CIS Benchmarks

CIS F5 Networks Benchmark

v1.0.0 - 11-01-2021

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

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for F5 Networks.
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 benchmark 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 F5 Networks family of products

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 intend to:

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

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount
  - acts as a 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:

Author
Omar Batis

Contributor
Darren Freidel

Recommendations

1 Accounts

1.1 Passwords

1.1.1 Ensure default password of root is not allowed (Automated)

Profile Applicability:

- Level 1

Description:

To assist users in changing default password for "root" account

Rationale:

Using Default passwords for 'root' access could cause a compromise to the overall system security

Impact:

Failure of changing default root's password brings high risk to the system as the root account might be abused by unauthorized users who would have full privilege on F5 systems

Audit:

```
Attempt to log in as root with default password
```

Remediation:

```
- Log in to the Configuration utility.
- For System, select Platform.
- Under User Administration, choose the Password box for either Root Account
or Admin Account.
- Enter the new password.
- Enter the same password in the Confirm box for the account that you chose
in step 3.
- Select Update.
- If you have updated the password for Admin Account, the system logs you out
of the Configuration
utility, and you must log in again using the new password.
```

References:

1. https://api-u.f5.com/support/kb-articles/K13121?pdf

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.2 Change Default Passwords Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●

1.1.2 Ensure default password of admin is not used (Automated)

Profile Applicability:

- Level 1

Description:

To assist users in changing default password for 'admin' account

Rationale:

Using Default passwords for 'admin' access could cause a compromise to the overall system security

Impact:

Failure of changing default root's password brings high risk to the system as the root account might be abused by unauthorized users who would have full privilege on F5 systems

Audit:

```
Attempt to log in as admin with default password
```

Remediation:

```
- Log in to the Configuration utility.
- For System, select Platform.
- Under User Administration, choose the Password box for either Root Account
or Admin Account.
- Enter the new password.
- Enter the same password in the Confirm box for the account that you chose
in step 3.
- Select Update.
- If you have updated the password for Admin Account, the system logs you out
of the Configuration
utility, and you must log in again using the new password.
```

References:

1. https://api-u.f5.com/support/kb-articles/K13121?pdf

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.2 Change Default Passwords Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●

1.1.3 Configure Secure Password Policy (Manual)

Profile Applicability:

- Level 1

Description:

To assist users in maintaining strong passwords, ensure that passwords are changed at appropriate intervals and new passwords to be used

Rationale:

Having a weak or non-existent password policy will allow users to use weak or easily cracked passwords.

Impact:

Without proper password management the users are more likely to select weak passwords or forget complex passwords. This can create security risks as these passwords make it easier for attackers to crack.

Audit:

```
Secure Password Enforcement
Enables or disables enforcement (character) restrictions, and a policy for
minimum password length and required characters. When you enable this
setting, the Configuration utility displays the Minimum Length and Required
Characters settings. The default value is Disabled prior to BIG-IP 14.0.0 and
Enabled after BIG-IP 14.0.0.

-Minimum Length
Specifies the minimum number of characters required for a password. The
default value is 6, and the system allows the range of values from 6 through
255. This setting appears in the Configuration utility, and the system only
enforces it when you enable the Secure Password Enforcement setting.

-Required Characters
Specifies the number of numeric, uppercase, lowercase, and other characters
required for a password. The default value for each character type is 0, and
the system allows the range of values from 0 through 127. This setting
appears in the Configuration utility, and the system only enforces it when
you enable the Secure Password Enforcement setting.

-Password Memory
Specifies, for each user account, the number of former passwords that the
BIG-IP system retains to prevent the user from reusing a recent password. The
default value is 0, and the system allows the range of values from 0 through
127.
```

```
-Minimum Duration
Specifies the minimum number of days before users can change their password.
The default value is 0, and the system allows the range of values from 0
through 255.

Note: Administrators cannot reset their passwords using the Configuration
utility while inside the Minimum Duration window.

-Maximum Duration
Specifies the maximum number of days that users' passwords are valid. The
default value is 99999, and the system allows the range of values from 1
through 99999. If a user does not change their password by the time they
reach the maximum duration, in versions prior to BIG-IP 13.1.0, an
administrator must change the user's password, and in BIG-IP 13.1.0 and
after, the user can reset their own password.

-Expiration Warning
Specifies the number of days prior to password expiration that the system
sends a warning message to a users. The default value is 7, and the system
allows the range of values from 1 to 255.

-Maximum Login Failures
Specifies the number of consecutive unsuccessful login attempts the system
allows before locking out the user. The default value is 0 where zero value
means it is disabled. The valid range is from 0 through 65535. Locked out
users must contact a system administrator to reinstate their access. For more
information about managing locked out user accounts, refer to K34556595:
Managing the login failures for a local user account on the BIG-IP system.
```

Remediation:

```
Configuring the password policy using the Configuration utility
1.      Log in to the Configuration utility.
2. Navigate to System > Users > Authentication.
3. Under Password Policy, locate the Secure Password Enforcement setting and
set it to meet below minimum requirements :

Configuring the password policy using tmsh
1. Log in to tmsh by typing the following command:
tmsh:
modify /auth password-policy


The minimum requirements :

- Secure Password Enforcement : Enabled
- Minimum Password Length is 12
- Required Lowercase is 1
- Required Uppercase is 1
- Required Numeric is 1
- Required Special Characters is 1
- Maximum Duration (in Days): 180
- Minimum Duration (in Days): 90
- Expiration Warning ( in days):14
- EnsurePassword Memory is 24
- Ensure Maximum Login Failures is 3
- User Lockout :  Automatically enable locked-out users after : 300 seconds

**Notice: Some settings can be done through Configuration Utility only while
others are done through tmsh only.**
```

