CONFIDENTIAL

TROJAN BRICKS SECURITY

CYBER SYSTEM SECURITY PLAN

Approvals

_____

Lola Wolfe, CEO

Table of Contents

1. System Description

1.1. System Attributes

System Name	*Trojan Bricks Security*
Impact Categorization	Confidentiality|HIGH|Integrity|MED|Availability|LOW
System Owner	*Jon Brown, COO, Trojan Bricks, Inc,* *15 John Street, Little Rock,* *jon@trojan.com, (501)503-1111*
Security Manager	*Lola Wolfe, CEO, Trojan Bricks, Inc,* *72 Mary Street, Little Rock,* *lola@trojan.com, (501)503-9999*
Primary System Administrator(s)	
Primary System Users	

1.2. System Description and Mission

This is the general support system for the Trojan Bricks, Inc. The aim of the system is to support the staff in their tasks and allow them to achieve the company's goals set by the management.

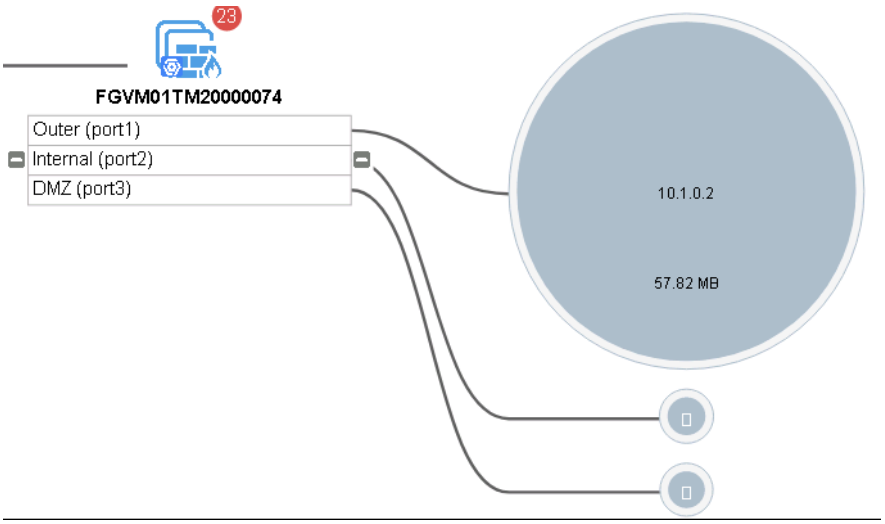
1.3. Security Requirements

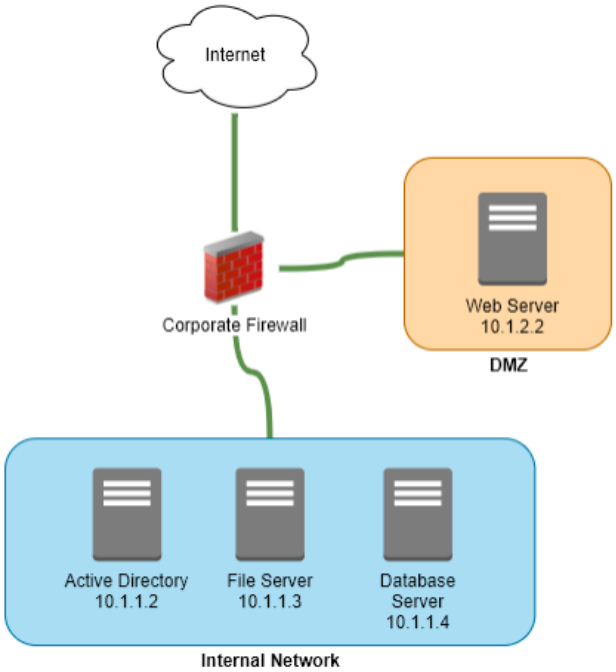
Requirement	Impact	Description
Confidentiality	High	Each segment of the information system is divided by the access privileges that have been given to different members of the organization depending on their hierarchy in their in the organization and the roles assigned to them. The roles vary according to their respective departments they belong to. Care has been given so that there is no access provided that undermines this division. Access control policies prevent unauthorized access of assets by users that don't have requisite roles for the system they are trying to access.
Integrity	Med	Threats that may arise are in the form of competitors trying to corrupt the company's database that may hold their marketing and design information. The security protocols must be design to safegaurd the company systems from such attacks.
Availability	Low	Availability is of a lower concern for the organization as it does not provide a consumer interface. Even if the organization's access to its data is delayed, it still would not not affect the organization to a very high degree once the systems have been restored

1.4. System Environment

The system comprises a single Internet facing web server from which all marketing and purchases take place. The web server has a back end mysql database (i.e. Database Server). An Active Directory server is used to manage all employee and contractor accounts, and a file server exists for sharing documents throughout the company.

1.5. Network Diagrams





1.6. Dependencies and Interconnections

The system consists of an internal server, a file server(Sweaty), a database server and a Web server. The system is separated from the internet via a firewall that splits the entire network into three regions:

The internal :that has all the protected information.

The DMZ: the web server that is kept separate from the protected information.

The outside: the internet.

2. Plan of Action and Milestones

Use this section to specify a plan of action to address unmet or partially met security control objectives or to track vulnerability mitigation.

POAM ID	***Security Control/Issue***	***Plan of Action***	***Responsible***	***Milestone Date***

3. Security Controls

3.1. AC: Access Control

3.1.1. AC-2: Account Management

Requirement:	The system owner identifies and selects the following types of information system accounts to support organizational missions/business functions: • User • Shared • Groups{Executive, Engineering, Accounting, Marketing, HR, Senior, Contractor, ITWorks, Evolution, TomHandC} • Administrator • Owner
Control Reference:	NIST 800-53 (Rev. 4) AC-2(a)
Last Review and Update:	May 6 2020

Implementation:

The system owner creates all the required groups to reflect the organization and creates separate roles for all employees to limit their privileges.

Requirement:	The system owner establishes conditions for group and role membership.
Control Reference:	NIST 800-53 (Rev. 4) AC-2(c)
Last Review and Update:	May 6 2020

Implementation:

The system owner assigns membership to various employees based on their job description and role in the organization.

A single individual may be assigned to multiple groups. This may relate to their position in the hierarchy and their respective department.

All individuals will have a single user account that is unique to them.

