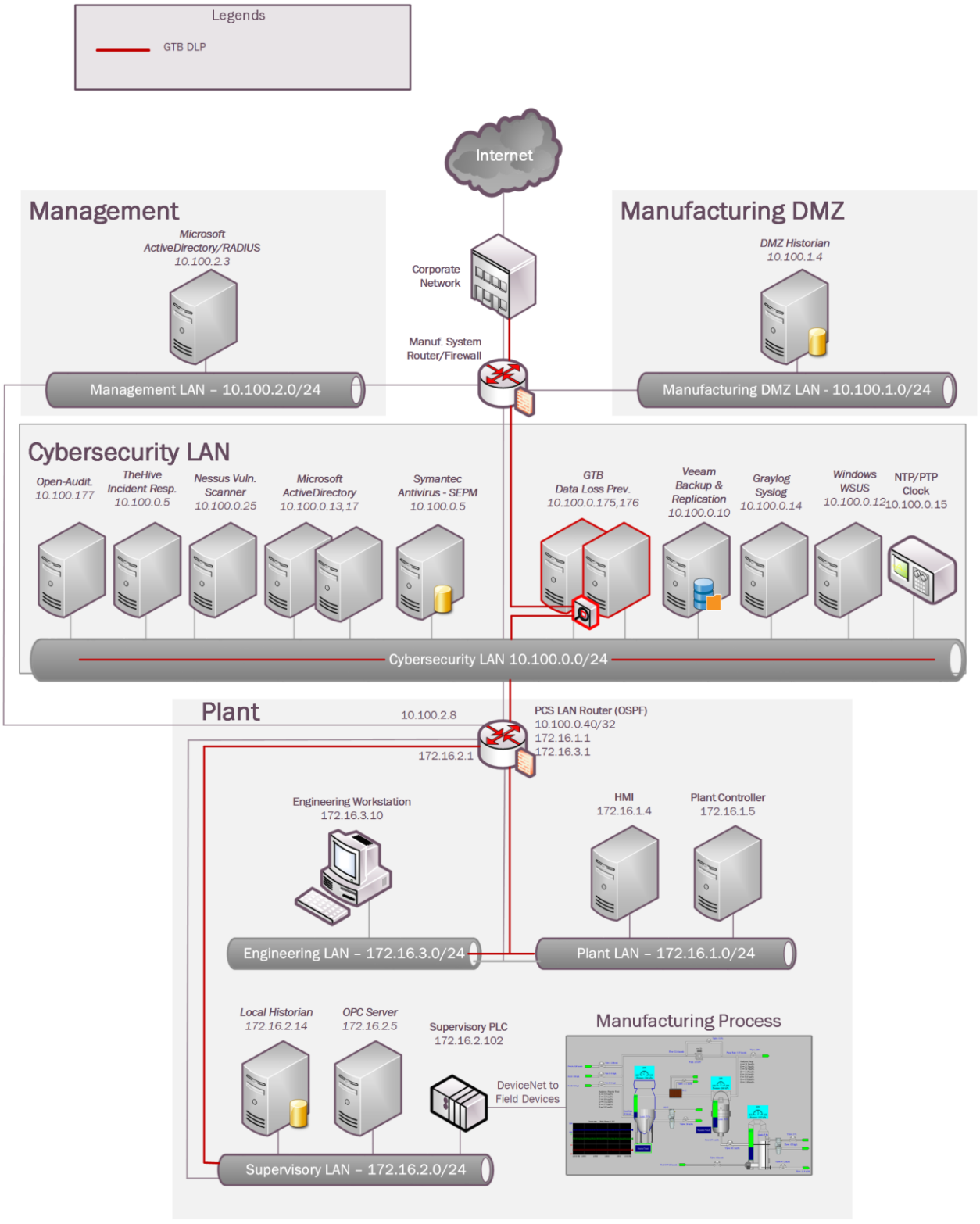
4.22.2 Technical Capabilities Provided by Solution