References:

1. https://support.f5.com/csp/article/K15497

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.2 Change Default Passwords Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●
v7	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.		●	●

2 AAA

2.1 Ensure that Remote Radius is used for Authentication Only (Automated)

Profile Applicability:

- Level 2

Description:

To specify the authentication mechanism that F5 systems use for external (remote) users

Rationale:

Uncontrolled and illegitimate authentication could provide access to unauthorized users

Impact:

Uncontrolled and illegitimate authentication mechanism provides access to illegitimates remote users on the systems. It is important to make sure of the right Authentication mechanism used. Radius is configured as Authentication Only. Radius in turns query LDAP for remote users authentication and authorization.

Audit:

```
On Configuration utility:
System > Users > Authentication
Under Authentication : Check "Service Type"
```

Remediation:

```
1-Log in to the Configuration utility using the administrator account.

2-Navigate to System > Users > Authentication.

3-In the Authentication section, click Change.

4-Select Remote - RADIUS from the User Directory drop-down menu.

5-Define the RADIUS server configuration settings, including the port and
shared secret settings:

6- For "Service Type": select "Authentication Only"

7-Click Finished.
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.2 Ensure redundant remote authentication servers are configured (Manual)

Profile Applicability:

- Level 2

Description:

Having multiple points of authentication is important in the event that the primary remote authentication source goes down.

Rationale:

To make sure the redundant Radius servers are configured

Impact:

Having a single Authentication server reduce the availability for systems operators and admins to perform their tasks and support when the Radius server is down

Audit:

```
-On Configuration utility:
System > Users > Authentication
-You should see RADIUS configuration for Primary server only.
```

Remediation:

```

1-Log in to the Configuration utility using the administrator account.

2-Navigate to System > Users > Authentication.

3-In the Authentication section, click Change.

4-Select Remote - RADIUS from the User Directory drop-down menu.

5-Define the RADIUS server configuration settings, including the port and
shared secret settings:

6-For "Service Type": select "Authentication Only"

7-This should be completed for Primary RADIUS server as well as for Secondary
RADIUS server.

8-Click Finished.
```

References:

1. https://support.f5.com/csp/article/K17403

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.3 Ensure that "Fallback to local" option is disabled for Remote Authentication Settings (Manual)

Profile Applicability:

- Level 2

Description:

To prevent the system from checking local DB for remote users authentication

Rationale:

Impact:

Though the impact might be low, it is a good practice to segregate remote users from local and to limit local users' usage.

Audit:

```
1. Log in to the Configuration utility.

2. Go to System > Users > Authentication.

3. Under Authentication , you should see Fallback to Local "Disabled"
```

Remediation:

```
1. Log in to the Configuration utility.

2. Go to System > Users > Authentication.

3. Select Change.

4. Select the Fallback to Local check box.

5. Select Finished.
```

References:

1. https://support.f5.com/csp/article/K67025432

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	4.6 Use of Dedicated Machines For All Administrative Tasks Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.			●

2.4 Ensure External Users' role is set to "No Access" (Automated)

Profile Applicability:

- Level 2

Description:

To set a default role for remote users Authentication and authorization for remote users are handled by third party system

Rationale:

Impact:

Providing remote users with a preconfigured role might allow unauthorized access to these users.

Audit:

```
1. Log in to the Configuration utility.

2. Go to System > Users > Authentication.

3. Under External Users > Role : a predefined role is set
```

Remediation:

```
1. Log in to the Configuration utility.

2. Go to System > Users > Authentication.

3. Under External Users , click "Change".

4. Set Role to "No Access".
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	4.6 Use of Dedicated Machines For All Administrative Tasks Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.			●

2.5 Ensure External Users' has access to needed Partitions only (Automated)

Profile Applicability:

- Level 1

Description:

To limit access for remote users to needed partitions only granting a user access to "All Partitions" might provide the users unauthorized access.

Rationale:

Impact:

Though , there is one partition is configured currently on WD F5 systems (common) , It is a good practice to specify which partition the users allowed to access.

Audit:

```
1. Log in to the Configuration utility.

2. Go to System > Users > Authentication.

3. Under External Users > Partition Access , you can see no specific
partition is defined or it is set to "All"
```

Remediation:

```
1. Log in to the Configuration utility.

2. Go to System > Users > Authentication.

3. Under External Users , click "Change".

4. For Partition Access , specify which partitions are allowed for External
Users.
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	4.6 Use of Dedicated Machines For All Administrative Tasks Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.			●

2.6 Ensure External Users' Terminal Access is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

To prevent remote users from gaining terminal access

Rationale:

Audit:

```
1. Log in to the Configuration utility.

2. Go to System > Users > Authentication.

3. Under External Users >  you should see Terminal Access is set to "Enabled"
```

Remediation:

```
1. Log in to the Configuration utility.