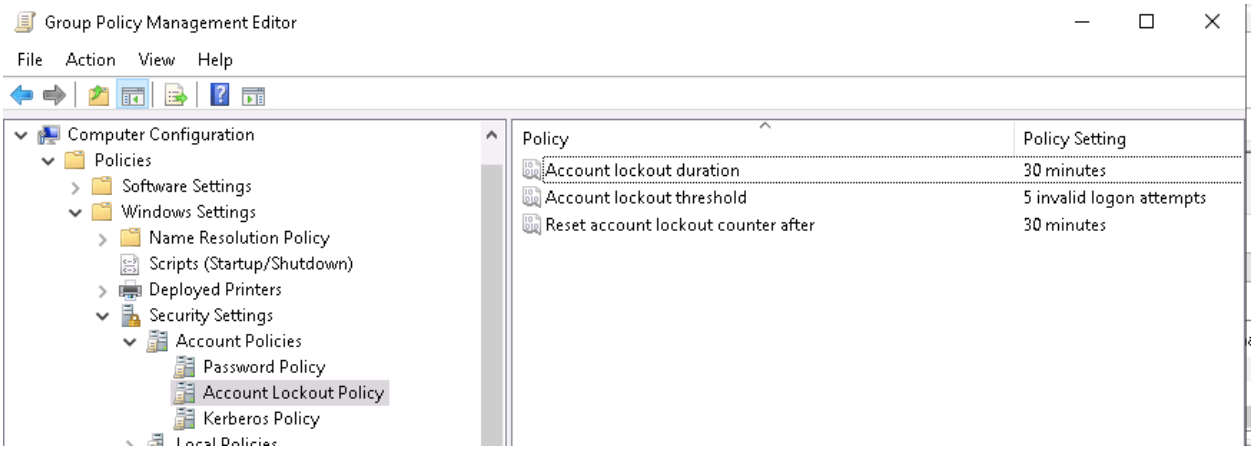
The administrator will have system privileges related to configuration.

The system owner will have the highest privileges and is responsible for all data within the organization.

3.1.2. AC-7: Unsuccessful Login

Requirement:	The system owner enforces a limit of 5 consecutive invalid logon attempts by a user after which the account is locked for 30 minutes.
Control Reference:	NIST 800-53 (Rev. 4) AC-7(a),(b)
Last Review and Update:	May 6 2020

Implementation:



3.2. AU: Audit and Accountability

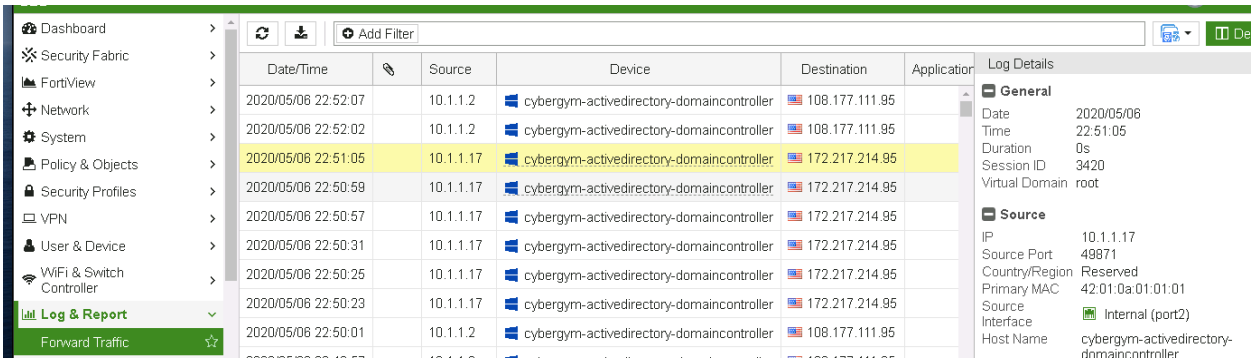
3.2.1. AU-2: Audit Events

Requirement:	• The system owner determines that the information system is capable of auditing the following events:
	  • Login
	  • Privilege changes
	• The system owner coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.

Control Reference:	NIST 800-53 (Rev. 4) AU-2(a),(b)
Last Review and Update:	May 6 2020

Implementation:

For the firewall, the log can be accessed through the Log & Report menu in the sidebar:



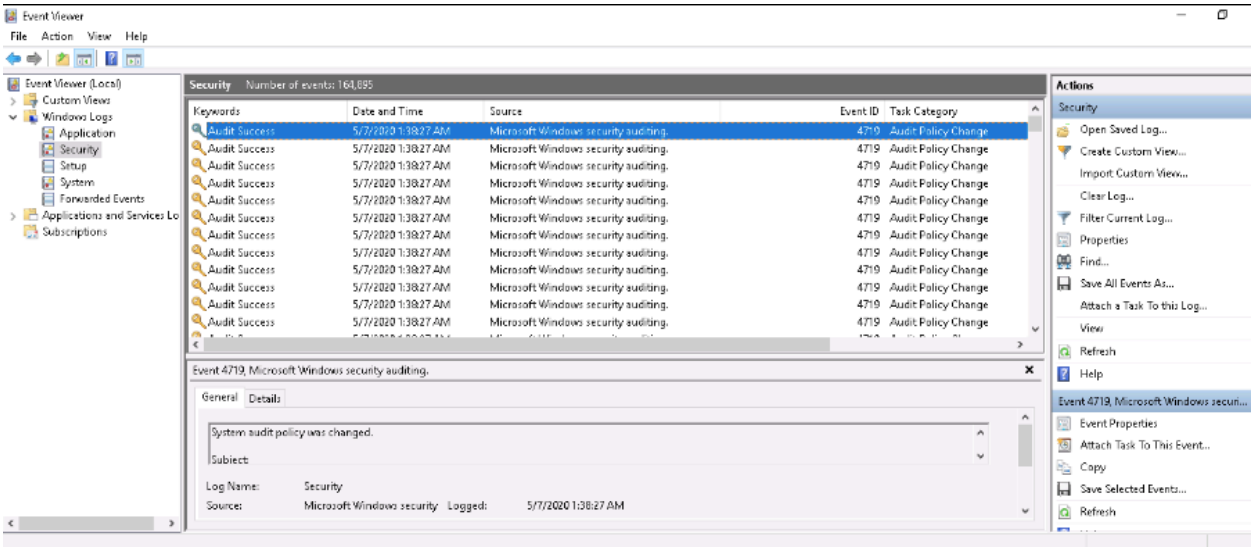
For the CentOS web server, the logs can be accessed in audit folder in the log directory:

```
boot  etc  lib   media  opt  root  sbin  sys  usr
[gymboss@jhdkjj-cybergym-teenyweb /]$ ls var/log
audit                 cron-20200310        maillog-20200413    secure-20200421
boot.log              cron-20200413        maillog-20200421    secure-20200506
boot.log-20200302     cron-20200421        maillog-20200506    spooler
boot.log-20200303     cron-20200506        messages            spooler-20200310
boot.log-20200310     dmesg                messages-20200310   spooler-20200413
boot.log-20200316     dmesg.old            messages-20200413   spooler-20200421
boot.log-20200413     firewalld            messages-20200421   spooler-20200506
boot.log-20200421     grubby               messages-20200506   tallylog
boot.log-20200506     grubby_prune_debug   ntpstats            tuned
btmp                  httpd                qemu-ga             wtmp
btmp-20200506         lastlog              secure              yum.log
chrony                maillog              secure-20200310
cron                  maillog-20200310     secure-20200413
[gymboss@jhdkjj-cybergym-teenyweb /]$
```

Command line tools can be used to parse through the logs and get meaningful insights:

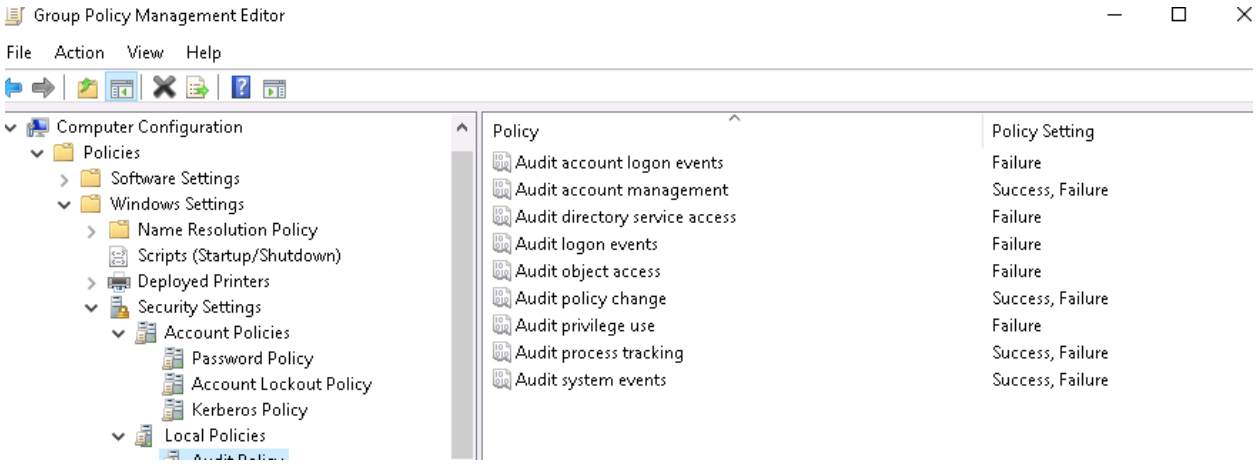

```
boot  etc  lib   media  opt  root  sbin  sys  usr
[gymboss@jhdkjj-cybergym-teenyweb /]$ ls var/log
audit                 cron-20200310        maillog-20200413    secure-20200421
boot.log              cron-20200413        maillog-20200421    secure-20200506
boot.log-20200302     cron-20200421        maillog-20200506    spooler
boot.log-20200303     cron-20200506        messages            spooler-20200310
boot.log-20200310     dmesg                messages-20200310   spooler-20200413
boot.log-20200316     dmesg.old            messages-20200413   spooler-20200421
boot.log-20200413     firewalld            messages-20200421   spooler-20200506
boot.log-20200421     grubby               messages-20200506   tallylog
boot.log-20200506     grubby_prune_debug   ntpstats            tuned
btmp                  httpd                qemu-ga             wtmp
btmp-20200506         lastlog              secure              yum.log
chrony                maillog              secure-20200310
cron                  maillog-20200310     secure-20200413
[gymboss@jhdkjj-cybergym-teenyweb /]$
```

Event Viewer can be used to access the logs in the base Windows server:



Requirement:	Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents. The system owner determines that the following events are to be audited within the information system: • login/logoff access log • File access log • Networking log • System services start/stop
Control Reference:	NIST 800-53 (Rev. 4) AU-2(c),(d)
Last Review and Update:	May 6 2020

Implementation:



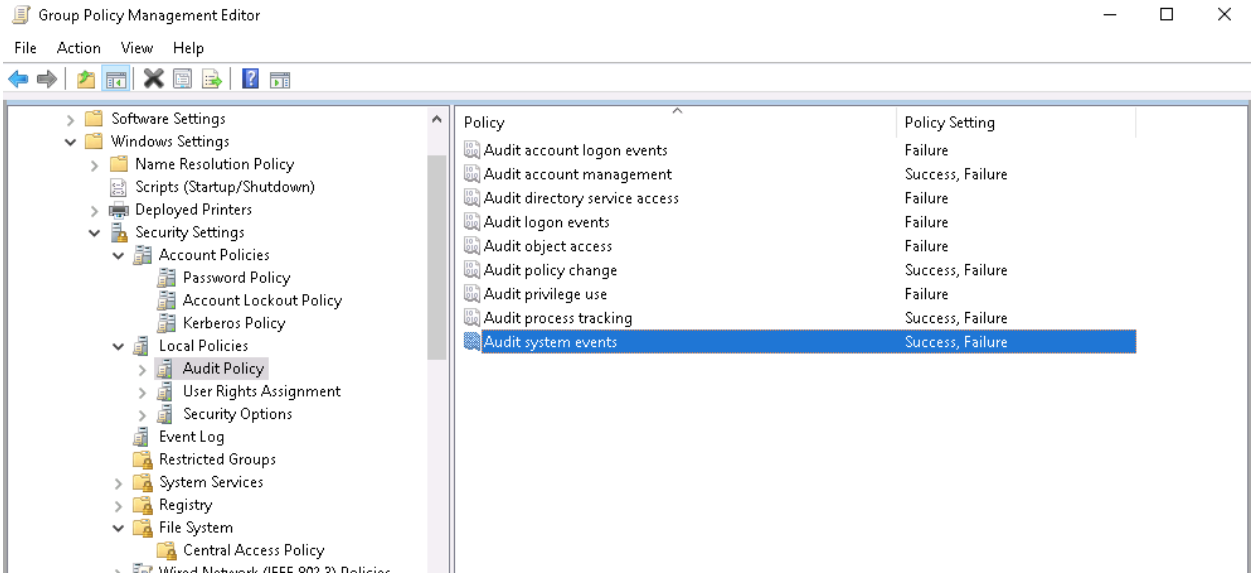
3.3. IA: Identification and Authentication

3.3.1. IA-5: Authenticator Management

Requirement:	Changing default content of authenticators prior to information system installation;
Control Reference:	NIST 800-53 (Rev. 4) IA-5(e)
Last Review and Update:	May 6 2020

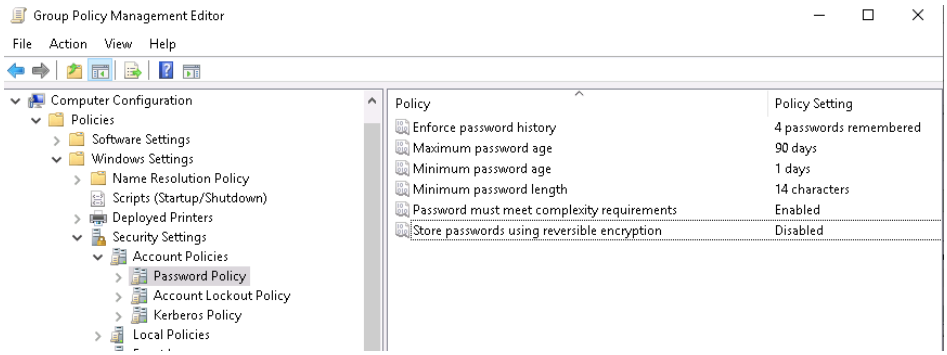
Implementation:

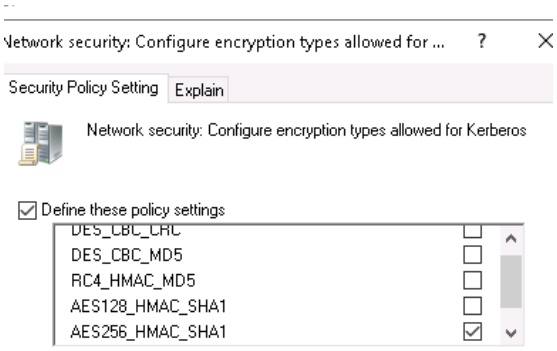
The administrator must enforce this by making sure no user uses the default credentials by checking the system logs to make sure account information was changed.