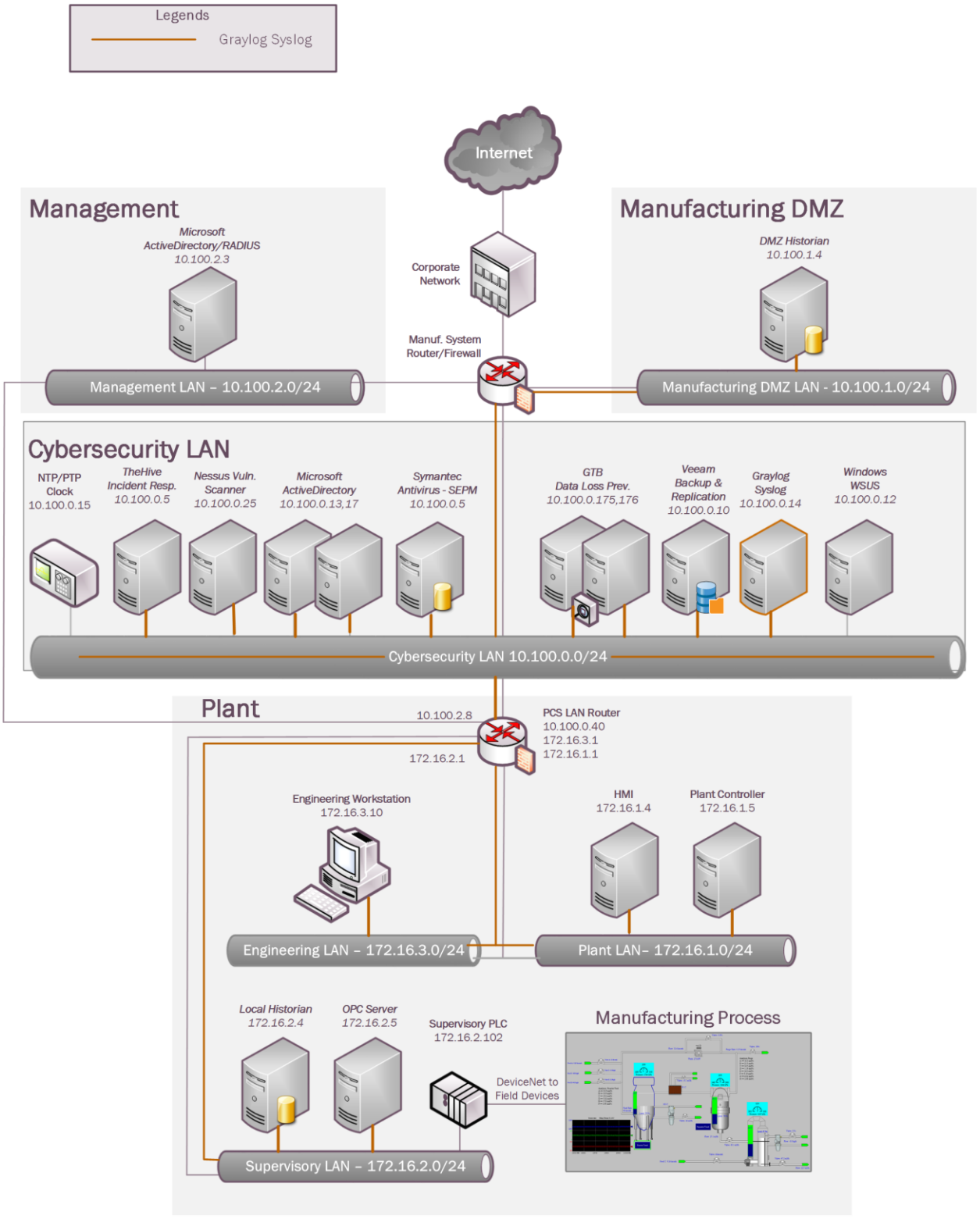
System Use Monitoring was provided by GTB Inspector, Ports and Services Lockdown, and Graylog.

4.22.3 Subcategories Addressed by Implementing Solution

PR.AC-1, PR.DS-5, PR.MA-2, DE.CM-3

4.22.4 Architecture Map of Where Solution was Implemented




Legends
Graylog Syslog
Internet
Management
Microsoft ActiveDirectory/RADIUS
10.100.2.3
Corporate Network
Manuf. System Router/Firewall
Management LAN – 10.100.2.0/24
Manufacturing DMZ
DMZ Historian
10.100.1.4
Manufacturing DMZ LAN - 10.100.1.0/24
Cybersecurity LAN
NTP/PTP Clock
10.100.0.15
TheHive Incident Resp.
10.100.0.5
Nessus Vuln. Scanner
10.100.0.25
Microsoft ActiveDirectory
10.100.0.13,17
Symantec Antivirus - SEPM
10.100.0.5
GTB Data Loss Prev.
10.100.0.175,176
Veeam Backup & Replication
10.100.0.10
Graylog Syslog
10.100.0.14
Windows WSUS
10.100.0.12
Cybersecurity LAN 10.100.0.0/24
Plant
10.100.2.8
PCS LAN Router
10.100.0.40
172.16.3.1
172.16.1.1
172.16.2.1
Engineering Workstation
172.16.3.10
HMI
172.16.1.4
Plant Controller
172.16.1.5
Engineering LAN – 172.16.3.0/24
Plant LAN– 172.16.1.0/24
Local Historian
172.16.2.4
OPC Server
172.16.2.5
Supervisory PLC
172.16.2.102
DeviceNet to Field Devices
Manufacturing Process
Supervisory LAN – 172.16.2.0/24

5925

5926

4.22.5 Installation Instructions and Configurations

System use monitoring was implemented using a combination of tools such as GTB Inspector, Graylog and native Windows Server Capabilities such as enabling Auditing, restricting administrative user accounts.