2. Go to System > Users > Authentication.

3. Under External Users , click "Change".

4. Set Terminal Access as "Disabled"
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	4.6 Use of Dedicated Machines For All Administrative Tasks Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.			●

3 GUI Interface Management

3.1 Ensure 'Idle timeout' is less than or equal to 10 minutes for Configuration utility sessions (Automated)

Profile Applicability:

- Level 1

Description:

To set an idle timeout for GUI sessions

Rationale:

Unattended administrative sessions may provide illegal access to the device

Impact:

Indefinite or even long session timeout windows can increase the risk of attackers abusing abandoned sessions.

Audit:

On Configuration utility:

```
System > Preferences, Under Security settings...check the value of Idle Time
Before Automatic Logout
```

Remediation:

On Configuration utility:

```
System > Preferences, Under Security settings...set the value of Idle Time
Before Automatic Logout to 600 seconds
```

Default Value:

1200

References:

1. https://support.f5.com/csp/article/K9908

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2 Ensure access to Configuration utility by clients using TLS version 1.2 or later (Automated)

Profile Applicability:

- Level 1

Description:

TLSv1.2 should be used for GUI connections

Rationale:

Restricting the configuration utility to use TLS version 1.2 is recommended

Impact:

Weak security protocols may expose vulnerability by disclosing data through SSL/TLS sessions

Audit:

Through CLI access, type the following command:

```
tmsh list sys httpd ssl-protocol
```

The output should show only TLSv1.2

Remediation:

If the value is different, execute the following command to modify the protocol used to access GUI:

```
tmsh modify /sys httpd ssl-protocol "TLSv1.2"
tmsh save sys config
```

Default Value:

ssl-protocol "All -SSLv2 -SSLv3 -TLSv1"

References:

1. https://support.f5.com/csp/article/K02321234

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.3 Ensure access to Configuration utility is restricted to needed IP addresses only (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended to maintain secure access to the GUI by allowing only trusted IP addresses or range of IP addresses

Rationale:

Any compromised network device within enterprise network would gain illegal access to F5 configuration utility abusing existing unresolved vulnerabilities.

Impact:

Allowing any IP address to access may expose the management interface of F5 to different types of attacks such as DoS

Audit:

The following command should show the list of allowed IP addresses:

```
tmsh list /sys httpd allow
```

Remediation:

If the output of the above command show ALL, the following command would be executed to modify the settings:

```
modify modify /sys httpd allow replace-all-with { <IP address or IP address
range> }
```

Default Value:

ALL

References:

1. https://support.f5.com/csp/article/K13309

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	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,.		●	●

4 CLI Interface Management

4.1 Ensure Prelogin 'Login Banner' is set (Manual)

Profile Applicability:

- Level 1

Description:

Rationale:

Impact:

Failure to display adequate warning messages could result in the loss of litigation capabilities.

Audit:

```
1-Log in to the Configuration utility.

2-Navigate to System > Configuration > Device
```

Remediation:

```
1-Log in to the Configuration utility.

2-Navigate to System > Configuration > Device

3-Click SSHD.

4-Enter the desired pre-login message banner in the text box and enable
appropriate options.

5-To enable this banner message, check the Show The Security Banner On The
Login Screen option.
To disable this message banner, clear the Show The Security Banner On The
Login Screen option.

6-Click Update.
```

References:

1. https://support.f5.com/csp/article/K6068

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.2 Ensure 'Idle timeout' is less than or equal to 10 minutes for SSH connections (Manual)

Profile Applicability:

- Level 1

Description:

To set an idle timeout for SSH sessions

Rationale:

Impact:

Indefinite or even long session timeout window increase the risk of attackers abusing abandoned sessions

Audit:

```
1-Log in to tmsh by typing the following command:
tmsh
2-Use the following command syntax:
list /sys sshd inactivity-timeout
```

Remediation:

```
1-Log in to tmsh by typing the following command:
tmsh

2-To configure an automatic logout idle time (10 minutes) for SSH sessions,
use the following command syntax:
modify /sys sshd inactivity-timeout 600
3-Save the change by typing the following command:
save /sys config
```

References:

1. https://support.f5.com/csp/article/K9908

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.3 Ensure 'Idle timeout' is less than or equal to 10 minutes for tmsh sessions (Manual)

Profile Applicability:

- Level 1

Description:

To set an idle timeout for tmsh sessions

Rationale:

Impact:

Indefinite or even long session timeout window increases the risk of attackers abusing abandoned sessions.

Audit:

```
1- Log in to tmsh by typing the following command:
tmsh
2-Issue the following command : list /cli global-settings idle-timeout
```

Remediation:

```
1.Log in to tmsh by typing the following command: tmsh
2.To configure an automatic logout idle time for tmsh sessions, use the
following command syntax: modify /cli global-settings idle-timeout 10
3.Save the change by typing the following command: save /sys config
```

References:

1. https://support.f5.com/csp/article/K9908#ssh

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.4 Ensure 'Idle timeout' is less than or equal to 10 minutes for serial console sessions (Manual)

Profile Applicability:

- Level 1

Description:

To set an idle timeout for serial console sessions.

Rationale:

Impact:

Indefinite or even long session timeout window increases the risk of attackers abusing abandoned sessions.