Requirement:	a.The system owner makes sure that the passwords have a minimum length of 14 characters and the defined complexity requirements are followed: 1. Password can't similar to the username and can't be a repetition of similar characters 2. Password must have unique characteristics as defined in the Microsoft docs for Group Policy Management. b.The system stores and transmits only cryptographically-protected passwords. c.The system owner enforces password minimum and maximum lifetime restrictions of 1 and 90 days respectively. d.The system owner makes sure that password reuse is prevented for 4 generations.
Control Reference:	NIST 800-53 (Rev. 4) IA-5(1)(a),(c),(d),(e)
Last Review and Update:	May 6 2020

Implementation:





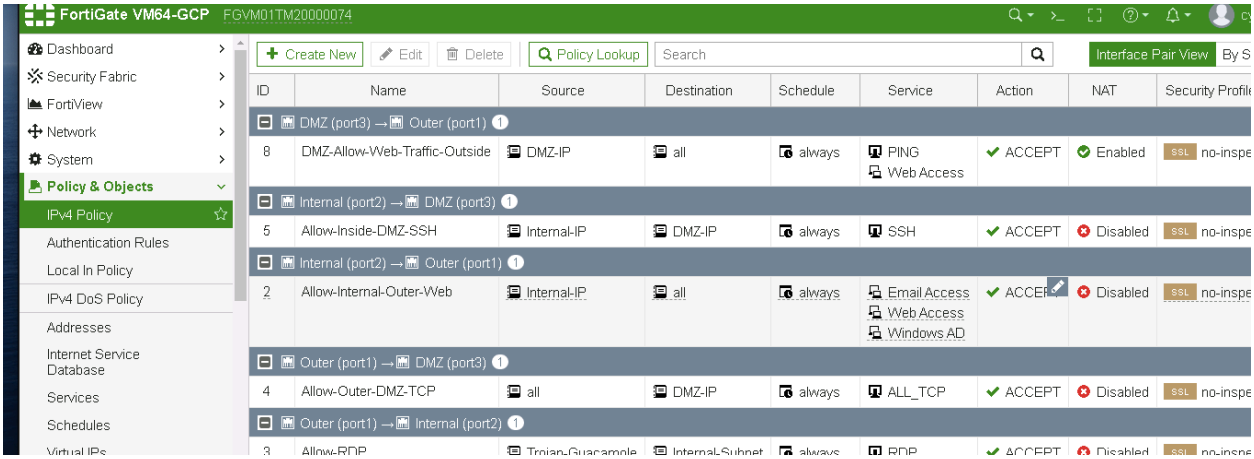
3.4. SC: System and Communications Protection

3.4.1. SC-7: Boundary Protection

Requirement:	The system owner monitors and controls communications at the external boundary of the system and at key internal boundaries within the system. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
Control Reference:	NIST 800-53 (Rev. 4) SC-7(a),(c)
Last Review and Update:	May 6 2020

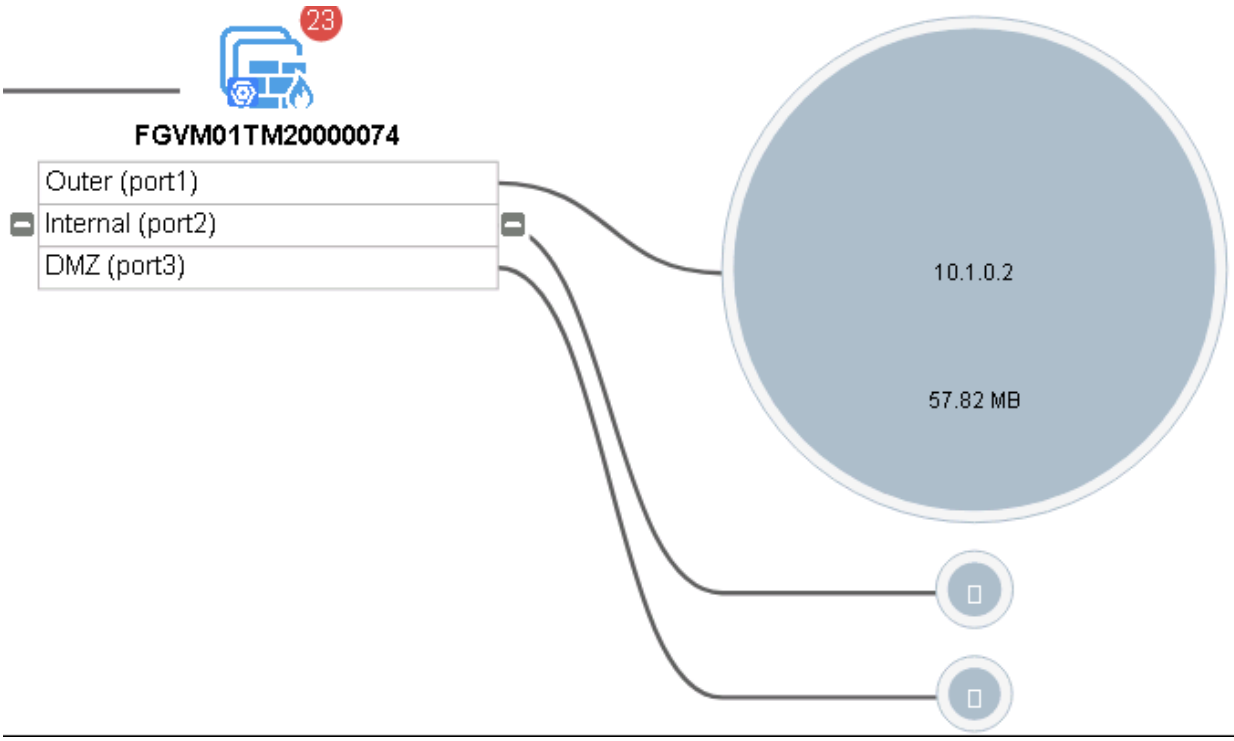
Implementation:

This is implemented through modification of firewall settings to control the type of traffic that is allowed.



Requirement:	The system owner implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks, i.e. creation of a DMZ zone for the implementation of the web server.
Control Reference:	NIST 800-53 (Rev. 4) SC-7(b)
Last Review and Update:	May 6 2020

Implementation:



Requirement:	The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).
Control Reference:	NIST 800-53 (Rev. 4) SC-7(5)
Last Review and Update:	May 6 2020

Implementation:

