CIS Benchmarks

CIS Check Point Firewall Benchmark

v1.1.0 - 06-29-2020

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Terms of Use 1
Overview 6
Intended Audience 6
Consensus Guidance 6
Typographical Conventions 7
Assessment Status 7
Profile Definitions 8
Acknowledgements 9
Recommendations 10
1 Password Policy 10
1.1 Ensure Minimum Password Length is set to 14 or higher (Automated) 11
1.2 Ensure Disallow Palindromes is selected (Automated) 13
1.3 Ensure Password Complexity is set to 3 (Automated) 15
1.4 Ensure Check for Password Reuse is selected and History Length is set to 12 or more (Automated) 17
1.5 Ensure Password Expiration is set to 90 days (Automated) 19
1.6 Ensure Warn users before password expiration is set to 7 days (Automated) 21
1.7 Ensure Lockout users after password expiration is set to 1 (Automated) 23
1.8 Ensure Deny access to unused accounts is selected (Automated) 25
1.9 Ensure Days of non-use before lock-out is set to 30 (Automated) 27
1.10 Ensure Force users to change password at first login after password was changed from Users page is selected (Automated) 29
1.11 Ensure Deny access after failed login attempts is slected (Automated) 31
1.12 Ensure Maximum number of failed attempts allowed is set to 5 or fewer (Automated) 33
1.13 Ensure Allow access again after time is set to 300 or more seconds (Automated) 35
2 Device Setup 37
2.1 General Settings 38

2.1.1 Ensure 'Login Banner' is set (Automated) 38
2.1.2 Ensure 'Message Of The Day (MOTD)' is set (Automated) 40
2.1.3 Ensure Core Dump is enabled (Automated) 42
2.1.4 Ensure Config-state is saved (Automated) 44
2.1.5 Ensure unused interfaces are disabled (Automated) 45
2.1.6 Ensure DNS server is configured (Automated) 47
2.1.7 Ensure IPv6 is disabled if not used (Automated) 49
2.1.8 Ensure Host Name is set (Automated) 50
2.1.9 Ensure Telnet is disabled (Automated) 51
2.1.10 Ensure DHCP is disabled (Automated) 53
2.2 SNMP 55
2.2.1 Ensure SNMP agent is disabled (Automated) 55
2.2.2 Ensure SNMP version is set to v3-Only (Automated) 57
2.2.3 Ensure SNMP traps is enabled (Automated) 59
2.2.4 Ensure SNMP traps receivers is set (Automated) 61
2.3 NTP 63
2.3.1 Ensure NTP is enabled and IP address is set for Primary and Secondary NTP server (Automated) 63
2.3.2 Ensure timezone is properly configured (Automated) 65
2.4 Backup 67
2.4.1 Ensure 'System Backup' is set. (Automated) 67
2.4.2 Ensure 'Snapshot' is set (Automated) 69
2.4.3 Configuring Scheduled Backups (Manual) 71
2.5 Authentication Settings 72
2.5.1 Ensure CLI session timeout is set to less than or equal to 10 minutes (Automated) 72
2.5.2 Ensure Web session timeout is set to less than or equal to 10 minutes (Automated) 74
2.5.3 Ensure Client Authentication is secured. (Automated) 76
2.5.4 Ensure Radius or TACACS+ server is configured (Automated) 78

2.5.5 Ensure allowed-client is set to those necessary for device management (Automated) 80
2.6 Logging 82
2.6.1 Ensure mgmtauditlogs is set to on (Automated) 82
2.6.2 Ensure auditlog is set to permanent (Automated) 84
2.6.3 Ensure cplogs is set to on (Automated) 86
3 Firewall Secure Settings 87
3.1 Enable the Firewall Stealth Rule (Automated) 88
3.2 Configure a Default Drop/Cleanup Rule (Automated) 89
3.3 Use Checkpoint Sections and Titles (Manual) 91
3.4 Ensure Hit count is Enable for the rules (Automated) 92
3.5 Ensure no Allow Rule with Any in Destination filed present in the Firewall Rules (Automated) 93
3.6 Ensure no Allow Rule with Any in Source filed present in the Firewall Rules (Automated) 94
3.7 Ensure no Allow Rule with Any in Services filed present in the Firewall Rules (Automated) 95
3.8 Logging should be enable for all Firewall Rules (Manual) 96
3.9 Review and Log Implied Rules (Automated) 97
3.10 Ensure Drop Out of State TCP Packets is enabled (Automated) 98
3.11 Ensure Drop Out of State ICMP Packets is enabled (Automated) 99
3.12 Ensure Anti-Spoofing is enabled and action is set to Prevent for all Interfaces (Automated) 100
3.13 Ensure Disk Space Alert is set (Automated) 102
3.14 Ensure Accept RIP is not enabled (Automated) 103
3.15 Ensure Accept Domain Name over TCP (Zone Transfer) is not enabled (Automated) 105
3.16 Ensure Accept Domain Name over UDP (Queries) is not enabled (Automated) 107
3.17 Ensure Accept ICMP Requests is not enabled (Automated) 109
3.18 Ensure Allow bi-directional NAT is enabled (Automated) 110
3.19 Ensure Automatic ARP Configuration NAT is enabled (Automated) 112

3.20 Ensure Logging is enabled for Track Options of Global Properties (Automated) 113
Appendix: Summary Table 115
Appendix: Change History 118

Overview

This document, Security Configuration Benchmark for Checkpoint Firewall, provides prescriptive guidance for establishing a secure configuration posture for Checkpoint Firewall versions R75.x – 80.x installed on Gaia Platform. This guide was tested against Checkpoint R80.10 installed on Gaia. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Check Point Firewall.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile apply to Check Point Firewall and intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile apply to Check Point Firewall and exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount
  - acts as defense in depth measure
  - may negatively inhibit the utility or performance of the technology.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Editor
Jayesh Rajan

Contributor
Jayesh Rajan
Danny Kane
Darren Freidel
Tom Fowler CISSP, CRISC, Xcel Energy

Recommendations

1 Password Policy

Setting for the Password Policy section of User Management

1.1 Ensure Minimum Password Length is set to 14 or higher (Automated)

Profile Applicability:

- Level 1

Description:

Defines the minimum length a password can be. The minimum number of characters of a password that is to be allowed for users or SNMP users. Does not apply to passwords that have already been set.

Rationale:

Password length has been found to be a primary factor in characterizing password strength. Passwords that are too short yield to brute force attacks as well as to dictionary attacks using words and commonly chosen passwords.

Audit:

Run the following command to verify the Minimum Password Length.
CLI:

```
Hostname>show password-controls min-password-length
Minimum Password Length 14
```

GUI:

```
Navigate to User Management > Password Policy
Ensure Minimum Password Length is set to 14 or higher.
```

Remediation:

Run the following command to set the min-password-length setting.
CLI:

```
Hostname>set password-controls min-password-length 14
```

GUI:

```
Navigate to User Management > Password Policy
Ensure 'Minimum Password Length' is set to 14 or higher.
```

Default Value:

6

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

1.2 Ensure Disallow Palindromes is selected (Automated)

Profile Applicability:

- Level 1

Description:

A palindrome is a sequence of letters, numbers, or characters that can be read the same in each direction. racecar, bob, and noon are some of the famous examples of Palindrome.

Rationale:

The Palindrome words are high on wordlists which are used before any brute-force attacks, and it's simpler to crack using the password cracking tools.

Audit:

Run the following command to verify the Disallow Palindrome setting.
CLI:

```
Hostname> show password-controls palindrome-check
Password Palindrome Check on
```

GUI:

```
Navigate to User Management > Password Policy
Ensure Disallow Palindrome setting is checked.
```

Remediation:

Run the following command to set the palindrome-check setting.
CLI:

```
Hostname>set password-controls palindrome-check on
```

GUI:

```
Navigate to User Management > Password Policy
Ensure 'Disallow Palindrome' is checked.
```

Default Value:

Selected

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

1.3 Ensure Password Complexity is set to 3 (Automated)

Profile Applicability:

- Level 1

Description:

This checks all new passwords to ensure that they meet basic requirements for strong passwords. The required number of character types are: Upper case alphabetic (A-Z), Lower case alphabetic (a-z), Digits (0-9), Other (everything else). A value of "1" effectively disables this check. Changes to this setting do not affect existing passwords.

Rationale:

Password complexity recommendations are derived from the USGCB (United States Government Configuration Baseline), Common Weakness Enumeration, and benchmarks published by the CIS (Center for Internet Security). Password complexity adds entropy to a password, in comparison to a simple password of the same length. A complex password is more difficult to attack, either directly against administrative interfaces or cryptographically, against captured password hashes. However, making a password of greater length will generally have a greater impact in this regard, in comparison to making a shorter password more complex.

Audit:

Run the following command to verify the Password Complexity.
CLI:

```
Hostname> show password-controls complexity
Password Complexity 3
```

GUI:

```
Navigate to User Management > Password Policy > Password Complexity:
Ensure '3 - Require three character types' checked.
```

Remediation:

Run the following command to set the password-controls complexity setting.
CLI:

```
Hostname>set password-controls complexity 3
```

GUI:

```
Navigate to User Management > Password Policy > Password Complexity:
checked the '3 - Require three character types' setting.
```

Default Value:

2

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

1.4 Ensure Check for Password Reuse is selected and History Length is set to 12 or more (Automated)

Profile Applicability:

- Level 1

Description:

Check for reuse of passwords. When a user's password is changed, the new password is checked against the recent passwords for the user. An identical password is not allowed. The number of passwords kept in the record is set by History length. Does not apply to SNMP passwords. Enables or disables password history checking and password history recording, for all users.

Rationale:

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. While current guidance emphasizes password length above frequent password changes, not enforcing password re-use guidance adds the temptation of using a small pool of passwords, which can make an attacker's job easier across an entire infrastructure.

