synapxe

Inspiring Tomorrow’s Health

Security Hardening Benchmark for Cisco FirePower Devices

STND-78-2143-Security Hardening Benchmark for Cisco FirePower Devices | Version 1.9

Revision Date: 16/5/2024

Approved By: Head of Department (HOD), Cloud Enablement Services (CES)

Information Classification: Restricted, Sensitive (Normal)

This document contains proprietary information that is confidential to the Synapxe Pte Ltd. Disclosure of this document in full or in part, may result in material damage to the Synapxe Pte Ltd. Written permission must be obtained prior to the disclosure of this document to a third party. Any hardcopy of this document, printed or photocopied, is considered an uncontrolled copy. The original, signed-off document is the controlled copy.

Table of Contents

1 Purpose

This document contains the baseline security controls for the Cisco FirePower devices.

2 Scope

This hardening baseline applies to the Cisco FirePower devices deployed in the H-Cloud network infrastructure.

3 10.FIREPOWER MANAGEMENT CENTRE (FMC)

3.1 General Security Control List

SN	Controls	Purpose	Required Settings -All settings are mandatory unless listed as Optional.	Configuration Reference -The instructions are purely for reference purpose and may differ across different product versions.
3.1.1	Hostname	Device Hostname should be unique and consistent across H-Cloud <System Name> host names should conform to the H-Cloud Naming Convention.	< DataCenterLocation > - < NetworkZone > - <Institution/cluster>-< DevicePurpose >< Running Numbers >	Login via GUI System > Maangement Interfaces > Shared Settings > Hostname > Save
3.1.2	Warning Banner	Standard login banner containing the authorized use legal disclaimer are to be configured to all security devices where possible.	Banner Message: *THIS SYSTEM IS SOLELY FOR THE USE OF AUTHORIZED USERS FOR OFFICIAL PURPOSES. YOU HAVE NO EXPECTATION OF PRIVACY IN ITS USE AND TO ENSURE THAT THE SYSTEM IS FUNCTIONING PROPERLY, INDIVIDUALS USING THIS COMPUTER SYSTEMS ARE SUBJECT TO HAVING ALL OF THEIR ACTIVITIES MONITORED AND RECORDED BY SYSTEM PERSONNEL.* *ANY UNAUTHORIZED ACCESS IS LIABLE TO PROSECUTION UNDER THE COMPUTER MISUSE ACT.*	System > Configuration > Login Banner > Custom Login Banner > THIS SYSTEM IS SOLELY FOR THE USE OF AUTHORIZED USERS FOR OFFICIAL PURPOSES. YOU HAVE NO EXPECTATION OF PRIVACY IN ITS USE AND TO ENSURE THAT THE SYSTEM IS FUNCTIONING PROPERLY, INDIVIDUALS USING THIS COMPUTER SYSTEMS ARE SUBJECT TO HAVING ALL OF THEIR ACTIVITIES MONITORED AND RECORDED BY SYSTEM PERSONNEL. ANY UNAUTHORIZED ACCESS IS LIABLE TO PROSECUTION UNDER THE COMPUTER MISUSE ACT. > Save
3.1.3	Clock and NTP	Devices must be configured to synchronize with the authorized H-Cloud NTP servers and set to SGT time zone.	**H-Cloud NTP Servers IP Address** All devices in HDC1 and HDC2 to configure the below NTP servers. 1. 10.247.2.11 2. 10.247.2.12 3. 10.247.34.11 4. 10.247.34.12	System > Configuration > Time Synchronization > Server Time via NTP: Enabled Set My Clock: via NTP: Use the authenticated NTP server only: Enabled Add NTP Server <NTP Server IP Address> Authentication Settings Key Type: SHA-1

				Key Number: <Key Number> Key Value: <Key Value> Save
3.1.4	Syslog	All security devices, must be configured to log errors and activity to the H-Cloud syslog servers.	**H-Cloud Syslog Servers IP Address** List of servers to configure for HDC1 devices: For Audit Log: 1. 10.247.20.161 OIP For eStreamer: 2. 10.234.241.x [IP and Port will be advised by ASOC during ASOC onboarding] 3. 10.247.20.161 OIP List of servers to configure for HDC2 devices: For eStreamer: 1. 10.234.245.x [IP and Port will be advised by ASOC during ASOC onboarding] 2. 10.247.32.231 OIP	System > Configuration > Audit Log > Send Audit Log to Syslog: Enabled Host: <Syslog Server IP Address> Facility: LOCAL7 Severity: INFO Save **Syslog Configuration via eStreamer** Login to FMC via GUI System > Integration > Other Integrations > eStreamer In eStreamer Event Configuration: Select Connection Events > Save Create Client > Add <IP Address> Save and Deploy