Implicit 1								
0	Implicit Deny	all	all	always	ALL	DENY		

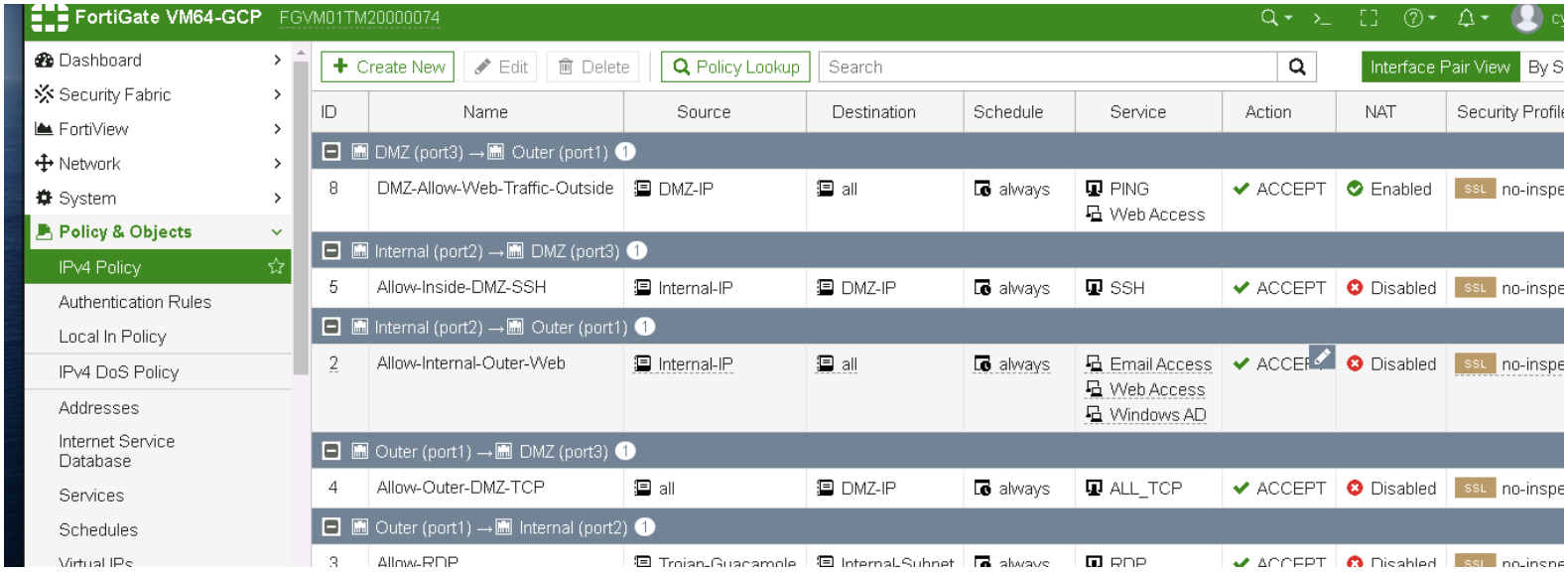
3.4.2. SC-8: Transmission Confidentiality and Integrity

Requirement:	The information system protects the integrity and confidentiality of transmitted information.
Control Reference:	NIST 800-53 (Rev. 4) SC-8
Last Review and Update:	May 6 2020

Implementation:

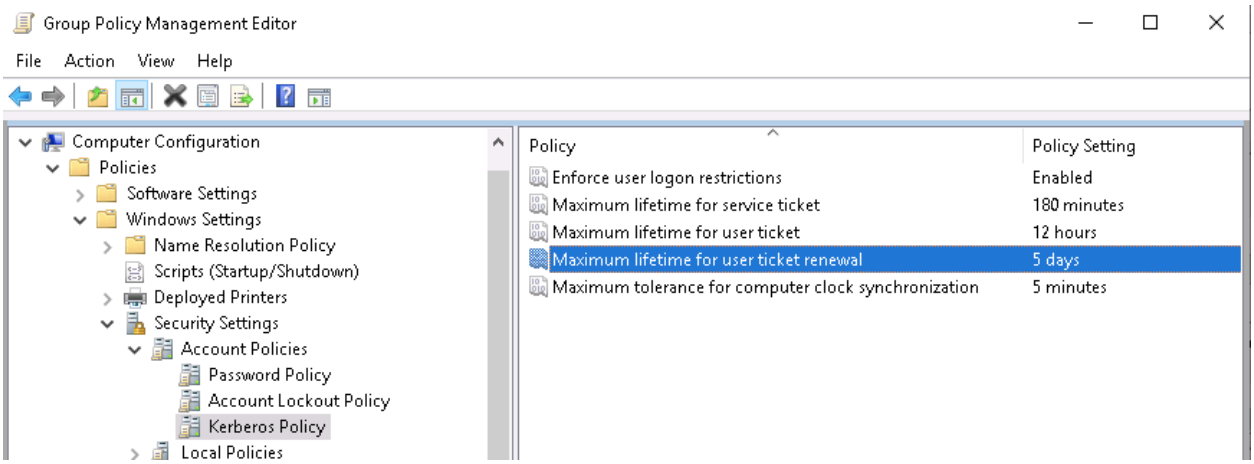
The confidentiality is protected by controlling all outgoing connections using firewalls. In addition, the use of certificates allow the transmissions to be secure.

Similarly, the integrity is protected by controlling all incoming connections.



Requirement:	The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information.
Control Reference:	NIST 800-53 (Rev. 4) SC-8(1)
Last Review and Update:	May 6 2020

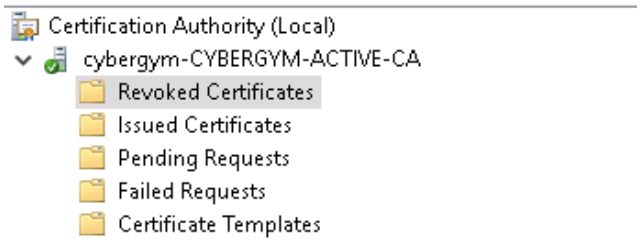
Implementation:



3.4.3. SC-12: Cryptographic Key Establishment and Management

Requirement:	The system owner establishes and manages cryptographic keys for required cryptography employed within the information system.
Control Reference:	NIST 800-53 (Rev. 4) SC-12
Last Review and Update:	May 6 2020

Implementation:



Issuing Certificates: Certificates are created to authenticate the true holder to decrypt a token.

Lifecycle:

- Generate Request: First, a public/private key pair is created for the server.
- Validate Request: The Certificate Authority validates the request prior to issuing the certificate.
- Digitally sign: The CA establishes the chain of trust by signing the certificate with the CA private key.
- Return the signed Certificate: Trust is established with the the Certificate via the CA.

Chain of Trust: Trust is established through the use of Certification Authority.

Revocation: If a certificate has its key compromised, it is placed in the revoked list and its removed from use.