Audit:

```
1-Log in to tmsh by typing the following command:
tmsh
2-Use the following command:
list /sys global-settings console-inactivity-timeout
```

Remediation:

```
- Log in to tmsh by typing the following command:
 tmsh
- To configure an automatic logout idle time for serial console sessions, use
the following command :
 modify /sys global-settings console-inactivity-timeout 600
- Save the change by typing the following command:
 save /sys config
```

References:

1. https://support.f5.com/csp/article/K9908#ssh

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	🟢	🟠	🔵
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	🟢	🟠	🔵

4.5 Ensure minimum SSH Encryption algorithm is set to aes128-cbc (Manual)

Profile Applicability:

- Level 1

Description:

To set strong SSH Encryption algorithm.

Rationale:

Impact:

Weak encryption algorithms make it possible for attackers to decrypt traffic and reduce the confidentiality capability that SSH provides for remote connections.

Audit:

```
-Log in to tmsh by typing the following command:
tmsh

-Type the following command:
 list /sys sshd all-properties.
```

Remediation:

```
1-Log in to tmsh by typing the following command:tmsh
2-To modify the sshd configuration, type the following command to start
the vi editor:edit /sys sshd all-properties
3-To change the list of ciphers, you can navigate to the line that starts
with the include statement, and use the keyword Ciphers :
include "Ciphers aes128-cbc,aes128-ctr,aes192-ctr,aes256-
ctr,arcfour128,arcfour256,arcfour"
```

References:

1. https://support.f5.com/csp/article/K80425458

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.6 Ensure to set SSH MAC algorithm to hmac-sha2-256 (Manual)

Profile Applicability:

- Level 1

Description:

To set strong Hashing algorithm

Rationale:

Impact:

Weak MAC algorithms make it possible for attackers to bypass authentication , steal keys and reduce the integrity capability that SSH provides for remote connections.

Audit:

```
1-Log in to tmsh by typing the following command:
tmsh

2-Type the following command:
list /sys sshd all-properties
```

Remediation:

```
1-Log in to tmsh by typing the following command:tmsh
2-To modify the sshd configuration, type the following command to start
the vi editor:edit /sys sshd all-properties
3-To change the list of ciphers, you can navigate to the line that starts
with the include statement, and use the keyword MACs ,and adding the list of
desired MACs to the 2-line include statement:
include "Ciphers aes128-cbc,aes128-ctr,aes192-ctr,aes256-
ctr,arcfour128,arcfour256,arcfour
MACs hmac-sha2-256"
```

References:

1. https://support.f5.com/csp/article/K80425458

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.7 Ensure to set Strong SSH KEY Exchange algorithm (Manual)

Profile Applicability:

- Level 1

Description:

To set strong Key Exchange algorithm

Rationale:

Impact:

Weak Key Exchange algorithms make it possible for attackers to bypass authentication , steal keys and reduce the integrity capability that SSH provides for remote connections .

Audit:

```
1-Log in to tmsh by typing the following command:
tmsh

2-Type the following command:
list /sys sshd all-properties
```

Remediation:

```
1-Log in to tmsh by typing the following command:tmsh

2-To modify the sshd configuration, type the following command to start the
vi editor:edit /sys sshd all-properties

3-Set a Key-Exchange algorithm with key of size 256 or longer  example
diffie-hellman-group14-sha256)

4-To change the list of ciphers, you can navigate to the line that starts
with the include statement, and use the keyword KexAlgorithms ,and adding the
list of desired KexAlgorithms to the 2-line include statement:
include "Ciphers aes128-cbc,aes128-ctr,aes192-ctr,aes256-
ctr,arcfour128,arcfour256,arcfour
MACs hmac-sha2-256
KexAlgorithms  diffie-hellman-group14-sha256
```

References:

1. https://support.f5.com/csp/article/K80425458

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

4.8 Ensure access SSH to CLI interface is restricted to needed IP addresses only (Manual)

Profile Applicability:

- Level 1

Description:

To limit ssh access to trusted IPs only

Rationale:

Impact:

Restricting access to the system MGT interface is to ensure that even if an attacker gains access to privileged credentials, his/her ability to get in and do damage is still limited.

Audit:

```
1-Log in to the Configuration utility.

2-Go to System > Platform.

3-For SSH IP Allow , check if there "All Addresses" selected.
```

Remediation:

```
1-Log in to the Configuration utility.

2-Go to System > Platform.

3-For SSH IP Allow, select Specify Range and then enter the IP addresses or
address ranges for the remote systems allowed to use SSH to communicate with
this system.
```

References:

1. https://support.f5.com/csp/article/K5380

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

5 System

5.1 Ensure redundant NTP servers are configured appropriately (Manual)

Profile Applicability:

- Level 1

Description:

To ensure redundant NTP servers are configured.

Rationale:

Impact:

Failing to connect to an NTP server results on incorrect time zone and date which impacts several functions on BIG-IP systems. It is recommended to have dual NTP servers configured to avoid single point of failure .