Audit:

Run the following command to verify the Check for Password Reuse and History Length setting.
CLI:

```
Hostname> show password-controls history-checking
Password History Checking on

Hostname> show password-controls history-length
Password History Length 12
```

GUI:

```
Navigate to User Management > Password Policy > Password History:
Ensure 'Check for Password Reuse' is checked.

Navigate to User Management > Password Policy > Password History:
Ensure 'History Length' is set to 12 or more.
```

Remediation:

Run the following command to set tie history-checking setting.
CLI:

```
Hostname>set password-controls history-checking on

Hostname>set password-controls history-length 12
```

GUI:

```
Navigate to User Management > Password Policy > Password History:
checked the 'Check for Password Reuse' setting.

Navigate to User Management > Password Policy > Password History:
Set 'History Length' is set to 12 or more.
```

Default Value:

Selected

CIS Controls:

Version 7

4.1 Maintain Inventory of Administrative Accounts

Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

1.5 Ensure Password Expiration is set to 90 days (Automated)

Profile Applicability:

- Level 1

Description:

The number of days for which a password is valid. After that time, the password expires. The count starts when the user changes their passwords. Users are required to change an expired password the next time they log in. If set to never, passwords do not expire. Does not apply to SNMP users.

Rationale:

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.

Audit:

Run the following command to verify the Password Expiration setting.
CLI:

```
Hostname> show password-controls password-expiration
Password Expiration Lifetime 90
```

GUI:

```
Navigate to User Management > Password Policy > Mandatory Password Changes:
Password Expiration:
Ensure 'Password expires after' is checked and set to 90 or less.
```

Remediation:

Run the following command to set the history-length setting.
CLI:

```
Hostname>set password-controls history-length 90
```

GUI:

```
Navigate to User Management > Password Policy > Mandatory Password Changes:
Password Expiration:
Set 'Password expires after' setting to 90 or less
```

Default Value:

Password never expire

CIS Controls:

Version 7

4.1 Maintain Inventory of Administrative Accounts

Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

1.6 Ensure Warn users before password expiration is set to 7 days (Automated)

Profile Applicability:

- Level 1

Description:

The number of days before the password expires that the user starts getting warned they will have to change it. A user that does not log in will not see the warning.

Rationale:

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

Audit:

Run the following command to verify the warn users before Password Expiration x days setting.
CLI:

```
Hostname> show password-controls expiration-warning-days
Password Expiration Warning Days 7
```

GUI:

```
Navigate to User Management > Password Policy > Mandatory Password Changes
Ensure 'Warn users before password expiration' is set to 7 days or less.
```

Remediation:

Run the following command to set the expiration-warning-days setting.
CLI:

```
Hostname>set password-controls expiration-warning-days 7
```

GUI:

```
Navigate to User Management > Password Policy > Mandatory Password Changes
Set 'Warn users before password expiration' is set to 7 days or less.
```

Default Value:

7 days

CIS Controls:

Version 7

4.1 Maintain Inventory of Administrative Accounts

Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

1.7 Ensure Lockout users after password expiration is set to 1 (Automated)

Profile Applicability:

- Level 1

Description:

Lockout users after password expiration. After a user's password has expired, they have this number of days to log in and change it. If they do change their password within that number of days they will be unable to log in: They are locked out. A value of never allows the user to wait as long as they want to change their password.

Rationale:

User accounts and their passwords are the front-line of defense against malicious users gaining access to critical systems and data. Just as important as ensuring strong passwords are used and changed regularly, unused accounts should be closely monitored and disabled, whenever possible. Inactive accounts could become targets of brute force or dictionary attacks to gain access to the network and critical data/devices attached to it.

Audit:

Run the following command to verify the lockout users after x days setting.
CLI:

```
Hostname> show password-controls expiration-lockout-days
Password Expiration Lockout Days 1
```

GUI:

```
Navigate to User Management > Password Policy > Mandatory Password Changes >
Lockout users after password expiration:
Ensure 'Lockout user after' is checked and set to 1 day.
```

Remediation:

Run the following command to set the expiration-lockout-days setting.
CLI:

```
Hostname>set password-controls expiration-lockout-days 1
```

GUI:

```
Navigate to User Management > Password Policy > Mandatory Password Changes >
Lockout users after password expiration:
Checked 'Lockout user after' setting and set to 1 day.
```

Default Value:

Never lockout users after password expires

CIS Controls:

Version 7

4.1 Maintain Inventory of Administrative Accounts

Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

4.9 Log and Alert on Unsuccessful Administrative Account Login

Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

1.8 Ensure Deny access to unused accounts is selected (Automated)

Profile Applicability:

- Level 1

Description:

Deny access to unused accounts. If there has been no successful login attempt in a set period of time, the user is locked out and cannot log in.

Rationale:

User accounts that have been unused for over a given period of time can be automatically disabled. Unused accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies

Audit:

Run the following command to verify the Deny access to unused accounts setting.
CLI:

```
Hostname> show password-controls deny-on-nonuse enable
Deny Access to Unused Accounts on
```

GUI:

```
Navigate to User Management > Password Policy > Deny access to unused
accounts:
Ensure 'Deny access to unused accounts' is checked.
```

Remediation:

Run the following command to set the deny-on-nonuse setting.
CLI:

```
Hostname>set password-controls deny-on-nonuse enable on
```

GUI:

```
Navigate to User Management > Password Policy > Deny access to unused
accounts:
Checked the 'Deny access to unused accounts' setting.
```

Default Value:

Not Selected

CIS Controls:

Version 7

4.1 Maintain Inventory of Administrative Accounts

Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.9 Ensure Days of non-use before lock-out is set to 30 (Automated)

Profile Applicability:

- Level 1

Description:

Days of non-use before lock-out. The number of days in which a user has not (successfully) logged in before that user is locked out. This only takes effect if Deny access to unused accounts is selected.

Rationale:

User accounts that have been unused for over a given period of time can be automatically disabled. It is recommended that accounts that are unused for 30 days should be disabled. Unused accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Audit:

Run the following command to verify the Days of non-use before lock-out setting.
CLI:

```
Hostname> show password-controls deny-on-nonuse allowed-days
Days Nonuse Before Lockout 30
```

GUI:

```
Navigate to User Management > Password Policy > Deny access to unused
accounts:
Ensure 'Days of non-use before lock-out' is set to 30 or less.
```

Note: This setting only takes effect if 'Deny access to unused accounts' is enabled.

Remediation:

Run the following command to set the deny-on-nonuse allowed-days setting.
CLI:

```
Hostname>set password-controls deny-on-nonuse allowed-days 30
```

GUI:

```
Navigate to User Management > Password Policy > Deny access to unused
accounts:
Set 'Days of non-use before lock-out' to 30 or less.
```

Note: This setting only takes effect if 'Deny access to unused accounts' is enabled.

Default Value:

365

CIS Controls:

Version 7

4.1 Maintain Inventory of Administrative Accounts

Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.10 Ensure Force users to change password at first login after password was changed from Users page is selected (Automated)

Profile Applicability:

- Level 1

Description:

Force users to change password at first login after their password was changed using the command set user password or from the WebUI User Management > Users page.

Rationale:

This forces the user to change the password and not to use the password set by the Administrator.

Audit:

Run the following command to verify the Force users to change password at first login after password was changed from Users page setting.
CLI:

```
Hostname>show password-controls force-change-when
Force Password Change When Password
```

GUI:

```
Navigate to User Management > Password Policy > Mandatory Password Change:
Ensure 'Force users to change password at first login after password was
changed from Users page' is checked.
```

Remediation:

Run the following command to set force-change-when setting.
CLI:

```
Hostname>set password-controls force-change-when password
```

GUI:

```
Navigate to User Management > Password Policy > Mandatory Password Change:
Checked the 'Force users to change password at first login after password was
changed from Users page' setting.
```

Default Value:

Not Selected

CIS Controls:

Version 7

4.1 Maintain Inventory of Administrative Accounts

Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.11 Ensure Deny access after failed login attempts is selected (Automated)

Profile Applicability:

- Level 1

Description:

If the configured limit is reached, the user is locked out (unable to log in) for a configurable period of time.

Rationale:

Locking out user IDs after n unsuccessful consecutive login attempts mitigate brute force password attacks against your systems.

Audit:

Run the following command to verify the Deny access after failed login attempts setting.
CLI:

```
Hostname> show password-controls deny-on-fail enable
Deny Access After Failed Attempts on
```

GUI:

```
Navigate to User Management > Password Policy > Deny Access After Failed
Login Attempts:
Ensure 'Deny access after failed login attempts' is checked.
```

Remediation:

Run the following command to set the deny-on-fail setting.
CLI:

```
Hostname>set password-controls deny-on-fail enable on
```

GUI:

```
Navigate to User Management > Password Policy > Deny Access After Failed
Login Attempts:
Checked the 'Deny access after failed login attempts' setting.
```

Default Value:

Not selected

CIS Controls:

Version 7

4.1 Maintain Inventory of Administrative Accounts

Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

4.9 Log and Alert on Unsuccessful Administrative Account Login

Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.12 Ensure Maximum number of failed attempts allowed is set to 5 or fewer (Automated)

Profile Applicability:

- Level 1

Description:

This only takes effect if Deny access after failed attempts is enabled. The number of failed login attempts that a user is allowed before being locked out. After making that many successive failed attempts, future attempts will fail. When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero.

Rationale:

Repeated failed login attempts could either be a valid user who has forgotten the password, or a malicious attempt to gain access to the system. For this reason, this setting should be as restrictive as possible to mitigate brute force attack attempts to discover a user's password.

Audit:

Run the following command to verify the Deny access after failed login attempts setting.
CLI:

```
Hostname> show password-controls deny-on-fail failures-allowed
Maximum Failed Attempts 5
```

GUI:

```
Navigate to User Management > Password Policy > Deny Access After Failed
Login Attempts:
Ensure ' Maximum number of failed attempts allowed is set to' is set to 5or
fewer.
```

Remediation:

Run the following command to set the deny-on-fail failures-allowed setting.
CLI:

```
Hostname>set password-controls deny-on-fail failures-allowed 5
```

GUI:

```
Navigate to User Management > Password Policy > Deny Access After Failed
Login Attempts:
checked and set ' Maximum number of failed attempts allowed is set to'
setting to 5 or fewer.
```

Default Value:

10

References:

1. https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/73101.htm#o94478

Notes:

Looking for input regarding a value for this recommendation.