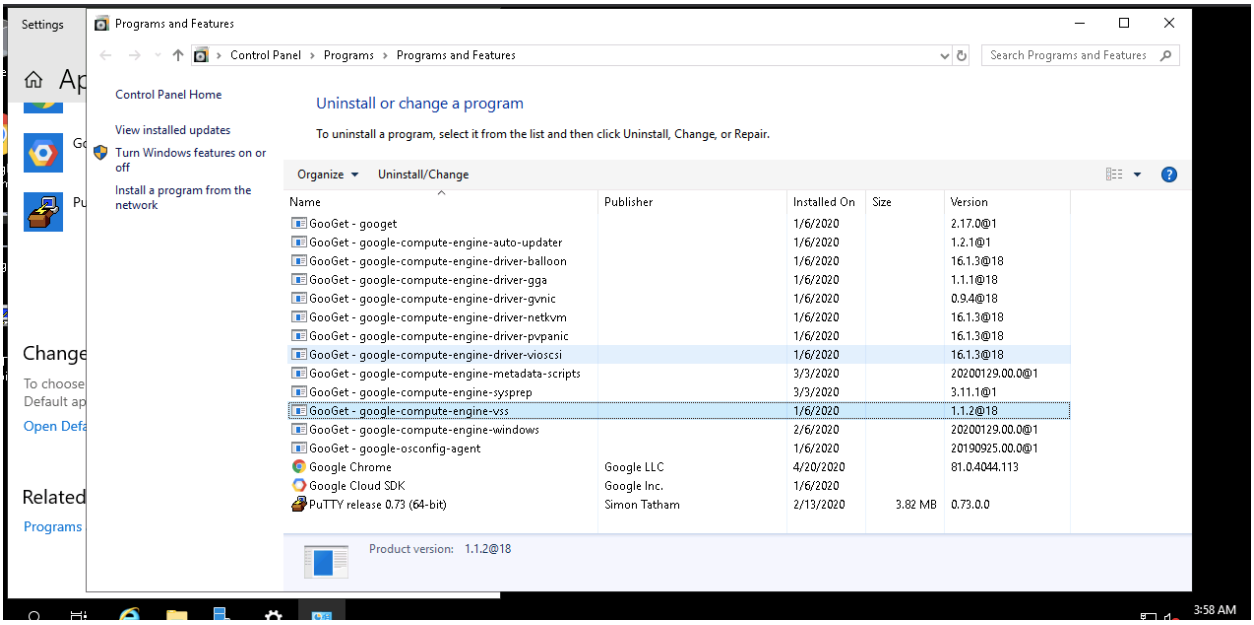
3.5. SI: System and Information Integrity

3.5.1. SI-2: Flaw Remediation

Requirement:	System owner identifies, reports, and corrects information system flaws.
Control Reference:	NIST 800-53 (Rev. 4) SI-2(a)
Last Review and Update:	May 6 2020

Implementation:

The system owner first identifies the various software components that are part of the system at any given time.



The system owner checks the NATIONAL VULNERABILITY DATABASE monthly for each software component that has been installed in the system.

- Keyword (text search): google chrome
- Search Type: Search All

Vuln ID	Summary	CVSS Severity
CVE-2020-6456	Insufficient validation of untrusted input in clipboard in Google Chrome prior to 81.0.4044.92 allowed a local attacker to bypass site isolation via crafted clipboard contents. **Published:** April 13, 2020; 02:15:13 PM -04:00	V3.1: 6.5 MEDIUM V2: 4.3 MEDIUM
CVE-2020-6455	Out of bounds read in WebSQL in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **Published:** April 13, 2020; 02:15:13 PM -04:00	V3.1: 8.8 HIGH V2: 6.8 MEDIUM
CVE-2020-6454	Use after free in extensions in Google Chrome prior to 81.0.4044.92 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. **Published:** April 13, 2020; 02:15:12 PM -04:00	V3.1: 8.8 HIGH V2: 6.8 MEDIUM
CVE-2020-6452	Heap buffer overflow in media in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	V3.1: 8.8 HIGH V2: 6.8 MEDIUM

Any software vulnerabilities found must be noted and kept on record and the available patches added to the workflow to be tested.

Requirement:	System owner tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation
Control Reference:	NIST 800-53 (Rev. 4) SI-2(b)
Last Review and Update:	May 6 2020

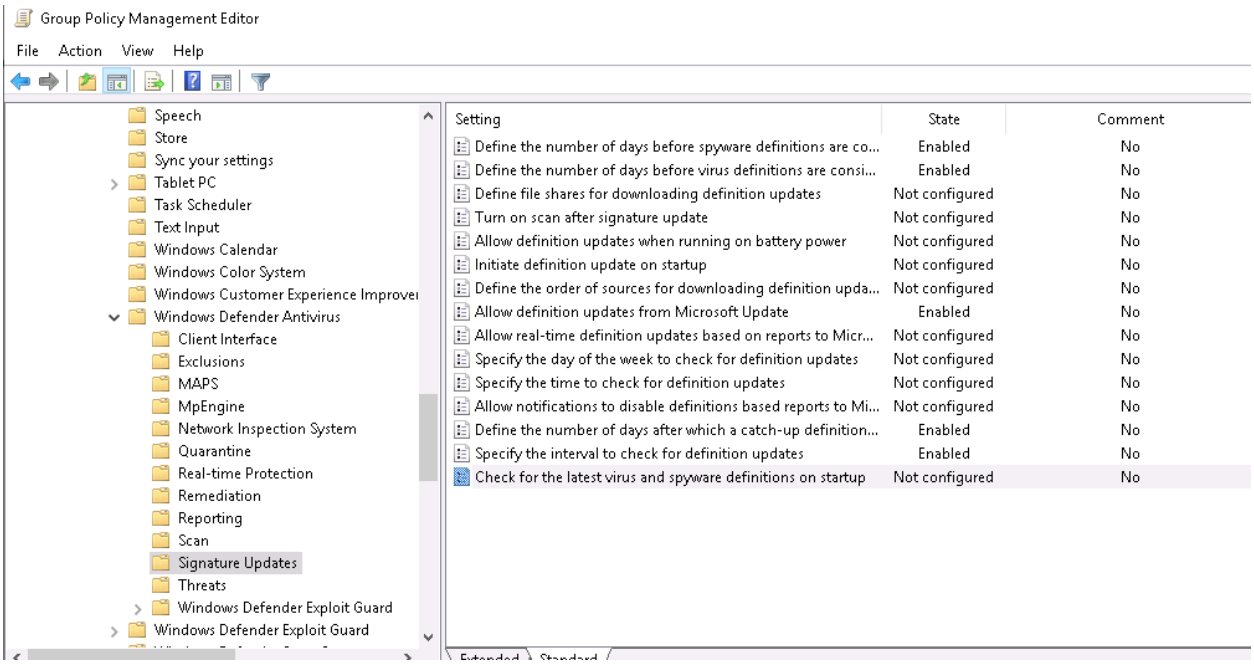
Implementation:

The system owner must load the update onto a system that is not connected to the network for testing. The testing should cover both the affected part of the software that were patched but also the unaffected parts to make sure the system behavior doesn't change after the update. Only when all tests are satisfactory, must the patch be applied to the whole system. If it is not up to the established standard, the previous version must be retained. In case of prolonged exposure(180 days), the software vendor must be contacted and an alternative software must be considered as a viable option to replace the current system component.