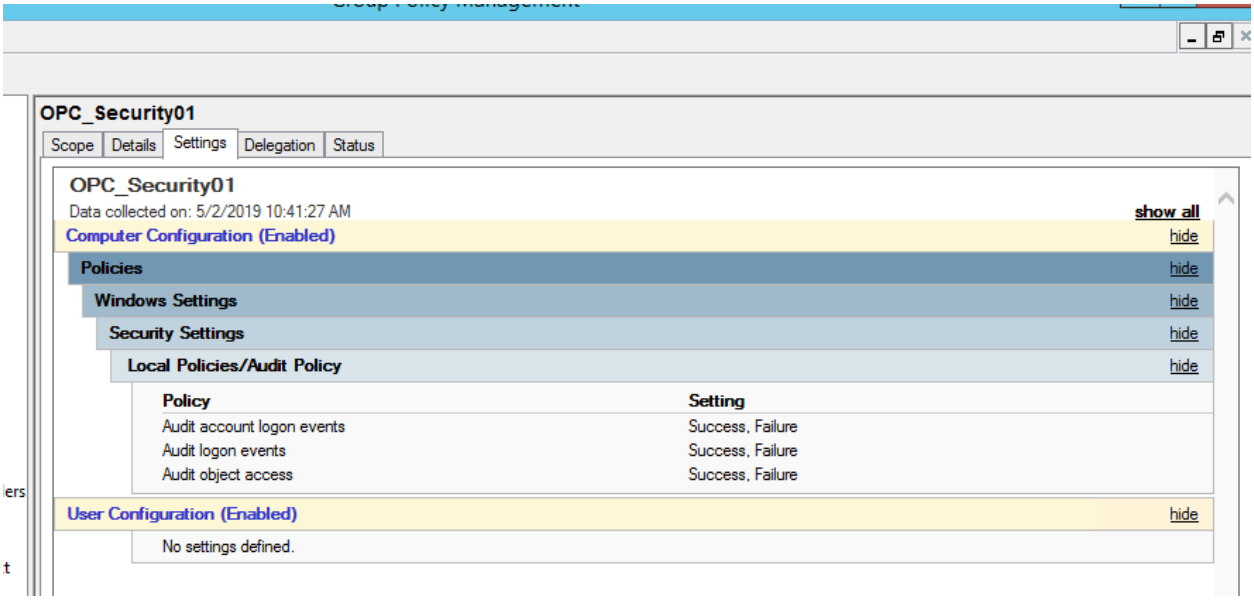
GTB DLP: See Section 4.15.5 for instructions.

Graylog: See Section 4.16.5 for instructions

Auditing Logon events:

Open Group Policy manager on domain controller.

Right click on Group Policy and select edit.



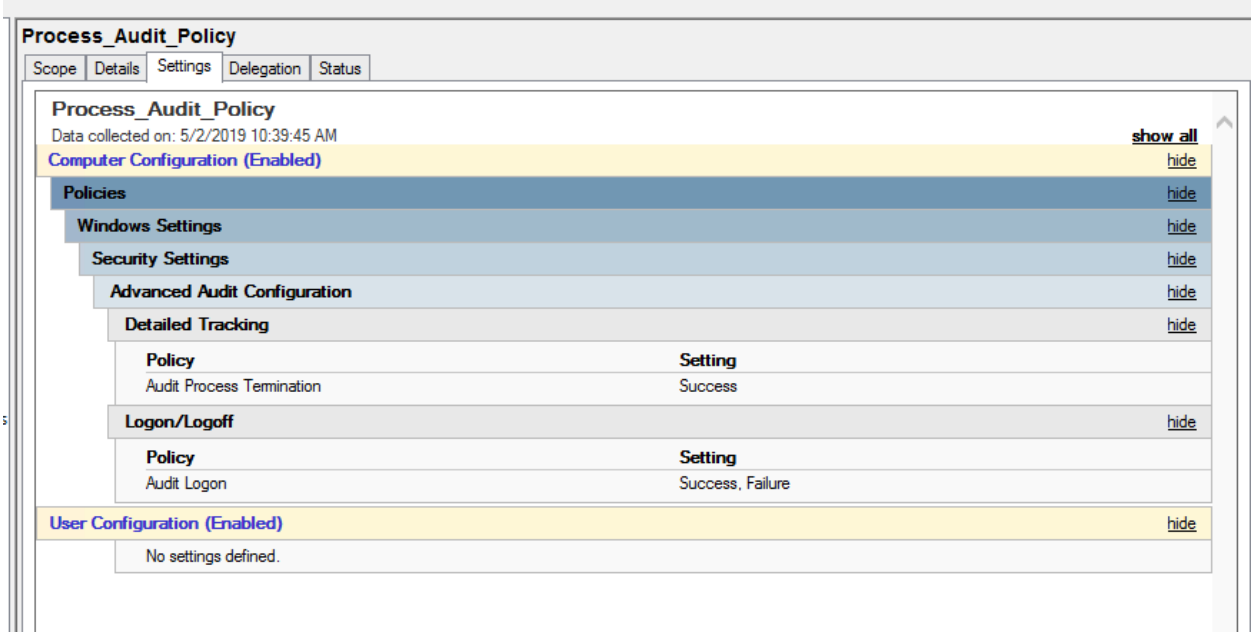
Navigate to Computer Configuration→Polices→Windows Settings→Security Settings→Local Polices→Audit Policy

Now change setting to reflect Success, Failure

Auditing Process Termination:

While in Group Policy manager navigate to Computer Configuration→Polices→Windows Settings→Security Settings→Advanced Audit Configuration→

Change Detailed Tracking and Logon/Logoff to Success / Success, Failure (See Image)



Restricting Administrative Users:

The local Administrators group on each system was reviewed and only those accounts that needed to have Administrative privileges on the system were added to this group.