Note from checkpoint documentation....

Warning: Enabling this leaves you open to a "denial of service" -- if an attacker issues unsuccessful login attempts often enough you will be locked out. Please consider the advantages and disadvantages of this option, in light of your security policy, before enabling it.

CIS Controls:

Version 7

4.1 Maintain Inventory of Administrative Accounts

Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.13 Ensure Allow access again after time is set to 300 or more seconds (Automated)

Profile Applicability:

- Level 1

Description:

Allow access again after a user has been locked out (due to failed login attempts). The user is allowed access after the configured time if there have been no login attempts during that time). This setting only takes effect if Deny access after failed login attempts is selected.

Rationale:

Users can accidentally lock themselves out of their accounts if they mistype their password multiple times. To reduce the chance of such accidental lockouts, the Allow access again after time setting determines the number of seconds that must elapse before the counter that tracks failed logon attempts and triggers lockouts is reset to 0.

Audit:

Run the following command to verify the Allow access again after time setting.
CLI:

```
Hostname> show password-controls deny-on-fail allow-after
Unlock User After Seconds 300
```

GUI:

```
Navigate to User Management > Password Policy > Deny Access After Failed
Login Attempts:
Ensure 'Allow access again after time' is set to 300 or more seconds.
```

Remediation:

Run the following command to set the deny-on-fail allow-afte setting.
CLI:

```
Hostname> set password-controls deny-on-fail allow-after 300
```

GUI:

```
Navigate to User Management > Password Policy > Deny Access After Failed
Login Attempts:
Set the 'Allow access again after time' setting to 300 or more seconds.
```

Default Value:

1200 (20 minutes)

Notes:

Looking for input regarding a value for this recommendation.

CIS Controls:

Version 7

4.1 Maintain Inventory of Administrative Accounts

Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2 Device Setup

2.1 General Settings

2.1.1 Ensure 'Login Banner' is set (Automated)

Profile Applicability:

- Level 1

Description:

Configure a login banner, ideally approved by the organization's legal team. This banner should, at minimum, prohibit unauthorized access, provide notice of logging or monitoring, and avoid using the word "welcome" or similar words of invitation.

Rationale:

Through a properly stated login banner, the risk of unintentional access to the device by unauthorized users is reduced. Should legal action take place against a person accessing the device without authorization, the login banner greatly diminishes a defendant's claim of ignorance.

Audit:

Run the following command to verify the Banner configured on the device and it's status.
CLI:

```
Hostname>show configuration message
set message banner on

set message banner on line msgvalue "Organization defined Banner"
```

GUI:

```
Navigate to System Management -> Messages -> Banner message
Ensure Banner Message should be checked and "Organization defined Banner"
should be set.
```

Remediation:

Run the following command to enable and set the Banner.
CLI:

```
Hostname>set message banner on msgvalue "Organization_Banner"
```

GUI:

```
Navigate to System Management > Messages
Checked the Banner message and configured the organization defined banner.
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.2 Ensure 'Message Of The Day (MOTD)' is set (Automated)

Profile Applicability:

- Level 1

Description:

Sets the MOTD message.

Rationale:

Network banners are electronic messages that provide notice of legal rights to users of computer networks. From a legal standpoint, banners have four primary functions.

- First, banners may be used to generate consent to real-time monitoring under Title III.
- Second, banners may be used to generate consent to the retrieval of stored files and records pursuant to ECPA.
- Third, in the case of government networks, banners may eliminate any Fourth Amendment "reasonable expectation of privacy" that government employees or other users might otherwise retain in their use of the government's network under O'Connor v.

Audit:

Run the following command to verify the MOTD Banner is configured on the device and it's status.
CLI:

```
Hostname>show configuration message
set message motd on
set message motd on line msgvalue "MOTD BANNER"
```

GUI:

```
Navigate to System Management -> Messages -> Message of the day
Ensure Message of the day should be checked and "MOTD" Banner should be set.
```

Remediation:

Run the following command to enable and configured the MOTD setting.
CLI:

```
Hostname> set message motd on msgvalue "MOTD BANNER"
```

GUI:

```
Navigate to System Management -> Messages -> Message of the day
Checked the Message of the day and add "MOTD Banner".
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.3 Ensure Core Dump is enabled (Automated)

Profile Applicability:

- Level 1

Description:

A Core Dump contains the recorded state of the working memory and CPU's contents of the Gaia system at the time that a Gaia process terminated abnormally. The core file is stored in the /var/log/dump/usermode directory.

Rationale:

The Core Dump helps in troubleshooting to identify for which reason the process/system got crashed.

Audit:

Run the following command to check the status of Core Dump.

```
Hostname> show core-dump status
```

GUI:

```
Navigate to System Management > Core Dump
```

Remediation:

Run the following command to set Core Dump.

```
Hostname> set core-dump enable
```

GUI:

```
Navigate to System Management > Core Dump > select Enable Core Dumps
```

Default Value:

enabled

CIS Controls:

Version 7

5.4 Deploy System Configuration Management Tools

Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

2.1.4 Ensure Config-state is saved (Automated)

Profile Applicability:

- Level 1

Description:

The 'Config state' setting provides the detail of the current configuration which is saved or unsaved. Saved state indicates the current configuration of the system is matched with the saved configuration, while unsaved state indicates a configuration change has been made and it has not been saved to the configuration file.

Rationale:

The Unsaved state indicates that some configuration changes are made in the system. Administrator needs to review whether all changes are authorized or not by verifying configuration change logs.

Audit:

Run the following command to check the status of config-state.

```
Hostname> show config-state
```

Remediation:

Run the following command to save the configuration.

```
Hostname> save config
```

Default Value:

NA

CIS Controls:

Version 7

5.2 Maintain Secure Images

Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.

2.1.5 Ensure unused interfaces are disabled (Automated)

Profile Applicability:

- Level 1

Description:

Disables the unused interfaces.

Rationale:

Shutting down the unused interfaces is a complement to physical security. In fact, an attacker connecting physically to an unused port of the security appliance can use the interface to gain access to the device if the relevant interface has not been disabled and the source restriction to management access is not enabled.

Audit:

Run the following command to check the status of all interfaces and verify interface state is off if it is not in used.
CLI:

```
Hostname> show interfaces all
```

GUI:

```
Navigate to Network Management > Network Interfaces
```

Remediation:

Run the following command disable the unused interface.
CLI:

```
Hostname> set interface <Interface_Number> state off
```

GUI:

```
Navigate to Network Management > Network Interfaces > Open unused Interface >
unchecked Enable
```

Default Value:

NA

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

9.1 Associate Active Ports, Services and Protocols to Asset Inventory

Associate active ports, services and protocols to the hardware assets in the asset inventory.

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.6 Ensure DNS server is configured (Automated)

Profile Applicability:

- Level 1

Description:

Gaia uses the Domain Name Service (DNS) to translate host names into IP addresses. To enable DNS lookups, you must specify the primary DNS server for your system. You can also specify secondary and tertiary DNS servers. When resolving host names, the system consults the primary name server. If a failure or time-out occurs, the system consults the secondary name server, and if necessary, the tertiary.

Rationale:

The purpose is to perform the resolution of system hostnames to Internet Protocol (IP) addresses.

Audit:

Run the following command to check the Primary, Secondary and tertiary DNS are configured.
CLI:

```
Hostname> show dns primary
10.22.1.39
Hostname> show dns secondary
10.88.3.99
Hostname> show dns tertiary
10.10.1.2
```

GUI:

```
Navigate to Network Management > Hosts and DNS > DNS
```

Remediation:

Run the following command to set DNS server.
CLI:

```
Hostname> set dns primary <IP_Address>
Hostname> set dns secondary <IP_Address>
Hostname> set dns tertiary <IP_Address>
```

GUI:

```
Navigate to Network Management > Hosts and DNS > DNS
Set Primary, secondary and tertiary DNS server address.
```

Default Value:

Not Configured

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

2.1.7 Ensure IPv6 is disabled if not used (Automated)

Profile Applicability:

- Level 1

Description:

Although IPv6 has many advantages over IPv4, not all organizations have IPv6 or dual stack configurations implemented

Rationale:

If IPv6 or dual stack is not to be used, it is recommended that IPv6 be disabled to reduce the attack surface of the system.

Audit:

Run the following command to check IPv6 status.

```
Hostname> show ipv6-state
```

Remediation:

Run the following command to enable or disable IPv6.

```
Hostname> set ipv6-state on
Hostname> set ipv6-state off
```

Default Value:

ipv6 is disabled

CIS Controls:

Version 7

11.2 Document Traffic Configuration Rules

All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

2.1.8 Ensure Host Name is set (Automated)

Profile Applicability:

- Level 1

Description:

Changes the device default hostname.

Rationale:

The device hostname plays an important role in asset inventory and identification as a security requirement, but also in the public keys and certificate deployments as well as when correlating logs from different systems during an incident handling.