Audit:

```
1-Log in to the Configuration utility.

2-Navigate to System > Configuration > Device

3-Click NTP
```

Remediation:

```
1-Log in to the Configuration utility.

2-Navigate to System > Configuration > Device

3-Click NTP : add trusted NTP servers IP addresses .
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

5.2 Ensure to exclude inode information from ETags HTTP Header (Manual)

Profile Applicability:

- Level 1

Description:

To prevent the disclosure of inode information when accessing Configuration utility (GUI).

Rationale:

Impact:

When connecting to the Configuration utility, responses from the Apache server contain an Etag HTTP header that includes the file's inode information.(CVE-2003-1418).

Audit:

```
1-Log in to tmsh by entering the following command:
tmsh

2-check current HTTPD settings : list /sys httpd
```

Remediation:

```
1-Log in to tmsh by entering the following command: tmsh

2-To specify the format to be used for the Etag header, enter the following
command:

3-modify /sys httpd include "FileETag MTime Size"
  Save the configuration change by entering the following command:
 4-save /sys config

5-To restart the httpd service, enter the following command:
restart /sys service httpd
```

References:

1. https://support.f5.com/csp/article/K14206

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

5.3 Ensure port lockdown for self IP is set (Manual)

Profile Applicability:

- Level 1

Description:

to secure the BIG-IP system from unwanted connection attempts on self-IP.

Rationale:

Impact:

Default settings allow BIG-IP to listen on several ports on which some are not needed . Attackers may initiate attacks against the system self IPs on these ports . To reduce the risk , only needed ports should be enabled on self IPs.

Audit:

```
1-Log in to tmsh by typing the following command: tmsh

2-Type the command : tmsh list net self-allow

3-The output shows what protocols allowed for self-ip
```

Remediation:

```
1-Log in to the Configuration utility.

2-Go to Network > Self IPs.

3-Select the relevant self IP address.

4-If the specified interface does not need to listen to incoming connections
( Example BGP ,BDF ..etc) , set "Port Lockdown" to "Allow None"
5-If the specified interface need to listen for incoming connections , set
"Port Lockdown" to "Allow Custom". Then in the "Custom List" add needed ports
only.
```

References:

1. https://support.f5.com/csp/article/K17333

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 Securely Manage Network Infrastructure Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	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.	●	●	●

5.4 Ensure to disable unused services in BIG-IP configuration (Manual)

Profile Applicability:

- Level 1

Description:

To disable unused BIG-IP system daemons

Rationale:

Impact:

Many systems break-ins are a result of people taking advantage of security holes or problems with these programs. The more services that are running on your system, the more opportunities there are for others to use them, break into or take control of your system through them.

Audit:

```
1- Log in to the Configuration utility.

2- Go to System > Services > Services List

3-Check running service
```

Remediation:

```
1- Log in to the Configuration utility.

2- Go to System > Services > Services List

3-Select the unnecessary services you want to disable , then click "stop"

4-Click OK
```

References:

1. https://support.f5.com/csp/article/K05645522

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	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.		●	●

6 Monitoring and Auditing

6.1 Ensure that SNMP access is allowed to trusted agents IPs only (Manual)

Profile Applicability:

- Level 1

Description:

To limit access to trusted SNMP agents only

Rationale:

Impact:

Failing on restricting access to SNMP may allow unauthorised systems to gain access to the network device.

Audit:

```
1-Login to Configuration utility

2- Go to System > SNMP > Agent > Configuration

3- Check "Client Allow List" under SNMP Access
```

Remediation:

```
1-Login to Configuration utility

2- Go to System > SNMP > Agent > Configuration

3- Add trusted IP addresses in "Client Allow List"
```

References:

1. https://support.f5.com/csp/article/K13535

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

6.2 Ensure minimum SNMP version is set to V3 for agent access (Manual)

Profile Applicability:

- Level 1

Description:

To disable the usage of weak SNMP protocols

Rationale:

Impact:

Abuse of SNMP settings could allow an unauthorised third party to gain access to a network device when weak SNMP protocols are used.These protocols (prior to v3) lack the ability of authentication and encryption .

Audit:

```
1-Login to Configuration utility

2- Go to System > SNMP > Agent > SNMP Access (v1, v2c) : check if an entry is
listed.

3-Go to System > SNMP > Agent > SNMP Access (v3) : Check if an entry is
listed
```

Remediation:

```
1-Login to Configuration utility

2- Go to System > SNMP > Agent > SNMP Access (v1, v2c) :
Select all listed entries and click "Delete"

3-Go to System > SNMP > Agent > SNMP Access (v3) :
Make sure there is one entry at least , otherwise create one.
```

References:

1. https://support.f5.com/csp/article/K13625

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

6.3 Ensure to lockdown access logs to "Administrator , Resource Administrator and Auditor " roles only (Manual)

Profile Applicability:

- Level 1

Description:

To restrict access to the system logs.

Rationale:

Audit:

```
1-Login to Configuration utility

2-Go to System > Logs > Configuration > Options

3-Under "Log Access" , check who are allowed to access the logs.
```

Remediation:

```
1-Login to Configuration utility

2-Go to System > Logs > Configuration > Options

3- Under Log Access : select "Allow" for:
Administrator
Resource Administrator
Auditor

Select "Deny" for other users .
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.1 Establish and Maintain an Audit Log Management Process Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

6.4 Ensure that audit logging for "MCP, tmsh and GUI" is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

To enable audit logging on configuration changes that users or services make to the BIG-IP system.

Rationale:

Impact:

Audit logging provides a mechanism to investigate security incidents and unauthorised activities . It is also necessary for compliance auditing.