For instance: An active directory user account "opc-admin" was created to run OPC-server services and was granted Administrative privileges on the below 2 servers:

- OPC Server
- Controller Server

Remote Access to PLC is only permitted through Engineering workstation.

4.22.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the installation of GTB into the PCS due to its location within the network topology. No manufacturing process components across the boundary on a regular basis while the system is operational.

No performance measurement experiments were performed for the use of the Graylog due to its typical installation and usage location (i.e., external to the manufacturing system).

4.22.7 Link to Entire Performance Measurement Data Set

N/A

4.23 Ports and Services Lockdown

4.23.1 Technical Solution Overview

Ports and services lockdown solutions enable a manufacturer to discover and disable nonessential logical network ports and services. A logical port is a number assigned to a "logical" connection. Port numbers are assigned to a service, which is helpful to TCP/IP in identifying what ports it must send traffic to. Hackers use port scanners and vulnerability scanners to identify open ports on servers. By revealing which ports are open, the hacker can identify what kind of services are running and the type of system. Closing down unnecessary ports by uninstalling un-necessary programs considerably reduces the attack surface. These actions need to be performed manually.

Native OS capabilities, Open-Audit and Nessus scanner were leveraged to inventory list of ports and applications currently running on each device of the plant.

4.23.2 Technical Capabilities Provided by Solution

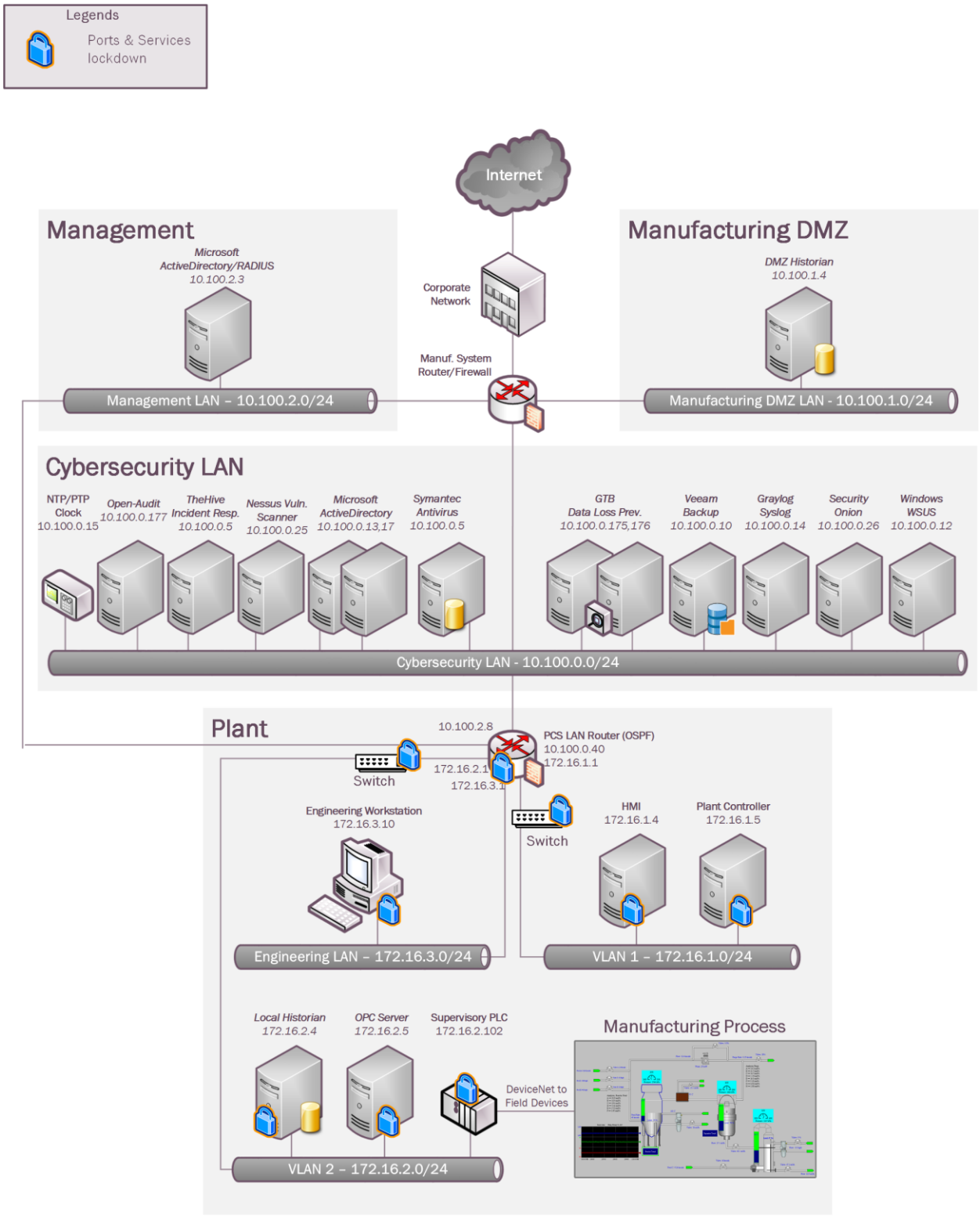
Ports and Services Lockdown provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Ports and Services Lockdown