Audit:

Run the following command to check Host Name.
CLI:

```
Hostname> show hostname
```

GUI:

```
Navigate to Network Management > Hosts and DNS > System Name > Host Name
```

Remediation:

Run the following command to set Host Name.
CLI:

```
Hostname> set hostname <name>
```

GUI:

```
Navigate to Network Management > Hosts and DNS > System Name > Host Name
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.9 Ensure Telnet is disabled (Automated)

Profile Applicability:

- Level 1

Description:

Disables the telnet access to the security appliance in the case it has been configured.

Rationale:

Telnet is an unsecure protocol as username and password are conveyed in clear text during the administrator authentication and can be retrieved through network sniffing.

Audit:

Run the following command to check the status of telnet.
CLI:

```
Hostname> show net-access telnet
```

GUI:

```
Navigate to System Management > Network Access > Enable Telnet
```

Remediation:

Run the following command to disable the telnet.
CLI:

```
Hostname> set net-access telnet off
```

GUI:

```
Navigate to System Management > Network Access > verify Enable Telnet is
unchecked.
```

Default Value:

Off

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.10 Ensure DHCP is disabled (Automated)

Profile Applicability:

- Level 1

Description:

Disable the Dynamic Host Configuration Protocol (DHCP) server on your device.

Rationale:

The DHCP server supplies automatic configuration parameters, such as dynamic IP address, to requesting systems. A dedicated server located in a secured management zone should be used to provide DHCP services instead. Attackers can potentially be used for denial-of-service (DoS) attacks.

Audit:

Run the following command to check the status of DHCP Server.
CLI:

```
Hostname> show dhcp server status
```

GUI:

```
Navigate to Network Management > DHCP Server > DHCP Server Configuration >
Enable DHCP Server
```

Remediation:

Run the following command to disable the DHCP.
CLI:

```
Hostname> set dhcp server disable
```

GUI:

```
Navigate to Network Management > DHCP Server > DHCP Server Configuration >
veriify Enable DHCP Server is unchecked
```

Default Value:

DHCP Server Disabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.2 SNMP

2.2.1 Ensure SNMP agent is disabled (Automated)

Profile Applicability:

- Level 1

Description:

The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.

Rationale:

The SNMP server can communicate using SNMP v1, which transmits data in the clear and does not require authentication to execute commands. Unless absolutely necessary, it is recommended that the SNMP service not be used. If SNMP is required the server should be configured to use only SNMPv3.

Audit:

Run the following command to check whether the SNMP agent is configured:
CLI:

```
Hostname> show snmp agent
SNMP Agent Disabled
```

GUI:

```
Navigate to System Management > SNMP  >  SNMP General Settings
Verify Enable SNMP agent is unchecked.
```

Remediation:

Run the following command to configure the SNMP.

```
CLI:
Hostname> set snmp agent off
```

GUI:

```
System Management > SNMP > Unhecked the Enable SNMP Agent
```

Default Value:

SNMP Agent Disabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.2.2 Ensure SNMP version is set to v3-Only (Automated)

Profile Applicability:

- Level 1

Description:

Sets the SNMP v3.

Rationale:

SNMP Version 3 provides security enhancements that are not available in SNMP Version 1 or SNMP Version 2c. SNMP Versions 1 and 2c transmit data between the SNMP server and SNMP agent in clear text. SNMP Version 3 adds authentication and privacy options to secure protocol operations. For configuration purposes, the authentication and privacy options are grouped together into security models. Security models apply to users and groups, and are divided into the following three types: •NoAuthPriv—No Authentication and No Privacy, which means that no security is applied to messages. •AuthNoPriv—Authentication but No Privacy, which means that messages are authenticated. •AuthPriv—Authentication and Privacy, which means that messages are authenticated and encrypted. It is recommended that packets should be authenticated and encrypted

Audit:

Run the following command to check whether the SNMP agent-version v3-only is configured
CLI:

```
Hostname> show snmp agent-version
v3-Only
```

GUI:

```
Navigate to System Management > SNMP  >  SNMP General Settings
Verify version is set to v3-Only.
```

Remediation:

Run the following command to configure the SNMP agent-version v3-only
CLI:

```
Hostname> set snmp agent-version v3-Only
```

GUI:

```
Navigate to System Management > SNMP > Select V3-Only in Version
```

Default Value:

Not Configured

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.2.3 Ensure SNMP traps is enabled (Automated)

Profile Applicability:

- Level 1

Description:

Enables SNMP traps to be sent to the NMS.

Rationale:

The purpose of the SNMP service is to monitor in real time the events occurring on systems in order to meet the security requirement of availability of systems and services. The traps are SNMP notifications sent to the NMS and should be enabled in order to be sent and processed by the NMS. The NMS will then provide a comprehensive aggregation and reporting of events generated, thus helping administrator.

Audit:

Run the following command to check whether the SNMP traps are configured:
CLI:

```
Hostname> show snmp traps enabled-traps
authorizationError
coldStart
configurationChange
```

GUI:

```
Navigate to System Management > SNMP  >  Enabled Traps
Verify authorizationError, coldStart, configurationChange, configurationSave,
linkUpLinkDown and lowDiskSpace alerts are selected.
```

Remediation:

Run the following command to Configure the SNMP traps.
CLI:

```
Hostname> set snmp traps trap authorizationError enable
Hostname> set snmp traps trap coldStart enable
Hostname> set snmp traps trap configurationChange enable
Hostname> set snmp traps trap configurationSave enable
Hostname> set snmp traps trap linkUpLinkDown enable
Hostname> set snmp traps trap lowDiskSpace enable
```

GUI:

```
Navigate to System Management > SNMP > Enabled Traps > Set and select the
following traps
uthorizationError, coldStart, configurationChange, configurationSave,
linkUpLinkDown and lowDiskSpace
```

Default Value:

Not Configured

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.2.4 Ensure SNMP traps receivers is set (Automated)

Profile Applicability:

- Level 1

Description:

Enables SNMP traps receivers where traps to be sent to.

Rationale:

The purpose of the SNMP service is to monitor in real time the events occurring on systems in order to meet the security requirement of availability of systems and services. The traps are SNMP notifications sent to the NMS or SNMP traps receivers and should be enabled in order to be sent and processed by the NMS. The NMS or SNMP traps receivers will then provide a comprehensive aggregation and reporting of events generated, thus helping administrator.

Audit:

Run the following command to check whether the SNMP traps receivers are configured:
CLI:

```
Hostname> show snmp traps receivers
Trap Receiver 10.7.26.5
Version v3
```

GUI:

```
Navigate to System Management > SNMP  >  Trap Receivers Settings
Verify Trap Receiver is configured.
```

Remediation:

Run the following command to Configure the SNMP traps receivers.
CLI:

```
Hostname> add snmp traps receiver 10.10.168.86 version v3
```

GUI:

```
Navigate to System Management > SNMP > Trap Receivers Setting > Add > Add IP
Address Version details.
```

Default Value:

Not Configured

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.3 NTP

2.3.1 Ensure NTP is enabled and IP address is set for Primary and Secondary NTP server (Automated)

Profile Applicability:

- Level 1

Description:

These settings enable the use of primary and secondary NTP servers to provide redundancy in case of a failure involving the primary NTP server.

Rationale:

NTP enables the device to maintain accurate time and date when receiving updates from a reliable NTP server. Accurate timestamps are critical when correlating events with other systems, troubleshooting, or performing investigative work. Logs and certain cryptographic functions, such as those utilizing certificates, rely on accurate time and date parameters. In addition, rules referencing a Schedule object will not function as intended if the device's time and date are incorrect. For additional security, authenticated NTP can be utilized. If Symmetric Key authentication is selected, only SHA1 should be used, as MD5 is considered severely compromised.

Audit:

Run the following command to check the status of NTP.
CLI:

```
Hostname> show ntp active
Yes
```

Run the following command to verify the IP address is configured for Primary and Secondary NTP server.

```
Hostname> show ntp servers

IP Address               Type              Version
------------             -------          ---------------
10.10.22.124             Primary           3
192.169.1.238            Secondary         3
```

GUI:

```
Navigate to System Management > Time  >  Set Time and Date
```

Verify Set Time and Date automatically using Network Time Protocol (NTP) option is checked and Primary NTP server and secondary NTP server address is configured.

Remediation:

Run the following command to enable the NTP and configure the Primary & Secondary NTP server.
CLI:

```
Hostname> set ntp active on
Hostname> set ntp server primary ntpserver.time.com version 3
Hostname> set ntp server primary 10.22.13.33 version 3
```

GUI:

```
System Management > Time > Set Time and Date > Checked Set Time and Date
automatically using Network Time Protocol (NTP) and configured the Primary
NTP Server and Secondary NTP server
```

Default Value:

No

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.3.2 Ensure timezone is properly configured (Automated)

Profile Applicability:

- Level 1

Description:

Sets the local time zone information so that the time displayed by the device is more relevant to those who are viewing it.

Rationale:

Having a correct time set on the device is important for two main reasons. The first reason is that digital certificates compare this time to the range defined by their Valid From and Valid To fields to define a specific validity period. The second reason is to have relevant time stamps when logging information. Whether you are sending messages to a Syslog server, sending messages to an SNMP monitoring station, or performing packet captures, timestamps have little usefulness if you cannot be certain of their accuracy.

Audit:

Run the following command to verify the Timezone.
CLI:

```
Hostname> show timezone
Time Zone: Asia/Kolkata (GMT +05:30)
```

GUI:

```
Navigate to System Management > Time  >  Set Timezone
```

Remediation:

Run the following command to Configure the Timezone used by the enterprise (GMT, UTC, EDT, PST).
CLI:

```
Hostname> set timezone Asia / Kolkata
```

GUI:

```
System Management > Time > Set Time Zone > Time Zone
```

Default Value:

Time Zone: America/New_York (GMT -05:00)

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.4 Backup

2.4.1 Ensure 'System Backup' is set. (Automated)

Profile Applicability:

- Level 1

Description:

List last-successful backup which is taken either locally or on a remote server. The backup can be taken locally on the device and also on a remote server via FTP, tftp or scp. The backup which is taken last is marked with (latest) in backup type.

Rationale:

The backup helps in restoring the configuration in the case of system failure or corruption or in the condition of device replacement.

Audit:

Run the following command to verify the last successful backup.
CLI:

```
Hostname>show backup last-successful
Backup Type: local ( latest )
Backup file location: /var/log/CPbackup/backups/backup_gw-
Checkpoint_28_Dec_2015_15_46.tgz
Backup process finished in 00:19 seconds
Backup Date: 28-Dec-2015 15:46:43
```

GUI:

```
Navigate to Maintenance > System Backup
```

Remediation:

Run the following command to Configure the backup.
CLI:

```
To take the backup local on the device.
Hostname> add backup local

To take the backup of FTP or SCP server.
Hostname>add backup [ftp|scp] ip [IP Address] path [Path to store backup]
username [Username] password [Password]

To take the backup on tftp server.
Hostname>add backup tftp [IP address of tftp server]
```

GUI:

```
Navigate to Maintenance > System Backup  >  Backup > Select (This appliance |
SCP Server | FTP Server | TFTP Server)
```

Default Value:

Not Configured

CIS Controls:

Version 7

5.2 Maintain Secure Images

Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.

5.5 Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

2.4.2 Ensure 'Snapshot' is set (Automated)

Profile Applicability:

- Level 1

Description:

An image of the system partition creates when takes the snapshots, includes all the configuration settings, Operating System and Checkpoint files. The locally stored firewall logs are not stored in the snapshots, as log partition is not included in the Snapshots. Snapshots can be restored on the same hardware on which it takes or on the same configuration hardware.

Rationale:

Snapshots are critical to system recovery in the event of a System crash.

Audit:

Run the following command to verify the list of snapshots taken on the system,
CLI:

```
Hostname>show snapshots
Restore points:
---------------
monthlysnapshot

Creation of an additional restore point will need 6.272G
Amount of space available for restore points is 7.34G
```

GUI:

```
Navigate to Maintenance > Snapshot Management
```

Remediation:

Run the following command to take the snapshot.
CLI:

```
To take the snapshot run the following command on the device.
Hostname> add snapshot [snapshot_name]
```

GUI:

```
Navigate to Maintenance > Snapshot Management > New
Provide the Name and description for the snapshot
```

Default Value:

Not Configured

CIS Controls:

Version 7

5.3 Securely Store Master Images

Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.

2.4.3 Configuring Scheduled Backups (Manual)

Profile Applicability:

- Level 1

Description:

The backup can be scheduled to take daily, weekly or monthly. The backup can be taken locally on the device and also on a remote server via FTP, tftp or scp. The backup which is taken last is marked with (latest) in backup type.

Rationale:

The backup helps in restoring the configuration in the case of system failure or corruption or in the condition of device replacement.

Audit:

GUI:

```
Navigate to Maintenance > System Backup > Scheduled Backup
```

Remediation:

GUI:

```
Navigate to Maintenance > System Backup > Scheduled Backup > Add Scheduled
Backup
Provide the Backup Type and Backup Schedule as per organization's policy.
```

CIS Controls:

Version 7

5.3 Securely Store Master Images

Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.

2.5 Authentication Settings

2.5.1 Ensure CLI session timeout is set to less than or equal to 10 minutes (Automated)

Profile Applicability:

- Level 1

Description:

Set the CLI Session Timeout value for device management to 10 minutes or less to automatically close inactive sessions.

Rationale:

An unattended computer with an open administrative session to the device could allow an unauthorized user access to the firewall's management interface

Audit:

Run the following command to check Inactivity Timeout for Command Line is set to 10 or less.
CLI:

```
Hostname>show inactivity-timeout
10
```

GUI:

```
Navigate to System Management > Session > Command Line Shell  >  Inactivity
Timeout - Set to 10 or less
```

Remediation:

Run the following command to Configure the Inactivity Timeout for Command Line.
CLI:

```
Hostname> set inactivity-timeout 10
```

GUI:

```
Navigate to System Management > Session > Command Line Shell  >  Inactivity
Timeout - Set to 10 or less
```

Default Value:

10

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.5.2 Ensure Web session timeout is set to less than or equal to 10 minutes (Automated)

Profile Applicability:

- Level 1

Description:

Set the WebUI Session Timeout value for device management to 10 minutes or less to automatically close inactive sessions.

Rationale:

An unattended computer with an open administrative session to the device could allow an unauthorized user access to the firewall's management interface

Audit:

Run the following command to check Inactivity Timeout for Web UI is set to 10 or less.
CLI:

```
Hostname> show web session-timeout
WebSessionTimeout 10
```

GUI:

```
Navigate to System Management > Session > Web UI  >  Inactivity Timeout - Set
to 10 or less
```

Remediation:

Run the following command to Configure the Inactivity Timeout for Web UI.
CLI:

```
Hostname> set web session-timeout 10
```

GUI:

```
Navigate to System Management > Session > Web UI  >  Inactivity Timeout - Set
to 10 or less
```

Default Value:

10

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.5.3 Ensure Client Authentication is secured. (Automated)

Profile Applicability:

- Level 1

Description:

Client Authentication allows a user and device to authenticate to the firewall and inherit pre-configured firewall rules for a set amount of time. By default, these connections are unencrypted yet can travel over unsecured networks. It is recommended that all Client Authentication connections be made using the HTTPS configuration. This both uniquely identifies the gateway and keeps the authentication credentials from being copied when going over the network.

Rationale:

The Client Authentication is used to authenticate a user or device to the firewall and by default, it works on HTTP port 900 and telnet port 259. The setting is stored in $FWDIR/conf/fwauthd.conf file. HTTP and telnet both are non-secure plaintext protocol and there is a number of published vulnerabilities, including the possibility of information disclosure and unauthorized access to the host system, which could permit sensitive data to be compromised. HTTPS configuration for all Client Authentication connections helps in identifying the gateway and keeps the authentication credentials from being copied when passes through the network.

Audit:

Verify telnet is disabled for Client Authentication.

```
Verify following lines are commented out or not present in
$FWDIR/conf/fwauthd.conf file.
259    fwssd       in.aclientd     wait    259
```

Verify Secure HTTP is used for Client Authentication.

```
Verify following lines have SSL setting enabled in $FWDIR/conf/fwauthd.conf.

900     fwssd       in.ahclientd    wait    900 ssl:defaultCert
```

Remediation:

Comment out or remove the following line from $FWDIR/conf/fwauthd.conf file, or disable the telnet service listening on port 259 by default, write a rule that prevents connections to the daemon in the rulebase.

```
#259    fwssd       in.aclientd     wait    259
```

Edit the following line to include SSL setting in $FWDIR/conf/fwauthd.conf file.

```
900     fwssd       in.ahclientd    wait    900 ssl:defaultCert
```

Default Value:

259 fwssd in.aclientd wait 259 900 fwssd in.ahclientd wait 900

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.5.4 Ensure Radius or TACACS+ server is configured (Automated)

Profile Applicability:

- Level 1

Description:

Configured the TACACS-Servers or Radius server for central authentication.

Rationale:

Authentication, authorization and accounting (AAA) scheme provide an authoritative source for managing and monitoring access for devices.

Audit:

Run the following command to check TACACS+ server status and TACACS+ servers list.
CLI:

```
Hostname> show aaa tacacs-servers state
Hostname> show aaa tacacs-servers list
```

GUI:

```
Navigate to User Management > Authentication Servers > TACACS+ configuration
> Enable TACACS+ authentication

Navigate to User Management > Authentication Servers > TACACS+ configuration
> Enable TACACS+ Servers
```

Run the following command to check radius servers list.
CLI:

```
Hostname> show aaa radius-servers list
```

GUI:

```
Navigate to User Management > Authentication Servers > Radius Servers
```

Remediation:

run the following command to enable and add TACACS+ servers.
CLI:

```
Hostname> set aaa tacacs-servers state on
Hostname> add aaa tacacs-servers priority <priority_value> server
<IP_Address> key <Key> timeout <timeout_value>
```

GUI:

```
Navigate to User Management > Authentication Servers > TACACS+ configuration
> Ensuere Enable TACACS+ authentication is checked

Navigate to User Management > Authentication Servers > TACACS+ configuration
> Enable TACACS+ Servers > Add Provide <Server_IP_Address>, <Priority> and
<Timeout>.
```

Run the following command to enable and add Radius servers.
CLI:

```
Hostname>add aaa radius-servers priority <priority_value> host <IP_Address>
secret <Key>  port <Port_number> timeout <timeout_value>
```

GUI:

```
Navigate to User Management > Authentication Servers > Radius Servers > Add
Provide <Server_IP_Address>, <Priority>, <UDP_Port> and <Timeout>.
```

Default Value:

Not Configured

CIS Controls:

Version 7

5.4 Deploy System Configuration Management Tools

Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

2.5.5 Ensure allowed-client is set to those necessary for device management (Automated)

Profile Applicability:

- Level 2

Description:

Permit only the necessary IP addresses to be used to manage the device.

Rationale:

Management access to the device should be restricted to the IP addresses or subnets used by firewall administrators. Permitting management access from other IP addresses increases the risk of unauthorized access through password guessing, stolen credentials, or other means.

Audit:

Run the following command to verify the Device access restrictions. Verify IP Addresses in allowed-client is limited to those necessary for device management.
CLI:

```
Hostname> show allowed-client all
Type                    Address                                 Mask Length

Host                    Any
Host                    10.22.2.1
Network                 172.16.31.0                             24
```

GUI:
Navigate to System Management > Host Access > Allowed Hosts

Remediation:

Run the following command to remove the IP Address or Network from allowed-client list.
CLI:

```
Hostname> delete allowed-client host (ipv4-address | ipv6-address) <IP
Address>
Hostname> delete allowed-client network (ipv4-address | ipv6-address)
<Network>
```

GUI:

```
Navigate to System Management > Host Access > Allowed Hosts > Select and
Delete the not required IP address or Network
```

Default Value:

Any

CIS Controls:

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

2.6 Logging

2.6.1 Ensure mgmtauditlogs is set to on (Automated)

Profile Applicability:

- Level 1

Description:

The mgmtauditlogs specifies if the Gaia sends the Gaia audit logs (for configuration changes that authorized users make) to a Check Point Management Server.

Rationale:

The mgmtauditlogs enables the logging functionality for configuration change done by the user. In Gaia os, we can export the Syslog messages from security gateway to Syslog server or security management server, and it can be reviewed as normal logs in SmartView Tracker. This enables organizations to monitor and analyze configuration change made by users.

Audit:

Run the following command to verify the mgmtauditlogs.
CLI:

```
Hostname> show syslog mgmtauditlogs
Sending audit logs to Management Server is enabled
```

GUI:

```
Navigate to System Management > System Logging > System Logging
Verify Send audit logs to management server upon successful configuration is
checked
```

Remediation:

Run the following command to enable the mgmtauditlogs.
CLI:

```
Hostname> set syslog mgmtauditlogs on
```

GUI:

```
Navigate to System Management > System Logging > System Logging
checked the Send audit logs to management server upon successful
configuration
```

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

2.6.2 Ensure auditlog is set to permanent (Automated)

Profile Applicability:

- Level 1

Description:

The auditlog specifies if the Gaia saves the logs for configuration changes that authorized users have done.

Rationale:

The auditlogs defines how it saves the configuration change logs. The configuration change log helps organizations to monitor and analyze configuration change made by users.

Audit:

Run the following command to verify the auditlog.
CLI:

```
Hostname> show syslog auditlog
permanent
```

GUI:

```
Navigate to System Management > System Logging > System Logging
Verify Send audit logs to syslog upon successful configuration is checked
```

Remediation:

Run the following command to enable the auditlog.
CLI:

```
Hostname> set syslog auditlog permanent
```

GUI:

```
Navigate to System Management > System Logging > System Logging
checked the Send audit logs to syslog upon successful configuration
```

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

2.6.3 Ensure cplogs is set to on (Automated)

Profile Applicability:

- Level 1

Description:

The cplogs specifies if the Gaia sends the Gaia system logs to a Check Point Management Server:

Rationale:

Audit:

Run the following command to verify the cplogs.
CLI:

```
Hostname> show syslog cplogs
Sending syslog syslogs to CheckPoint's logs is disabled
```

GUI:

```
Navigate to System Management > System Logging > System Logging
Verify Send Syslog messages to management server is checked
```

Remediation:

Run the following command to enable the cplogs.
CLI:

```
Hostname> set syslog cplogs on
```

GUI:

```
Navigate to System Management > System Logging > System Logging
checked the Send Syslog messages to management server
```

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

3 Firewall Secure Settings

3.1 Enable the Firewall Stealth Rule (Automated)

Profile Applicability:

- Level 2

Description:

Create a rule to drop Any Service from Any Source or Any VPN that attempts to connect to the gateway.

Rationale:

The stealth rule will limit access to the gateway to the control and service connections enabled as part of the design. As such, it is very important to enable access to the gateway as its role changes, for example, become a client VPN gateway. Another common example is enabling Client Authentication. If ports TCP 259 and 900 are not opened (or if you change the ports in the conf file), access will not work. Organizations with many Check Point gateways may want to document each gateway and the Check Point services it is intended and configured to accept.

Audit:

Login to the Management Server via SmartConsole and create or edit the stealth rule and make sure it is on top of all rules and only allowed sources and services are allowed to access the Gateway.

Remediation:

Login to the Management Server via SmartDashboard and create or edit the stealth rule, allowed only required IP address to manage the gateway and make sure it is on top of all rules.

CIS Controls:

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

3.2 Configure a Default Drop/Cleanup Rule (Automated)

Profile Applicability:

- Level 2

Description:

Ensure that the final rule in the rulebase explicitly drops all services, destinations, etc not specifically allowed in the previous rules. It is important that any access not explicitly allowed be explicitly dropped.

Rationale:

The Clean up rule is necessary to block all the traffic which is not allowed by earlier rules in the firewall. Ideally, Clean up rule be at the bottom in the Firewall rule base. By default an Implied Rule in Checkpoint firewall which does the same thing, but logging is not enabled for this rule.

Audit:

Verify the last rule is present in the rulebase which is denying all traffic from any source to any destination.

Remediation:

Create or edit the last rule in the rulebase which is denying all traffic from any source to any destination.

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

12.3 Deny Communications with Known Malicious IP Addresses

Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries,.

12.4 Deny Communication over Unauthorized Ports

Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

3.3 Use Checkpoint Sections and Titles (Manual)

Profile Applicability:

- Level 1

Description:

Use Sections to organize rules into related groups, whenever possible. Set each off with a descriptive Section Title.

Rationale:

Rulebase clarity helps all workers and reviewers. By organizing rules, inserting new rules is easier, and all can see the relationships among rules.

Audit:

Verify each rule has a description added and sections are used as per the requirement.

Remediation:

Add a description for each rule.

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices
Maintain standard, documented security configuration standards for all authorized network devices.

3.4 Ensure Hit count is Enable for the rules (Automated)

Profile Applicability:

- Level 2

Description:

The Hit Count setting shows the number of hits for the rules if enabled. When a new connection crosses a Firewall, hits are incremented for the matching rule.

Rationale:

The Hit Count is a very useful feature which helps in finding the unused rules, which can be reviewed and removed or update the rules accordingly as per the requirement.

Audit:

Go to the following path in Smart Console and verify Enable Hit Count is enabled.

```
Navigate to Global Properties > Hit Count
Verify 'Enable Hit Count' is checked
```

Remediation:

Go to the following path in Smart Console and Enable the Enable Hit Count setting.

```
Navigate to Global Properties > Hit Count
Checked the 'Enable Hit Count' setting
```

CIS Controls:

Version 7

11.2 Document Traffic Configuration Rules

All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

3.5 Ensure no Allow Rule with Any in Destination filed present in the Firewall Rules (Automated)

Profile Applicability:

- Level 2

Description:

The Firewall Rules with Any in Source field allows all the IP Addresses of the Network to access the specified destination configured in the Firewall rules for specific services.

Rationale:

Ideally, the traffic should be explicitly allowed from specific Source to specific Destination for the required services. This provides better control over the traffic passes through the firewall and reduce the chances of an exploit because of service misconfiguration.

Audit:

Verify there are no allowed rules present in the firewall which has Any used in the Source field. If there is any such rule present in the firewall, it should have a business justification and also it should be documented.

Remediation:

Delete the rule from the firewall which has Any used in the Source field.

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices
Maintain standard, documented security configuration standards for all authorized network devices.

3.6 Ensure no Allow Rule with Any in Source filed present in the Firewall Rules (Automated)

Profile Applicability:

- Level 2

Description:

The Firewall Rules with Any in the Destination field allows accessing all the IP Addresses of Network from specified Sources configured in the Firewall rules for specific services.

Rationale:

Ideally, the traffic should be explicitly allowed from the specific Source to specific Destination for the required services. This provides better control over the traffic passes through the firewall and reduce the chances of an exploit because of service misconfiguration.

Audit:

Verify there are no allowed rules present in the firewall which has Any used in the Destination field. If there is any such rule present in the firewall, it should have a business justification and also it should be documented.

Remediation:

Delete the rule from the firewall which has Any used in the Destination field.

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

3.7 Ensure no Allow Rule with Any in Services filed present in the Firewall Rules (Automated)

Profile Applicability:

- Level 2

Description:

The Firewall Rules with Any in the Service field allows accessing all the Services from specified Source to specified Destination configured in the Firewall rules.

Rationale:

There are many services like telnet, FTP, TFTP which are having many security issues. Hackers can take advantage of these services to gain the credentials, access to the systems or they can use these services for DoS attacks. These services need to be configured as per the needs of the business.

Audit:

Verify there are no allowed rules present in the firewall which has Any used in the Service field.

Remediation:

Delete the rule from the firewall which has Any used in the Service field.

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

3.8 Logging should be enable for all Firewall Rules (Manual)

Profile Applicability:

- Level 2

Description:

The Track Field defines how the events of the rule are captured.

Rationale:

The event log of firewall rules helps in identifying the allowed and blocked traffic and also helps in troubleshooting and forensic investigation. It is always good to enable logging for all the firewall rules, but by logging multiple firewall rules results in a huge log files, which requires huge disk space and management operations. Logs play an important role in security auditing, incident response, system maintenance and forensic investigation, and should be configured as per the business needs.

Audit:

Verify all Track field in all firewall rules should have set to Log.

Remediation:

Set the Track field to Log in all firewall rules.

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

11.2 Document Traffic Configuration Rules
All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

3.9 Review and Log Implied Rules (Automated)

Profile Applicability:

- Level 2

Description:

Rulebase clarity helps all workers and reviewers. Stating rules explicitly in the rulebase makes policy analysis and review significantly easier. Select the ‗Log Implied Rules' to ensure all understand when connectivity is denied or allowed through a subtle Implied Rule.

Rationale:

It is recommended to define rules explicitly rather than state them implicitly in the Implied Rules section of Global Properties. If Implied Rules are used, configure logging for implied rules by accessing the ‗Global Properties' dialog box.

Audit:

Go to the following path in the Smart Console and verify Log Implied Rules is enabled.

```
Navigate to Global Properties > Firewall
Verify Log Implied Rules is enabled
```

Remediation:

Go to the following path in the Smart Console and enabled the Log Implied Rules.

```
Navigate to Global Properties > Firewall
Enable the Log Implied Rules
```

Default Value:

Disabled

CIS Controls:

Version 7

6.7 Regularly Review Logs
On a regular basis, review logs to identify anomalies or abnormal events.

3.10 Ensure Drop Out of State TCP Packets is enabled (Automated)

Profile Applicability:

- Level 2

Description:

The Drop out of state TCP Packets setting will drop the out of state or non-synchronized TCP Packets for which firewall does not have a matching state table entry.

Rationale:

Bypassing security setting Drop out of state TCP Packets means that non-synchronized packets which do not belong to an established connection in the Firewall's connections table or non-TCP compliant traffic will not be dropped. This can be potentially used by attackers for Denial-of-service attacks by flooding non-synchronized TCP packets.

Audit:

Go to the following path and verify Drop Out of State TCP Packets and Log on Drop is enabled.

```
SmartConsole > Global Properties > Stateful Inspection
Verify Drop Out of State TCP Packets and Log on Drop is checked.
```

Remediation:

Go to the following path and checked the Drop Out of State TCP Packets and Log on Drop.