Audit:

```
1-Login to Configuration utility

2-Go to System > Logs > Configuration > Options

3- Under Audit Logging : check MCP,tmsh and GUI
```

Remediation:

```
1-Login to Configuration utility

2-Go to System > Logs > Configuration > Options

3- Under Audit Logging :
Select “Enable” for all items : “MCP” , “tmsh” and "GUI"
```

References:

1. https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-13-1-0/1.html
2. https://support.f5.com/csp/article/K07592334

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.1 Establish and Maintain an Audit Log Management Process Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

6.5 Ensure that Remote Syslog Servers are configured (Manual)

Profile Applicability:

- Level 1

Description:

To ensure that logs are sent to external servers

Rationale:

Impact:

In case of hardware failure , logs stored locally can be lost. This impacts the ability of investigating security incidents and be in compliance with the requirements of logs retention period .

Audit:

```
1-Log in to the Configuration utility.

2-Go to System > Logs > Configuration > Remote Logging.

3-Check "Remote Syslog Server List"
```

Remediation:

```
1-Log in to the Configuration utility.

2-Go to System > Logs > Configuration > Remote Logging.

3-For Remote IP, enter the destination syslog server IP address, or FQDN.
(DNS server configuration required)

4-For Remote Port, enter the remote syslog server UDP port (default is 514).

5-Select Add.

6-Select Update.
```

References:

1. https://support.f5.com/csp/article/K13080

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

Appendix: Recommendation Summary Table

Control		Set Correctly	
		Yes	No
1	**Accounts**		
1.1	**Passwords**		
1.1.1	Ensure default password of root is not allowed (Automated)	□	□
1.1.2	Ensure default password of admin is not used (Automated)	□	□
1.1.3	Configure Secure Password Policy (Manual)	□	□
2	**AAA**		
2.1	Ensure that Remote Radius is used for Authentication Only (Automated)	□	□
2.2	Ensure redundant remote authentication servers are configured (Manual)	□	□
2.3	Ensure that "Fallback to local" option is disabled for Remote Authentication Settings (Manual)	□	□
2.4	Ensure External Users' role is set to "No Access" (Automated)	□	□
2.5	Ensure External Users' has access to needed Partitions only (Automated)	□	□
2.6	Ensure External Users' Terminal Access is Disabled (Automated)	□	□
3	**GUI Interface Management**		
3.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for Configuration utility sessions (Automated)	□	□
3.2	Ensure access to Configuration utility by clients using TLS version 1.2 or later (Automated)	□	□
3.3	Ensure access to Configuration utility is restricted to needed IP addresses only (Automated)	□	□
4	**CLI Interface Management**		
4.1	Ensure Prelogin 'Login Banner' is set (Manual)	□	□
4.2	Ensure 'Idle timeout' is less than or equal to 10 minutes for SSH connections (Manual)	□	□
4.3	Ensure 'Idle timeout' is less than or equal to 10 minutes for tmsh sessions (Manual)	□	□
4.4	Ensure 'Idle timeout' is less than or equal to 10 minutes for serial console sessions (Manual)	□	□
4.5	Ensure minimum SSH Encryption algorithm is set to aes128-cbc (Manual)	□	□

4.6	Ensure to set SSH MAC algorithm to hmac-sha2-256 (Manual)	□	□
4.7	Ensure to set Strong SSH KEY Exchange algorithm (Manual)	□	□
4.8	Ensure access SSH to CLI interface is restricted to needed IP addresses only (Manual)	□	□
5	**System**		
5.1	Ensure redundant NTP servers are configured appropriately (Manual)	□	□
5.2	Ensure to exclude inode information from ETags HTTP Header (Manual)	□	□
5.3	Ensure port lockdown for self IP is set (Manual)	□	□
5.4	Ensure to disable unused services in BIG-IP configuration (Manual)	□	□
6	**Monitoring and Auditing**		
6.1	Ensure that SNMP access is allowed to trusted agents IPs only (Manual)	□	□
6.2	Ensure minimum SNMP version is set to V3 for agent access (Manual)	□	□
6.3	Ensure to lockdown access logs to "Administrator , Resource Administrator and Auditor " roles only (Manual)	□	□
6.4	Ensure that audit logging for "MCP, tmsh and GUI" is set to enabled (Manual)	□	□
6.5	Ensure that Remote Syslog Servers are configured (Manual)	□	□

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Ensure default password of root is not allowed	□	□
1.1.2	Ensure default password of admin is not used	□	□
1.1.3	Configure Secure Password Policy	□	□
2.1	Ensure that Remote Radius is used for Authentication Only	□	□
2.2	Ensure redundant remote authentication servers are configured	□	□
3.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for Configuration utility sessions	□	□
3.2	Ensure access to Configuration utility by clients using TLS version 1.2 or later	□	□
4.1	Ensure Prelogin 'Login Banner' is set	□	□
4.2	Ensure 'Idle timeout' is less than or equal to 10 minutes for SSH connections	□	□
4.3	Ensure 'Idle timeout' is less than or equal to 10 minutes for tmsh sessions	□	□
4.4	Ensure 'Idle timeout' is less than or equal to 10 minutes for serial console sessions	□	□
4.5	Ensure minimum SSH Encryption algorithm is set to aes128-cbc	□	□
4.6	Ensure to set SSH MAC algorithm to hmac-sha2-256	□	□
5.3	Ensure port lockdown for self IP is set	□	□
6.3	Ensure to lockdown access logs to "Administrator , Resource Administrator and Auditor " roles only	□	□
6.4	Ensure that audit logging for "MCP, tmsh and GUI" is set to enabled	□	□