Requirement:	System owner installs security-relevant software and firmware updates within 30 days of the release of the updates.
Control Reference:	NIST 800-53 (Rev. 4) SI-2(c)
Last Review and Update:	May 6 2020

Implementation:

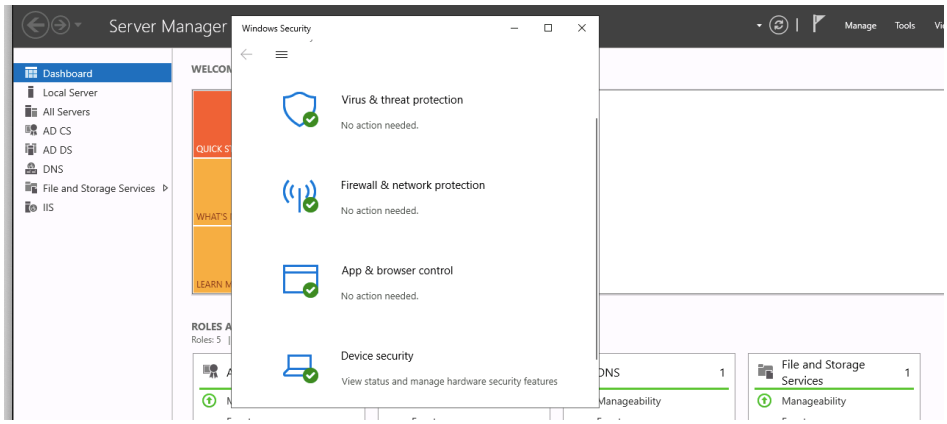
The software updates that pass the testing phase should be installed. The 90 day period allows for the update to be tested and if a critical update is released in the meanwhile, the update process can be modified to include the latest release if it passes testing.

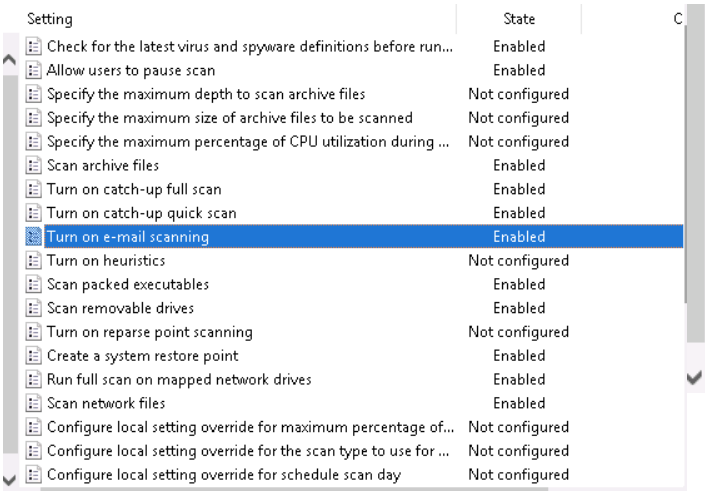


3.5.2. SI-3: Malicious Code Protection

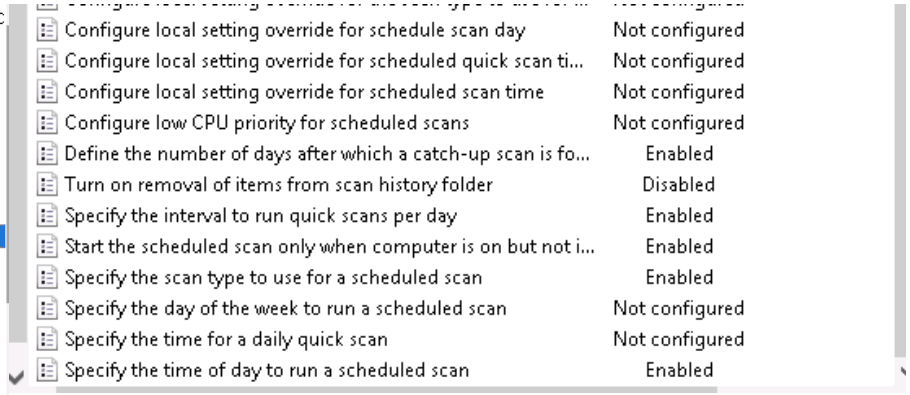
Requirement:	The system owner employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
Control Reference:	NIST 800-53 (Rev. 4) SI-3
Last Review and Update:	May 6 2020

Implementation:





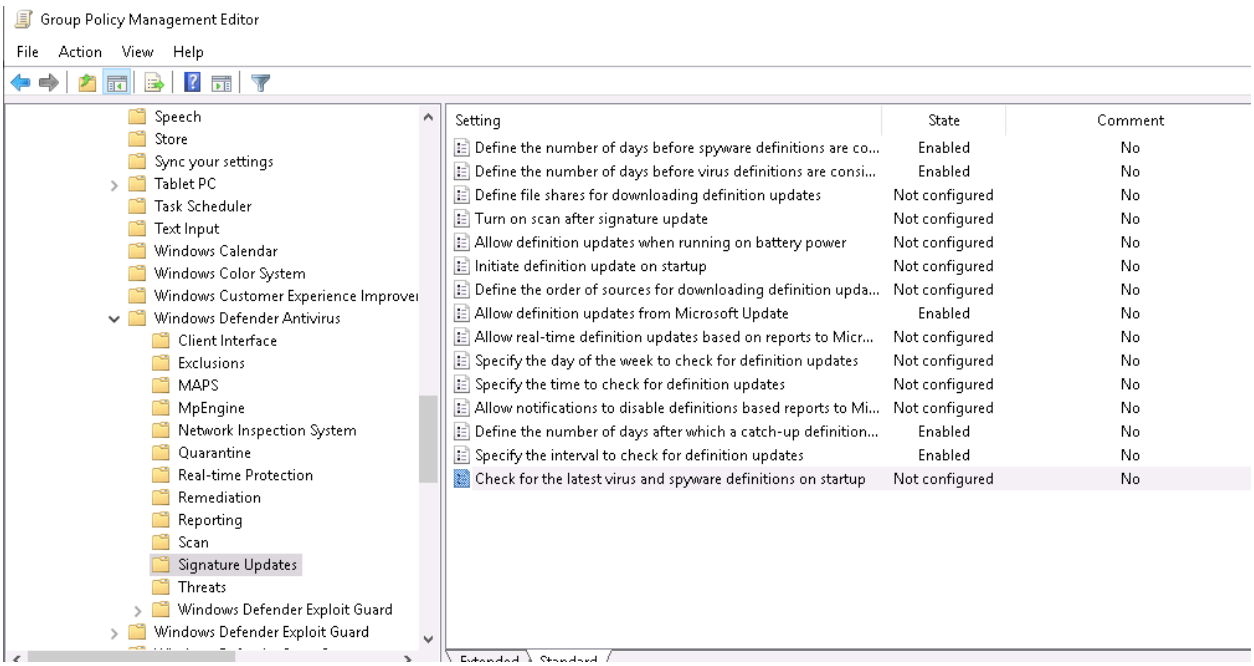
Setting	State
Check for the latest virus and spyware definitions before run...	Enabled
Allow users to pause scan	Enabled
Specify the maximum depth to scan archive files	Not configured
Specify the maximum size of archive files to be scanned	Not configured
Specify the maximum percentage of CPU utilization during ...	Not configured
Scan archive files	Enabled
Turn on catch-up full scan	Enabled
Turn on catch-up quick scan	Enabled
Turn on e-mail scanning	Enabled
Turn on heuristics	Not configured
Scan packed executables	Enabled
Scan removable drives	Enabled
Turn on reparse point scanning	Not configured
Create a system restore point	Enabled
Run full scan on mapped network drives	Enabled
Scan network files	Enabled
Configure local setting override for maximum percentage of...	Not configured
Configure local setting override for the scan type to use for ...	Not configured
Configure local setting override for schedule scan day	Not configured