```
SmartConsole > Global Properties > Stateful Inspection
Checked the Drop Out of State TCP Packets and Log on Drop
```

Default Value:

Enabled

CIS Controls:

Version 7

12.1 Maintain an Inventory of Network Boundaries
Maintain an up-to-date inventory of all of the organization's network boundaries.

3.11 Ensure Drop Out of State ICMP Packets is enabled (Automated)

Profile Applicability:

- Level 2

Description:

This drops the out of state ICMP packets.

Rationale:

The Firewall verifies that each ICMP reply packet matches a previous request, and each ICMP error matches an existing connection. Out of State ICMP packets should be dropped and logged.

Audit:

Go to the following path and verify Drop Out of State ICMP Packets and Log on Drop is enabled.

```
SmartConsole > Global Properties > Stateful Inspection
Verify Drop Out of State ICMP Packets and Log on Drop is checked.
```

Remediation:

Go to the following path and checked the Drop Out of State ICMP Packets and Log on Drop.

```
SmartConsole > Global Properties > Stateful Inspection
Checked the Drop Out of State ICMP Packets and Log on Drop
```

Default Value:

Enabled

CIS Controls:

Version 7

12.1 Maintain an Inventory of Network Boundaries
Maintain an up-to-date inventory of all of the organization's network boundaries.

3.12 Ensure Anti-Spoofing is enabled and action is set to Prevent for all Interfaces (Automated)

Profile Applicability:

- Level 2

Description:

The Anti-Spoofing is a technique which is used to identify and drop the packets that have a false source IP address. The Anti-Spoofing detect mode is only monitor the Anti-spoofing events while prevent mode drops the Anti-spoofing events.

Rationale:

Hackers change the packet's IP address and make a packet which looks like it is from a trusted source. If your network is not protected with the IP-spoofing, hackers can exploit the vulnerability to gain access to the network.

Audit:

For all managed gateways verify that Anti-Spoofing is enabled, Anti-Spoofing action is set to Prevent and tracking is set to Log.

```
SmartConsole > Gateways & Servers > select managed Gateway > Network
Management > Select each interface > General > Modify
- Verify Perform Anti-Spoofing based on Interface topology is checked
- Verify Anti-Spoofing action is set to Prevent
- Verify Spoof Tracking is set to Log
```

Remediation:

For all managed gateways enable the Anti-Spoofing, set the Anti-Spoofing action to Prevent and set the tracking to Log.

```
SmartConsole > Gateways & Servers > select managed Gateway > Network
Management > Select each interface > General > Modify
- Checked the Perform Anti-Spoofing based on Interface topology
- Set the Anti-Spoofing action to Prevent
- Set the Spoof Tracking to Log
```

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

12.2 Scan for Unauthorized Connections across Trusted Network Boundaries

Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.

3.13 Ensure Disk Space Alert is set (Automated)

Profile Applicability:

- Level 1

Description:

This is used to generate the Log and Alert when disk space reaches the configured limit.

Rationale:

The device might get inaccessible and the logs are not getting stored once the disk space reaches to the maximum capacity. It is imperative that organizations log critical infrastructure appropriately, store and archive these logs in a central location

Audit:

Verify Disk Space Alert is configured if disk space goes beyond the organization defined configured limit.

```
SmartConsole > Gateways & Servers > Select each Gateway > Logs > Local
Storage
* When disk space is below is checked and value MBytes or Percentage is
configured
* Issue alert is set to Log, Popup Alert, Mail or SNMP trap alert.
```

Remediation:

Go to the following path and configured the Disk Space Alert.

```
SmartConsole > Gateways & Servers > Select each Gateway > Logs > Local
Storage

* Checked the When disk space is below and value MBytes or Percentage is
configured as per the Organization Policy.
* Set the Issue alert to Log, Popup Alert, Mail or SNMP trap alert.
```

CIS Controls:

Version 7

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

3.14 Ensure Accept RIP is not enabled (Automated)

Profile Applicability:

- Level 2

Description:

The Accept RIP is a Global property setting which you can set either to accept or reject the RIP packets which is using UDP Port 520. RIP maintains information about reachable systems and routes to those systems.

Rationale:

The security policy is made up of rules in the Firewall Rule Base. Other than the rules defined by the administrator, The Check Point Security Gateway also creates Implied Rules, which are defined in the Firewall Global Properties. The Check Point Security Gateway places the implied rules first, last, or before last in the Firewall Rule Base. The administrator can decide whether or not to log implied rules.

First — The Implicit rule will be placed before the explicit rules. Last — The Implicit rule will be placed after the explicit rules. Before Last — The Implicit rule will be placed before the last explicit rule.

Audit:

Verify Accept RIP under Global Properties is not enabled.

```
SmartConsole > Gateways & Servers > select each Gateway > Firewall
Veiry Accept RIP is unchecked.
```

Remediation:

Go to the following path and Configured the Accept RIP.

```
SmartConsole > Gateways & Servers > select each Gateway > Firewall
Unchecked the Accept RIP
```

Default Value:

Disabled

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

3.15 Ensure Accept Domain Name over TCP (Zone Transfer) is not enabled (Automated)

Profile Applicability:

- Level 2

Description:

The 'Domain Name Over TCP (Zone transfer)' is a global property setting which is used to allow or reject all the TCP-type DNS packets to and from anywhere. These rules are considered as rule zero which are executed before any user-defined rules.

Rationale:

If this rule is enabled, it accepts Domain Name (DNS) queries and replies over TCP, to allow downloading of the domain name-resolving tables used for zone transfers between servers. For clients, DNS over TCP is only used if the tables to be transferred are very large. The security policy is made up of rules in the Firewall Rule Base. Other than the rules defined by the administrator, The Check Point Security Gateway also creates Implied Rules, which are defined in the Firewall Global Properties. The Check Point Security Gateway places the implied rules first, last, or before last in the Firewall Rule Base. The administrator can decide whether or not to log implied rules.

- First > The Implicit rule will be placed before the explicit rules.
- Last > The Implicit rule will be placed after the explicit rules.
- Before Last > The Implicit rule will be placed before the last explicit rule.

Audit:

Verify Accept Accept Domain Name over TCP (Zone Transfer) under Global Properties is not enabled.

```
SmartConsole > Gateways & Servers > select each Gateway > Firewall
Veiry Accept Accept Domain Name over TCP (Zone Transfer) is unchecked.
```

Remediation:

Go to the following path and Configured the Accept Accept Domain Name over TCP (Zone Transfer).

```
SmartConsole > Gateways & Servers > select each Gateway > Firewall
Unchecked the Accept Accept Domain Name over TCP (Zone Transfer)
```

CIS Controls:

Version 7

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes

Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

3.16 Ensure Accept Domain Name over UDP (Queries) is not enabled (Automated)

Profile Applicability:

- Level 2

Description:

The 'Domain Name Over UDP (Queries)' is a global property setting which is used to allow or reject all the UDP-type DNS packets to and from anywhere. These rules are considered as rule zero which are execute before any user-defined rules.

Rationale:

If this rule is set to enable it allows the DNS traffic to pass over the firewall without any control. The security policy is made up of rules in the Firewall Rule Base. Other than the rules defined by the administrator, The Check Point Security Gateway also creates Implied Rules, which are defined in the Firewall Global Properties. The Check Point Security Gateway places the implied rules first, last, or before last in the Firewall Rule Base. The administrator can decide whether or not to log implied rules.

- First > The Implicit rule will be placed before the explicit rules.
- Last > The Implicit rule will be placed after the explicit rules.
- Before Last > The Implicit rule will be placed before the last explicit rule.

Audit:

Verify Accept Accept Domain Name over UDP (Queries) under Global Properties is not enabled.

```
SmartConsole > Gateways & Servers > select each Gateway > Firewall
Verify Accept Accept Domain Name over UDP (Queries) is unchecked.
```

Remediation:

Go to the following path and Configured the Accept Accept Domain Name over UDP (Queries).

```
SmartConsole > Gateways & Servers > select each Gateway > Firewall
Unchecked the Accept Accept Domain Name over UDP (Queries)
```

CIS Controls:

Version 7

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes

Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

3.17 Ensure Accept ICMP Requests is not enabled (Automated)

Profile Applicability:

- Level 2

Description:

The 'Accept ICMP requests' is a global property setting which is used to allow the ICMP requests from any location. ICMP is used to send control messages (for example, ping, destination unreachable, source quench, route change) to other systems. These rules are considered as rule zero which are executed before any user-defined rules.

Rationale:

If this rule is enabled, it allows the echo requests, timestamp requests, information requests, and mask requests. This can be used by a malicious user to create a denial of service condition by flooding the network with broadcast echo requests and revealing mask request information. The security policy is made up of rules in the Firewall Rule Base. Other than the rules defined by the administrator, The Check Point Security Gateway also creates Implied Rules, which are defined in the Firewall Global Properties. The Check Point Security Gateway places the implied rules first, last, or before last in the Firewall Rule Base. The administrator can decide whether or not to log implied rules.

- First > The Implicit rule will be placed before the explicit rules.
- Last > The Implicit rule will be placed after the explicit rules.
- Before Last > The Implicit rule will be placed before the last explicit rule.

Audit:

Verify Accept Accept ICMP Requests under Global Properties is not enabled.

```
SmartConsole > Gateways & Servers > select each Gateway > Firewall
Verify Accept Accept ICMP Requests is unchecked.
```

Remediation:

Go to the following path and Configured the Accept Accept ICMP Requests.

```
SmartConsole > Gateways & Servers > select each Gateway > Firewall
Unchecked the Accept Accept ICMP Requests
```

3.18 Ensure Allow bi-directional NAT is enabled (Automated)

Profile Applicability:

- Level 2

Description:

Allow bi-directional NAT applies to automatic NAT rules in the NAT Rule Base and allows two automatic NAT rules to match a connection. Without Bidirectional NAT, only one automatic NAT rule can match a connection.

Rationale:

When NAT is defined for a network object, an automatic NAT rule is generated which performs the required translation. If there are two such objects and one is the source of a connection and the other the destination, then without Bidirectional NAT, only one of these objects will be translated, because only one of the automatically generated NAT rules will be applied, and so a connection between the two objects will only be allowed in one direction. With Bidirectional NAT, both automatic NAT rules are applied, and both objects will be translated, so connections between the two objects will be allowed in both directions.

Audit:

Verify Allow bi-directional NAT under Global Properties is enabled.