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Ensure default password of root is not allowed	□	□
1.1.2	Ensure default password of admin is not used	□	□
1.1.3	Configure Secure Password Policy	□	□
2.1	Ensure that Remote Radius is used for Authentication Only	□	□
2.2	Ensure redundant remote authentication servers are configured	□	□
3.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for Configuration utility sessions	□	□
3.2	Ensure access to Configuration utility by clients using TLS version 1.2 or later	□	□
3.3	Ensure access to Configuration utility is restricted to needed IP addresses only	□	□
4.1	Ensure Prelogin 'Login Banner' is set	□	□
4.2	Ensure 'Idle timeout' is less than or equal to 10 minutes for SSH connections	□	□
4.3	Ensure 'Idle timeout' is less than or equal to 10 minutes for tmsh sessions	□	□
4.4	Ensure 'Idle timeout' is less than or equal to 10 minutes for serial console sessions	□	□
4.5	Ensure minimum SSH Encryption algorithm is set to aes128-cbc	□	□
4.6	Ensure to set SSH MAC algorithm to hmac-sha2-256	□	□
4.7	Ensure to set Strong SSH KEY Exchange algorithm	□	□
4.8	Ensure access SSH to CLI interface is restricted to needed IP addresses only	□	□
5.1	Ensure redundant NTP servers are configured appropriately	□	□
5.2	Ensure to exclude inode information from ETags HTTP Header	□	□
5.3	Ensure port lockdown for self IP is set	□	□
5.4	Ensure to disable unused services in BIG-IP configuration	□	□
6.1	Ensure that SNMP access is allowed to trusted agents IPs only	□	□
6.2	Ensure minimum SNMP version is set to V3 for agent access	□	□
6.3	Ensure to lockdown access logs to "Administrator , Resource Administrator and Auditor " roles only	□	□

6.4	Ensure that audit logging for "MCP, tmsh and GUI" is set to enabled	□	□
6.5	Ensure that Remote Syslog Servers are configured	□	□

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Ensure default password of root is not allowed	□	□
1.1.2	Ensure default password of admin is not used	□	□
1.1.3	Configure Secure Password Policy	□	□
2.1	Ensure that Remote Radius is used for Authentication Only	□	□
2.2	Ensure redundant remote authentication servers are configured	□	□
2.3	Ensure that "Fallback to local" option is disabled for Remote Authentication Settings	□	□
2.4	Ensure External Users' role is set to "No Access"	□	□
2.5	Ensure External Users' has access to needed Partitions only	□	□
2.6	Ensure External Users' Terminal Access is Disabled	□	□
3.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for Configuration utility sessions	□	□
3.2	Ensure access to Configuration utility by clients using TLS version 1.2 or later	□	□
3.3	Ensure access to Configuration utility is restricted to needed IP addresses only	□	□
4.1	Ensure Prelogin 'Login Banner' is set	□	□
4.2	Ensure 'Idle timeout' is less than or equal to 10 minutes for SSH connections	□	□
4.3	Ensure 'Idle timeout' is less than or equal to 10 minutes for tmsh sessions	□	□
4.4	Ensure 'Idle timeout' is less than or equal to 10 minutes for serial console sessions	□	□
4.5	Ensure minimum SSH Encryption algorithm is set to aes128-cbc	□	□
4.6	Ensure to set SSH MAC algorithm to hmac-sha2-256	□	□
4.7	Ensure to set Strong SSH KEY Exchange algorithm	□	□
4.8	Ensure access SSH to CLI interface is restricted to needed IP addresses only	□	□
5.1	Ensure redundant NTP servers are configured appropriately	□	□
5.2	Ensure to exclude inode information from ETags HTTP Header	□	□
5.3	Ensure port lockdown for self IP is set	□	□
5.4	Ensure to disable unused services in BIG-IP configuration	□	□

6.1	Ensure that SNMP access is allowed to trusted agents IPs only	□	□
6.2	Ensure minimum SNMP version is set to V3 for agent access	□	□
6.3	Ensure to lockdown access logs to "Administrator , Resource Administrator and Auditor " roles only	□	□
6.4	Ensure that audit logging for "MCP, tmsh and GUI" is set to enabled	□	□
6.5	Ensure that Remote Syslog Servers are configured	□	□

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Ensure default password of root is not allowed	□	□
1.1.2	Ensure default password of admin is not used	□	□
1.1.3	Configure Secure Password Policy	□	□
2.3	Ensure that "Fallback to local" option is disabled for Remote Authentication Settings	□	□
2.4	Ensure External Users' role is set to "No Access"	□	□
2.5	Ensure External Users' has access to needed Partitions only	□	□
2.6	Ensure External Users' Terminal Access is Disabled	□	□
3.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for Configuration utility sessions	□	□
3.2	Ensure access to Configuration utility by clients using TLS version 1.2 or later	□	□
3.3	Ensure access to Configuration utility is restricted to needed IP addresses only	□	□
4.1	Ensure Prelogin 'Login Banner' is set	□	□
4.2	Ensure 'Idle timeout' is less than or equal to 10 minutes for SSH connections	□	□
4.3	Ensure 'Idle timeout' is less than or equal to 10 minutes for tmsh sessions	□	□
4.4	Ensure 'Idle timeout' is less than or equal to 10 minutes for serial console sessions	□	□
4.5	Ensure minimum SSH Encryption algorithm is set to aes128-cbc	□	□
4.6	Ensure to set SSH MAC algorithm to hmac-sha2-256	□	□
4.7	Ensure to set Strong SSH KEY Exchange algorithm	□	□
4.8	Ensure access SSH to CLI interface is restricted to needed IP addresses only	□	□
5.2	Ensure to exclude inode information from ETags HTTP Header	□	□
6.3	Ensure to lockdown access logs to "Administrator , Resource Administrator and Auditor " roles only	□	□
6.4	Ensure that audit logging for "MCP, tmsh and GUI" is set to enabled	□	□