Configure local setting override for schedule scan day	Not configured
Configure local setting override for scheduled quick scan ti...	Not configured
Configure local setting override for scheduled scan time	Not configured
Configure low CPU priority for scheduled scans	Not configured
Define the number of days after which a catch-up scan is fo...	Enabled
Turn on removal of items from scan history folder	Disabled
Specify the interval to run quick scans per day	Enabled
Start the scheduled scan only when computer is on but not i...	Enabled
Specify the scan type to use for a scheduled scan	Enabled
Specify the day of the week to run a scheduled scan	Not configured
Specify the time for a daily quick scan	Not configured
Specify the time of day to run a scheduled scan	Enabled

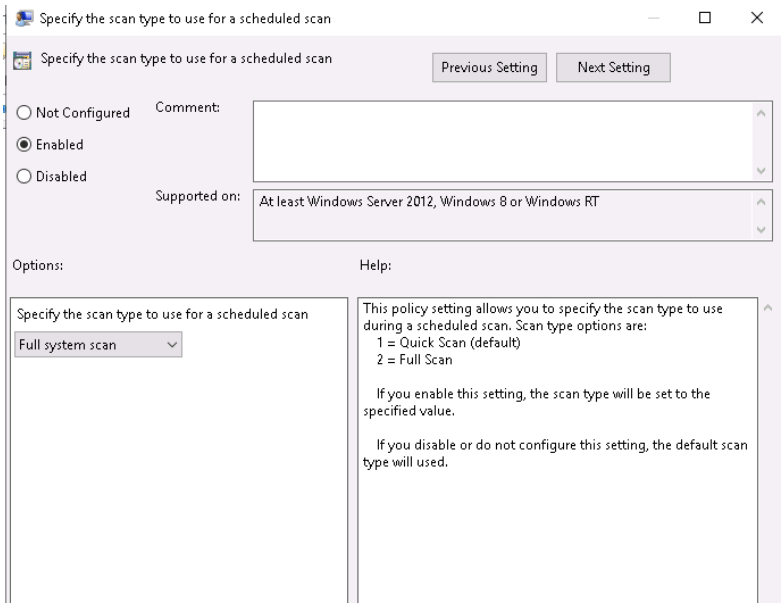
Requirement:	The system owner updates malicious code protection mechanisms whenever new releases are available.
Control Reference:	NIST 800-53 (Rev. 4) SI-3
Last Review and Update:	April 12 2020

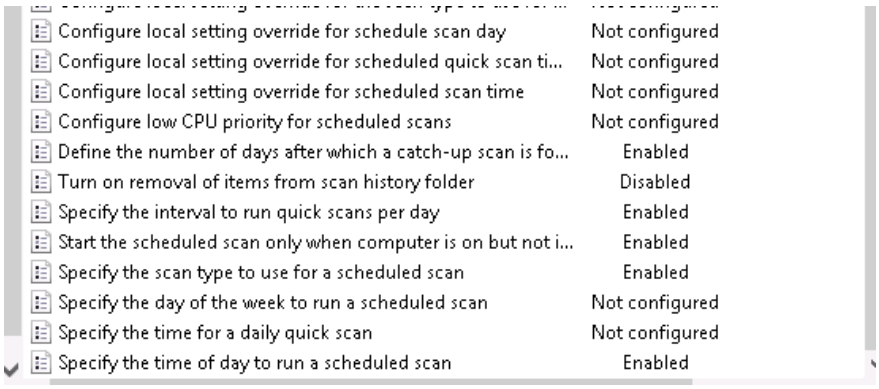
Implementation:



Requirement:	The system owner performs periodic scans of the information system. The system owner configures the Windows Security application to block malicious code, quarantine malicious code and send alert to administrator.
Control Reference:	NIST 800-53 (Rev. 4) SI-3
Last Review and Update:	April 12 2020

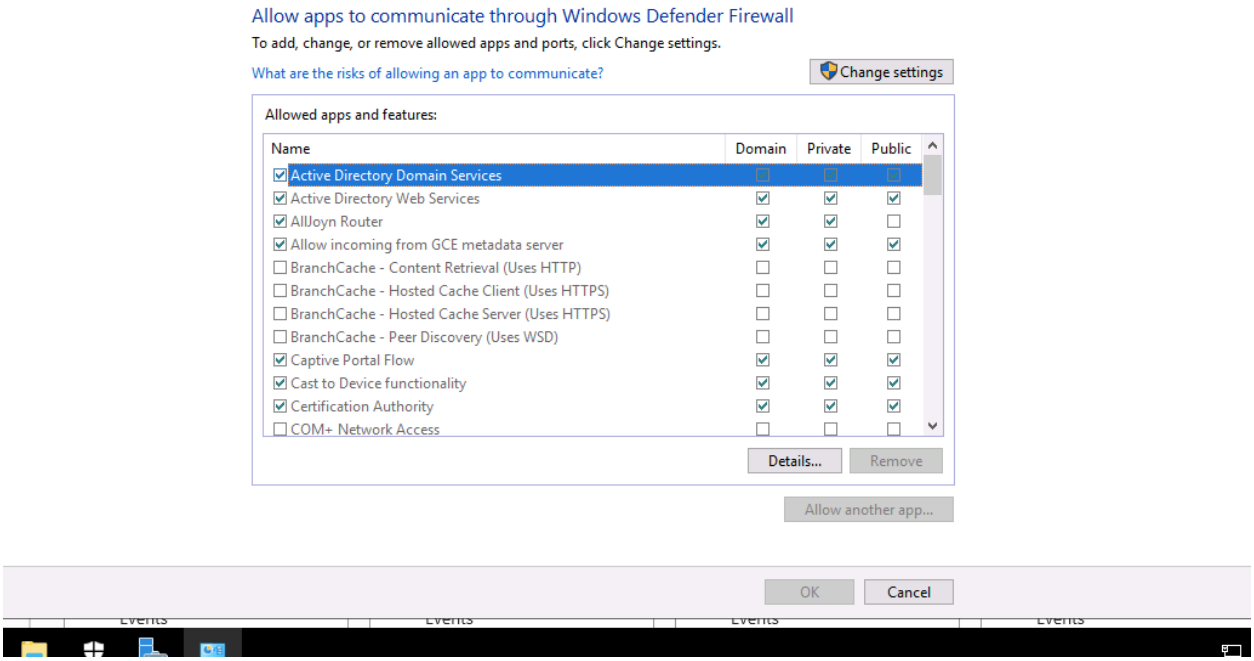
Implementation:





Requirement:	System owner addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
Control Reference:	NIST 800-53 (Rev. 4) SI-3(d)
Last Review and Update:	May 6 2020

Implementation:



4. Cyber Security Incident Response Plan

<This maps to control family IR. It is included outside of the security controls section because it is useful for individuals to quickly find in an event of a cyber security incident.

For the project provide a few paragraphs of things you would need to consider when responding to an incident. This does not need to be comprehensive.>

5. Recovery Plan

<This maps to control family CP. It is included outside of the security controls section because it is useful for individuals to quickly find in an event of a disaster.

For the project provide a few paragraphs of things you would need to consider when recovering from a disaster. Include documentation about taking system backups and steps for saving logs before writing over or destroying old configurations.>

6. Contacts – Vendor, Supplier, Internal

<See NIST 800-18, Section 3.5>