4.23.3 Subcategories Addressed by Implementing Solution

PR.IP-1, PR.PT-3

4.23.4 Architecture Map of Where Solution was Implemented



4.23.5 Installation Instructions and Configurations

The following steps were performed on all Windows systems of the Plant

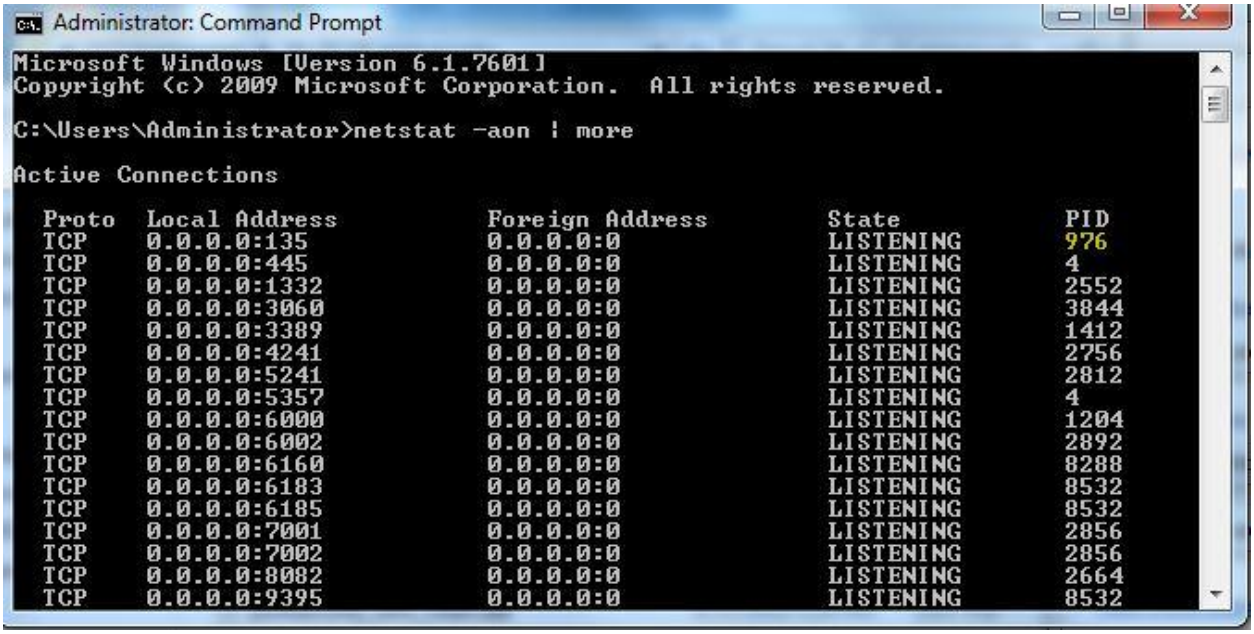
- Removal of Un-wanted programs
- Disable unsecure services

Removal of Un-wanted programs:

A software inventory of each system was performed using Open-Audit. The inventory reports were reviewed, and a list of unwanted programs were identified. These includes some software that's comes by default with the OS. These programs were then uninstalled.

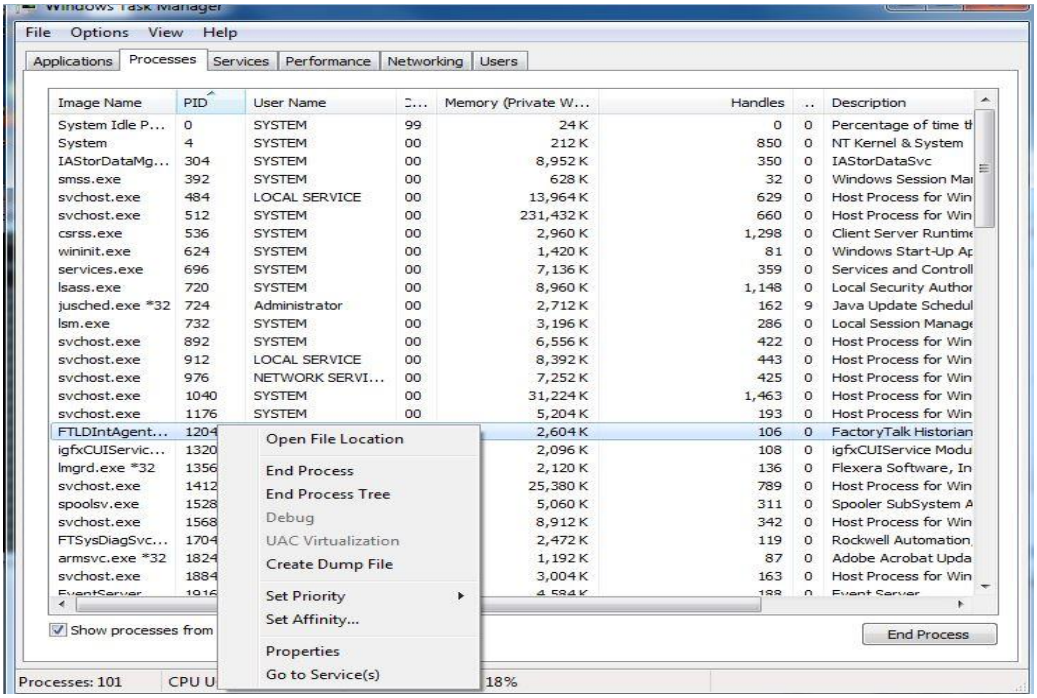
Netstat utility was used to gather information about which applications are running or using which TCP/IP ports on each system