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Ensure default password of root is not allowed	□	□
1.1.2	Ensure default password of admin is not used	□	□
1.1.3	Configure Secure Password Policy	□	□
2.1	Ensure that Remote Radius is used for Authentication Only	□	□
2.2	Ensure redundant remote authentication servers are configured	□	□
2.3	Ensure that "Fallback to local" option is disabled for Remote Authentication Settings	□	□
2.4	Ensure External Users' role is set to "No Access"	□	□
2.5	Ensure External Users' has access to needed Partitions only	□	□
2.6	Ensure External Users' Terminal Access is Disabled	□	□
3.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for Configuration utility sessions	□	□
3.2	Ensure access to Configuration utility by clients using TLS version 1.2 or later	□	□
3.3	Ensure access to Configuration utility is restricted to needed IP addresses only	□	□
4.1	Ensure Prelogin 'Login Banner' is set	□	□
4.2	Ensure 'Idle timeout' is less than or equal to 10 minutes for SSH connections	□	□
4.3	Ensure 'Idle timeout' is less than or equal to 10 minutes for tmsh sessions	□	□
4.4	Ensure 'Idle timeout' is less than or equal to 10 minutes for serial console sessions	□	□
4.5	Ensure minimum SSH Encryption algorithm is set to aes128-cbc	□	□
4.6	Ensure to set SSH MAC algorithm to hmac-sha2-256	□	□
4.7	Ensure to set Strong SSH KEY Exchange algorithm	□	□
4.8	Ensure access SSH to CLI interface is restricted to needed IP addresses only	□	□
5.1	Ensure redundant NTP servers are configured appropriately	□	□
5.2	Ensure to exclude inode information from ETags HTTP Header	□	□
5.3	Ensure port lockdown for self IP is set	□	□
5.4	Ensure to disable unused services in BIG-IP configuration	□	□

6.1	Ensure that SNMP access is allowed to trusted agents IPs only	□	□
6.2	Ensure minimum SNMP version is set to V3 for agent access	□	□
6.3	Ensure to lockdown access logs to "Administrator , Resource Administrator and Auditor " roles only	□	□
6.4	Ensure that audit logging for "MCP, tmsh and GUI" is set to enabled	□	□
6.5	Ensure that Remote Syslog Servers are configured	□	□

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Ensure default password of root is not allowed	□	□
1.1.2	Ensure default password of admin is not used	□	□
1.1.3	Configure Secure Password Policy	□	□
2.1	Ensure that Remote Radius is used for Authentication Only	□	□
2.2	Ensure redundant remote authentication servers are configured	□	□
2.3	Ensure that "Fallback to local" option is disabled for Remote Authentication Settings	□	□
2.4	Ensure External Users' role is set to "No Access"	□	□
2.5	Ensure External Users' has access to needed Partitions only	□	□
2.6	Ensure External Users' Terminal Access is Disabled	□	□
3.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for Configuration utility sessions	□	□
3.2	Ensure access to Configuration utility by clients using TLS version 1.2 or later	□	□
3.3	Ensure access to Configuration utility is restricted to needed IP addresses only	□	□
4.1	Ensure Prelogin 'Login Banner' is set	□	□
4.2	Ensure 'Idle timeout' is less than or equal to 10 minutes for SSH connections	□	□
4.3	Ensure 'Idle timeout' is less than or equal to 10 minutes for tmsh sessions	□	□
4.4	Ensure 'Idle timeout' is less than or equal to 10 minutes for serial console sessions	□	□
4.5	Ensure minimum SSH Encryption algorithm is set to aes128-cbc	□	□
4.6	Ensure to set SSH MAC algorithm to hmac-sha2-256	□	□
4.7	Ensure to set Strong SSH KEY Exchange algorithm	□	□
4.8	Ensure access SSH to CLI interface is restricted to needed IP addresses only	□	□
5.1	Ensure redundant NTP servers are configured appropriately	□	□
5.2	Ensure to exclude inode information from ETags HTTP Header	□	□
5.3	Ensure port lockdown for self IP is set	□	□
5.4	Ensure to disable unused services in BIG-IP configuration	□	□

6.1	Ensure that SNMP access is allowed to trusted agents IPs only	□	□
6.2	Ensure minimum SNMP version is set to V3 for agent access	□	□
6.3	Ensure to lockdown access logs to "Administrator , Resource Administrator and Auditor " roles only	□	□
6.4	Ensure that audit logging for "MCP, tmsh and GUI" is set to enabled	□	□
6.5	Ensure that Remote Syslog Servers are configured	□	□

Appendix: Change History

Date	Version	Changes for this version