```
SmartConsole > Gateways & Servers > select each Gateway > NAT - Network
Address Translation
Verify Allow bi-directional NAT is checked.
```

Remediation:

Go to the following path and Configured the Allow bi-directional NAT.

```
SmartConsole > Gateways & Servers > select each Gateway > NAT - Network
Address Translation
Unchecked the Allow bi-directional NAT
```

CIS Controls:

Version 7

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes

Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

3.19 Ensure Automatic ARP Configuration NAT is enabled (Automated)

Profile Applicability:

- Level 2

Description:

Proxy ARP is a mechanism that allows the configuration of a Gateway to respond to ARP requests on behalf of other hosts.

Rationale:

Automatic ARP configuration ensures that ARP requests for a translated (NATed) machine, network or address range are answered by the Check Point Security Gateway. This option removes the requirement for manual ARP configuration for automatic NAT rules (using the arp command in Unix or the local.arp file in Windows).

The command fw ctl arp displays the ARP proxy table on Check Point Security Gateways that run on Windows. On Unix, use the arp -a command.

Audit:

Verify Automatic ARP Configuration NAT under Global Properties is enabled.

```
SmartConsole > Gateways & Servers > select each Gateway > NAT - Network
Address Translation
Verify Automatic ARP Configuration NAT is checked.
```

Remediation:

Go to the following path and Configured the Automatic ARP Configuration NAT.

```
SmartConsole > Gateways & Servers > select each Gateway > NAT - Network
Address Translation
Unchecked the Automatic ARP Configuration NAT
```

CIS Controls:

Version 7

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

3.20 Ensure Logging is enabled for Track Options of Global Properties (Automated)

Profile Applicability:

- Level 1

Description:

This defines the system-wide logging and alerting of parameters.

Rationale:

This enables the logging and alerting for specific types of parameters.

VPN successful key exchange: specifies the action to be taken when VPN keys are successfully exchanged.

VPN packet handling errors: specifies the action to be taken when encryption or decryption errors occur. A log entry contains the action performed (Drop or Reject) and a short description of the error cause, for example, scheme or method mismatch.

VPN configuration & key exchange errors: specifies the action to be taken when logging configuration or key exchange errors occur, for example, when attempting to establish encrypted communication with a network object inside the same encryption domain.

IP Options drop: specifies the action to take when a packet with IP Options is encountered. The Check Point Security Gateway always drops these packets, but you can log them or issue an alert.

Administrative notifications: specifies the action to be taken when an administrative event (for example, when a certificate is about to expire) occurs.

SLA violation: specifies the action to be taken when an SLA violation occurs, as defined in the Virtual Links window.

Connection matched by SAM: specifies the action to be taken when a connection is blocked by SAM (Suspicious Activities Monitoring).

Dynamic object resolution failure: specifies the action to be taken when a dynamic object cannot be resolved.

Log every authenticated HTTP connection: specifies that a log entry should be generated for every authenticated HTTP connection.

Audit:

Verify Logging is set to Log or Popup Alert or Mail Alert or SNMP Trap Alert for the following events

```
SmartConsole > Global Properties > Log and Alert > Track Options
VPN successful key exchange
VPN packet handling errors
VPN configuration & key exchange errors
IP Options drop
Administrative Notification
Connection matched by SAM
Dynamic object resolution failure
Packet is incorrectly tagged
Packet tagging brute force attack

Verify Log every authenticated HTTP connection is enabled.
```

Remediation:

Logging is set to Log or Popup Alert or Mail Alert or SNMP Trap Alert for the following events

```
SmartConsole > Global Properties > Log and Alert > Track Options
VPN successful key exchange
VPN packet handling errors
VPN configuration & key exchange errors
IP Options drop
Administrative Notification
Connection matched by SAM
Dynamic object resolution failure
Packet is incorrectly tagged
Packet tagging brute force attack

Checked the  Log every authenticated HTTP connection.
```

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Password Policy**		
1.1	Ensure Minimum Password Length is set to 14 or higher (Automated)	☐	☐
1.2	Ensure Disallow Palindromes is selected (Automated)	☐	☐
1.3	Ensure Password Complexity is set to 3 (Automated)	☐	☐
1.4	Ensure Check for Password Reuse is selected and History Length is set to 12 or more (Automated)	☐	☐
1.5	Ensure Password Expiration is set to 90 days (Automated)	☐	☐
1.6	Ensure Warn users before password expiration is set to 7 days (Automated)	☐	☐
1.7	Ensure Lockout users after password expiration is set to 1 (Automated)	☐	☐
1.8	Ensure Deny access to unused accounts is selected (Automated)	☐	☐
1.9	Ensure Days of non-use before lock-out is set to 30 (Automated)	☐	☐
1.10	Ensure Force users to change password at first login after password was changed from Users page is selected (Automated)	☐	☐
1.11	Ensure Deny access after failed login attempts is selected (Automated)	☐	☐
1.12	Ensure Maximum number of failed attempts allowed is set to 5 or fewer (Automated)	☐	☐
1.13	Ensure Allow access again after time is set to 300 or more seconds (Automated)	☐	☐
2	**Device Setup**		
2.1	**General Settings**		
2.1.1	Ensure 'Login Banner' is set (Automated)	☐	☐
2.1.2	Ensure 'Message Of The Day (MOTD)' is set (Automated)	☐	☐
2.1.3	Ensure Core Dump is enabled (Automated)	☐	☐
2.1.4	Ensure Config-state is saved (Automated)	☐	☐
2.1.5	Ensure unused interfaces are disabled (Automated)	☐	☐
2.1.6	Ensure DNS server is configured (Automated)	☐	☐
2.1.7	Ensure IPv6 is disabled if not used (Automated)	☐	☐
2.1.8	Ensure Host Name is set (Automated)	☐	☐
2.1.9	Ensure Telnet is disabled (Automated)	☐	☐
2.1.10	Ensure DHCP is disabled (Automated)	☐	☐

2.2	**SNMP**		
2.2.1	Ensure SNMP agent is disabled (Automated)	☐	☐
2.2.2	Ensure SNMP version is set to v3-Only (Automated)	☐	☐
2.2.3	Ensure SNMP traps is enabled (Automated)	☐	☐
2.2.4	Ensure SNMP traps receivers is set (Automated)	☐	☐
2.3	**NTP**		
2.3.1	Ensure NTP is enabled and IP address is set for Primary and Secondary NTP server (Automated)	☐	☐
2.3.2	Ensure timezone is properly configured (Automated)	☐	☐
2.4	**Backup**		
2.4.1	Ensure 'System Backup' is set. (Automated)	☐	☐
2.4.2	Ensure 'Snapshot' is set (Automated)	☐	☐
2.4.3	Configuring Scheduled Backups (Manual)	☐	☐
2.5	**Authentication Settings**		
2.5.1	Ensure CLI session timeout is set to less than or equal to 10 minutes (Automated)	☐	☐
2.5.2	Ensure Web session timeout is set to less than or equal to 10 minutes (Automated)	☐	☐
2.5.3	Ensure Client Authentication is secured. (Automated)	☐	☐
2.5.4	Ensure Radius or TACACS+ server is configured (Automated)	☐	☐
2.5.5	Ensure allowed-client is set to those necessary for device management (Automated)	☐	☐
2.6	**Logging**		
2.6.1	Ensure mgmtauditlogs is set to on (Automated)	☐	☐
2.6.2	Ensure auditlog is set to permanent (Automated)	☐	☐
2.6.3	Ensure cplogs is set to on (Automated)	☐	☐
3	**Firewall Secure Settings**		
3.1	Enable the Firewall Stealth Rule (Automated)	☐	☐
3.2	Configure a Default Drop/Cleanup Rule (Automated)	☐	☐
3.3	Use Checkpoint Sections and Titles (Manual)	☐	☐
3.4	Ensure Hit count is Enable for the rules (Automated)	☐	☐
3.5	Ensure no Allow Rule with Any in Destination filed present in the Firewall Rules (Automated)	☐	☐
3.6	Ensure no Allow Rule with Any in Source filed present in the Firewall Rules (Automated)	☐	☐
3.7	Ensure no Allow Rule with Any in Services filed present in the Firewall Rules (Automated)	☐	☐
3.8	Logging should be enable for all Firewall Rules (Manual)	☐	☐
3.9	Review and Log Implied Rules (Automated)	☐	☐
3.10	Ensure Drop Out of State TCP Packets is enabled (Automated)	☐	☐

3.11	Ensure Drop Out of State ICMP Packets is enabled (Automated)	☐	☐
3.12	Ensure Anti-Spoofing is enabled and action is set to Prevent for all Interfaces (Automated)	☐	☐
3.13	Ensure Disk Space Alert is set (Automated)	☐	☐
3.14	Ensure Accept RIP is not enabled (Automated)	☐	☐
3.15	Ensure Accept Domain Name over TCP (Zone Transfer) is not enabled (Automated)	☐	☐
3.16	Ensure Accept Domain Name over UDP (Queries) is not enabled (Automated)	☐	☐
3.17	Ensure Accept ICMP Requests is not enabled (Automated)	☐	☐
3.18	Ensure Allow bi-directional NAT is enabled (Automated)	☐	☐
3.19	Ensure Automatic ARP Configuration NAT is enabled (Automated)	☐	☐
3.20	Ensure Logging is enabled for Track Options of Global Properties (Automated)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Jun 5, 2018	1.0.0 NEXT	_Listing Order, Status_ on **[section] 1.10 Apply latest Gaia OS patches** were updated.
Jan 8, 2019	1.1.0	ADD - Create subsection for Restricting Access (Ticket 6082)