For instance: `netstat -aon | more` will generate a list of processes, PID



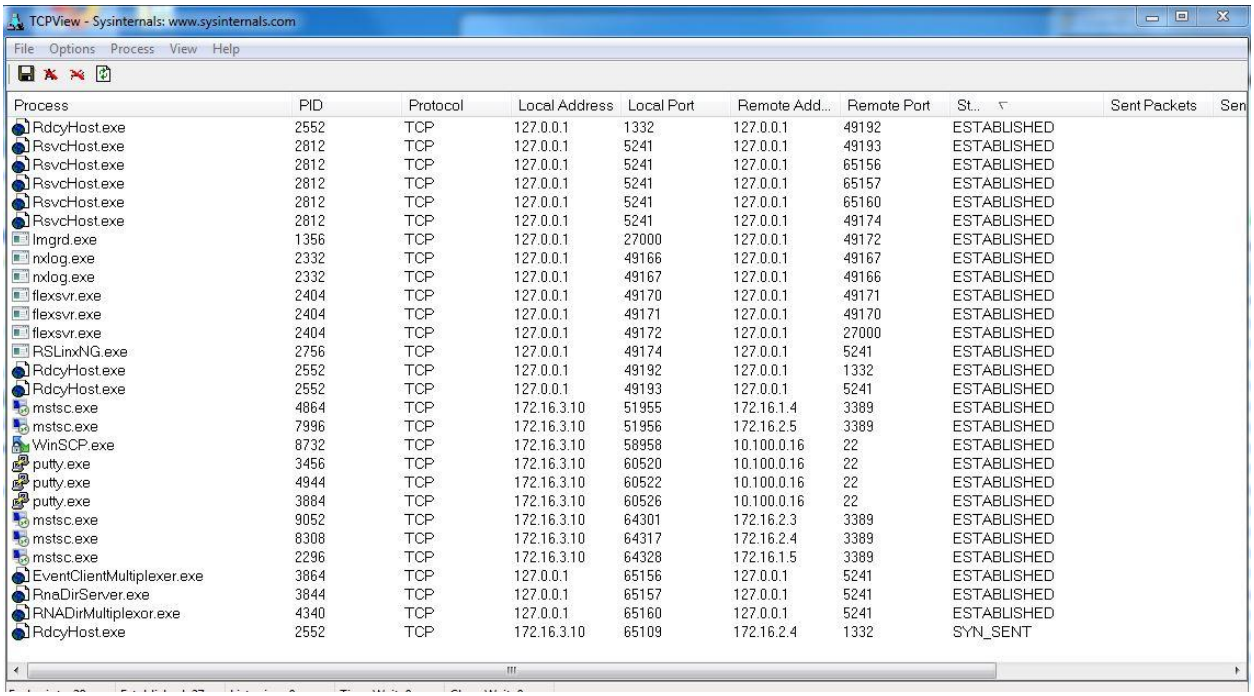
The PID from the above output can be used with Windows Task Manager for further analysis. Within Task Manager (Windows 7), enable the PID column by clicking on **View** >> **Select Columns**.

Next, you might have to use the option to Show Processes for All Users, and then you'll be able to find the PID in the list. Once you're there, you can use the End Process, Open File Location, or Go to Service(s) options to control the process or stop it.



Other alternatives are using **Resource Monitor** (resmon.exe) and **TCPView** from SysInternals [1].

TCPView:



The following steps were performed on all network devices of the Plant

- Disabling unsecure services such as Telnet, SNMP (1 and 2)
- If SNMP is required, change the default community string
- Setting a password for enable

  Cisco commands to set a password for enable:

```
router1(config)# enable
router1(config)# configure terminal
router1(config)# enable secret <password>
```

- Restrict ssh access to select machines.

  Cisco commands to restrict access [2]:

```
router1(config)# enable
router1(config)# configure terminal
router1(config)# access-list 1 permit 172.16.0.0 0.0.255.255
router1(config)# line vty 0 15
router1(config-line)# access-class 1 in
```

The following steps were performed on the PLC

- Disabled unsecure services such as Telnet, SNMP and HTTP
- Remote Access to the PLC was permitted only through the Engineering Workstation.

4.23.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the managed network interfaces due to their implementation method (i.e., manually disabled network ports and removed unwanted Windows programs and services).

4.23.7 Link to Entire Performance Measurement Data Set

N/A

4.24 Media Protection

4.24.1 Technical Solution Overview

Port locks provide a low-cost solution for protecting USB ports. Implementation and ease of use provide for quick install and easy removal. USB Port locks provide a simple yet effective solution to restrict USB use. Once USB Port lock has been inserted and engaged there is no way of removing lock device without damaging USB port unless key is used. Each USB Port lock can block up to two ports. These ports are the inserted port, and the port directly to either side depending on the blocking plate direction. USB Port Lock can be purchased with a collar that protects attached USB Mice and Keyboards from removal without prior approval.

4.24.2 Technical Capabilities Provided by Solution

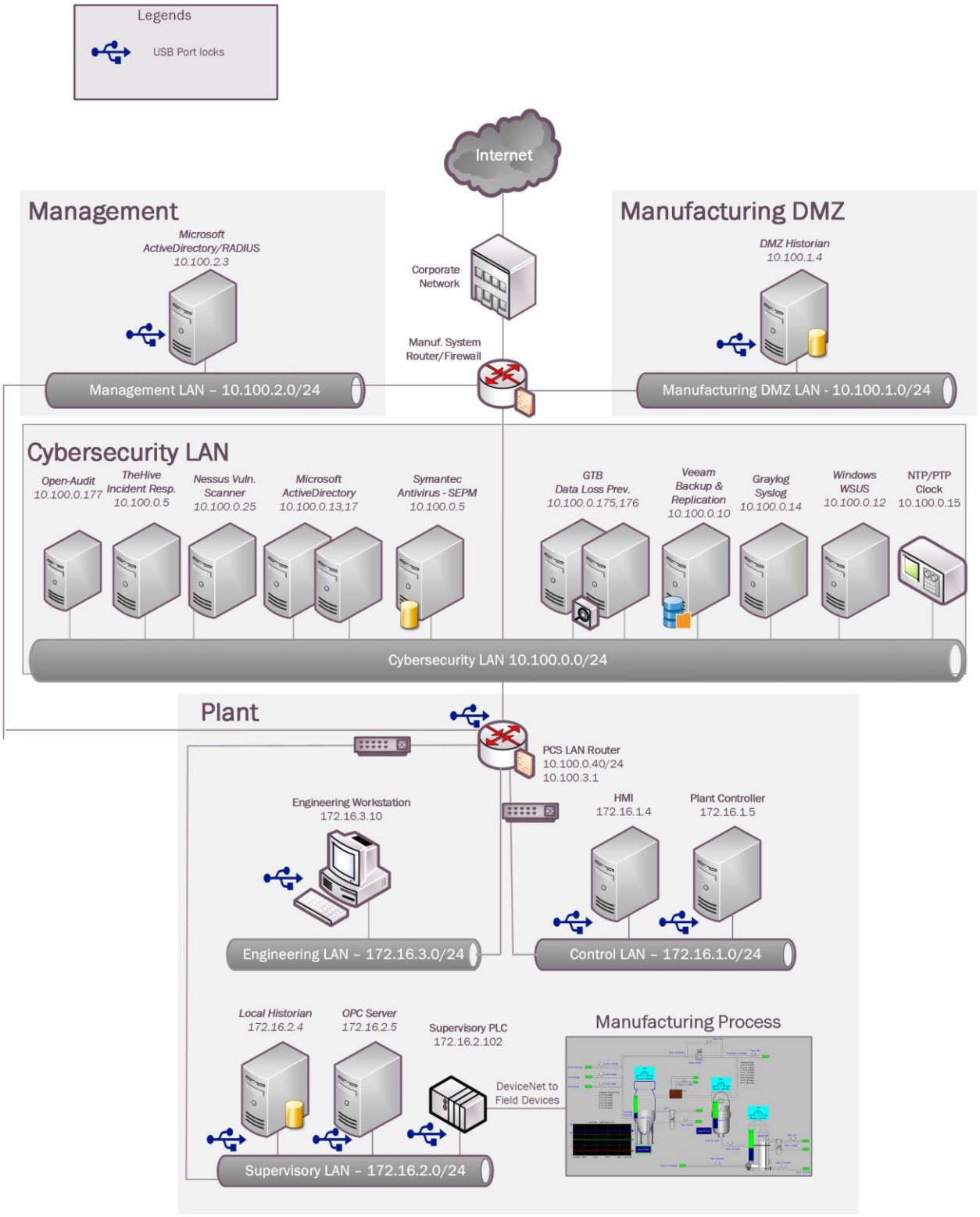
Media Protection provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Media Protection

4.24.3 Subcategories Addressed by Implementation

PR.PT-2

4.24.4 Architecture Map of Where Solution was Implemented



4.24.5 Installation Instructions and Configurations

- **Products / Tools found to meet capability:**
  - Kensington USB Port Locks
  - Symantec Endpoint Protection (USB Policy Enforcement)
  - Group Policy Management (GPO) Active Directory
- **Product / Tools selected to be implemented in testbed:**
  - Kensington USB Port Locks (Protects Linux Machines)
  - Symantec Endpoint Protection (USB Policy Enforcement - Protects Windows Machines)
  - Group Policy (GPO) Active Directory (Protects Windows Machines)
- **Products Overview:**
  - USB Port locks from Kensington provide an alternative for small manufactures that don't have the resources or primarily run Linux machines within their environment to have a solution that protections from rogue USB devices being used without approval.
    - **Pros:** Quick solution, Hardware only solution, inexpensive
    - **Cons:** Feels like having to force device into USB Port first few times

Insert USB Port lock then push locking button in to secure. Kensington provides inserts to block multiple ports including locks designed for securing USB Keyboards and Mice.

Lessons learned:

Patience is required when using this product so as not to inadvertently damage USB port

4.24.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the USB port locks due to their implementation method (i.e., physically restricting access to USB ports).

4.24.7 Link to Entire Performance Measurement Data Set

N/A

Appendix A - Acronyms and Abbreviations

Selected acronyms and abbreviations used in this document are defined below.

CSF	Cybersecurity Framework
FIPS	Federal Information Processing Standards
HMI	Human Machine Interface
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ISA	The International Society of Automation
IT	Information Technology
LAN	Local Area Network
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OT	Operational Technology
PLC	Programmable Logic Controller
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network

Appendix B - Glossary

Selected terms used in in this document are defined below.

Business/Mission Objectives - Broad expression of business goals. Specified target outcome for business operations.

Capacity Planning - Systematic determination of resource requirements for the projected output, over a specific period. [businessdictionary.com]

Category - The subdivision of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities.

Critical Infrastructure - Essential services and related assets that underpin American society and serve as the backbone of the nation's economy, security, and health. [DHS]

Criticality Reviews - A determination of the ranking and priority of manufacturing system components, services, processes, and inputs in order to establish operational thresholds and recovery objectives.

Critical Services - The subset of mission essential services required to conduct manufacturing operations. Function or capability that is required to maintain health, safety, the environment and availability for the equipment under control. [62443]

Cyber Risk - Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system.

Cybersecurity - The process of protecting information by preventing, detecting, and responding to attacks. [CSF]

Defense-in-depth - The application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another. [62443 1-1]

Event - Any observable occurrence on a manufacturing system. Events can include cybersecurity changes that may have an impact on manufacturing operations (including mission, capabilities, or reputation). [CSF]

Firmware - Software program or set of instructions programmed on the flash ROM of a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware. [Techterms.com]

Framework - The Cybersecurity Framework developed for defining protection of critical infrastructure. It provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. Includes activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes.

Function - Primary unit within the Cybersecurity Framework. Exhibits basic cybersecurity activities at their highest level.

Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [CSF]

Integrator - A value-added engineering organization that focuses on industrial control and information systems, manufacturing execution systems, and plant automation, that has application knowledge and technical expertise, and provides an integrated solution to an engineering problem. This solution includes final project engineering, documentation, procurement of hardware, development of custom software, installation, testing, and commissioning. [CSIA.com]

Manufacturing Operations - Activities concerning the facility operation, system processes, materials input/output, maintenance, supply and distribution, health, and safety, emergency response, human resources, security, information technology and other contributing measures to the manufacturing enterprise.

Network Access - any access across a network connection in lieu of local access (i.e., user being physically present at the device).

Operational technology - Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. [Gartner.com]

Programmable Logic Controller - A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing. [800-82]

Profile - A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories. [CSF]

- Target Profile - the desired outcome or 'to be' state of cybersecurity implementation
- Current Profile – the 'as is' state of system cybersecurity

Protocol - A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. [800-82]

Remote Access - Access by users (or information systems) communicating external to an information system security perimeter. Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). [800-53]

Resilience Requirements - The business-driven availability and reliability characteristics for the manufacturing system that specify recovery tolerances from disruptions and major incidents.

Risk Assessment - The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis. Incorporates threat and vulnerability analyses. [800-82]

Risk Tolerance - The level of risk that the Manufacturer is willing to accept in pursuit of strategic goals and objectives. [800-53]

Router - A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network. The most common form of router operates on IP packets. [800-82]

Security Control - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system, its components, processes, and data. [800-82]

Subcategory - The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated." [CSF]

Supporting Services - Providers of external system services to the manufacturer through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. Supporting services include, for example, Telecommunications, engineering services, power, water, software, tech support, and security. [800-53]

Switch - A device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination. [Whatis.com]

System Categorization - The characterization of a manufacturing system, its components, and operations, based on an assessment of the potential impact that a loss of availability, integrity, or confidentiality would have on organizational operations, organizational assets, or individuals. [FIPS 199]

6230 **Third-Party Relationships** - relationships with external entities. External entities may include,
6231 for example, service providers, vendors, supply-side partners, demand-side partners, alliances,
6232 consortiums, and investors, and may include both contractual and non-contractual parties.
6233 [DHS]

6234 **Third-party Providers -** Service providers, integrators, vendors, telecommunications, and
6235 infrastructure support that are external to the organization that operates the manufacturing
6236 system.
6237
6238 **Thresholds -** Values used to establish concrete decision points and operational control limits to
6239 trigger management action and response escalation.

Appendix C - References

1. Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013. https://www.govinfo.gov/app/details/FR-2013-02-19/2013-03915

2. National Institute of Standards and Technology (2014) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), February 12, 2014. https://doi.org/10.6028/NIST.CSWP.02122014

3. Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. https://doi.org/10.6028/NIST.SP.800-82r2

4. Stouffer K, Zimmerman T, Tang CY, Lubell J, Cichonski J, McCarthy J (2017) Cybersecurity Framework Manufacturing Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 8183, Includes updates as of May 20, 2019. https://doi.org/10.6028/NIST.IR.8183