3.2 Health Monitoring

SN	Controls	Purpose	Required Settings -All settings are mandatory unless listed as Optional.	Configuration Reference -The instructions are purely for reference purpose and may differ across different product versions.
3.2.1	SNMP Settings	SNMP is an application layer protocol that helps the exchange of management information between the network devices.	**H-Cloud EG Servers IP Address** List of servers to configure for HDC1 devices: 1. 10.247.22.53 2. 10.247.22.54 3. 10.247.22.55 4. 10.247.22.56 List of servers to configure for HDC2 devices: 1. 10.247.54.53 2. 10.247.54.54 3. 10.247.54.55 4. 10.247.54.56 Username: <EG Username> Password: ****** Version: v3 Authentication Type: SHA Privacy Protocol: AES128	**Configure SNMP User** System > Configuration > SNMP > SNMP Version: Version3 Add User: Username: <username> Authentication: MD5 Authentication Password:****** Verify Password: ***** **Configure Access List** System > Configuration > Access List > Add/Delete/Edit Rules IP Address: <SNMP Server IP> Port: SNMP Add > Save
3.2.2	Health Monitor Alerts	Configure an alert response that governs the Firepower Management Center's communication with the SNMP, syslog, or email server where	Please refer to 3.1.3 for Syslog and 3.2.1 for SNMP Settings.	**To Configure Monitor Alert** Policies > Actions > Alerts > Create Alert SNMP/Syslog ***To Create SNMP Alert*** Name: <Server>_SNMP Trap Server: <SNMP Server IP> Version: V3 User Name: <Username>

		you send the health alert.		Authentication Protocol: SHA Password: ****** Privacy Protocol: DES Password: ****** ***To Create Syslog Alert*** Name: <Server>_SYSLOG Host: <Syslog Server IP Address> Port: 514 Facility: Local7 Severity: INFO ***To Create Heath Monitor Alert*** System > Health > Monitor Alerts > Save Health Alert Name: <Health Alert Name> Severity: Critical/Normal/Error/Recovered Module: Select below Modules Appliance Heartbeat Backlog Status CPU Usage Card Reset Disk Status Cluster/Failover Status Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit Interface Status Memory Usage Power Supply Process Status RRD Server Process Security Intelligence Smart License Monitor Time Series Data Monitor Time Synchronization Status Alert: <Server>_SYSLOG/<Server>_SNMP

3.3 Management Access Control List

SN	**Controls**	**Purpose**	**Required Settings** -All settings are mandatory unless listed as Optional.	**Configuration Reference** -The instructions are purely for reference purpose and may differ across different product versions.
3.3.1	Restrict Remote Access	Access-list is used to secure the management access to the system by IP and port.	**H-Cloud PAM Servers (HTTPS, SSH)** 1. 10.247.22.62 2. 10.247.22.20-10.247.22.22 3. 10.247.22.39-10.247.22.43 4. 10.247.22.126-10.247.22.133 5. 10.247.22.24 6. 10.247.22.77-10.247.22.79 7. 10.247.54.62 8. 10.247.54.20-10.247.54.22 9. 10.247.54.39-10.247.54.43 10. 10.247.54.122-10.247.54.129 11. 10.247.54.24 12. 10.247.54.77-10.247.54.79 13. 10.247.22.80-10.247.22.81	System > Configuration > Access-list > Add/Delete/Edit Rules > Save IP Address: <PAM/Utility Server IP Address> Port: <SSH/HTTPS/SNMP>

			14. 10.247.54.81-10.247.54.82 **H-Cloud Security Utility Servers (HTTPS, SSH)** 1. 10.247.22.4 2. 10.247.54.4 **Security Compliance Server (HTTPS, SSH)** 1. 10.247.17.62 2. 10.247.22.135 **Algosec Server (HTTPS, SSH)** 1. 10.247.126.25-10.247.126.27 [*Optional*] **EVMS Scanner IP (HTTPS, SSH)** 1. 10.247.17.106 2. 10.247.49.98	
3.3.2	Session Timeout	To limit the length of account login to secure the device from unauthorized users to exploit the unattended sessions.	***Browser Settings:*** Browser Session Timeout (Minutes): 15 ***Shell Settings:*** Shell Timeout (Minutes): 15	System > Configuration > Shell Timeout > ***Browser Settings:*** Browser Session Timeout (Minutes): 15 ***Shell Settings:*** Shell Timeout (Minutes): 15
3.3.3	Web GUI	By default, GUI uses a default self-signed certificate. To secure the information between GUI and your jumphost, it is recommended to replace the certificate with a trusted certificate authority.	***Country Name:*** SG ***State of Province:*** SG ***Locality or City:*** SG ***Organization:*** SYNAPXE ***Organizational Unit:*** HCLOUD ***Common Name:*** <Hostname>. HCloud.healthgrp.com.sg *Note: Certificates generated before 01 September 2023 may use Integrated Health Information Systems for "Organization".*	**Generate CSR via GUI** System > Configuration > HTTPS Certificate > Generate New CSR ***Country Name:*** SG ***State of Province:*** SG ***Locality or City:*** SG ***Organization:*** SYNAPXE ***Organizational Unit:*** HCLOUD ***Common Name:*** <Hostname>. HCloud.healthgrp.com.sg **PKI Certificate Installation via GUI** System > Configuration > HTTPS Certificate > Import HTTPS Server Certificate > Server Certificate > Save **PKI Certificate Installation via CLI** Login to FMC via CLI #Expert #Sudo su #cd /etc/ssl/ #vi <new_certname>.crt – *to create new certificate file. In editor press i to insert then copy paste the certificate content, :wq to quit and save the editor* #mv certname.crt to server.crt – *to apply the new certificate* #pmtool restart https – to restart GUI service
3.3.4	Local Accounts	Local admin accounts used for breakfix. Password strength check must be enabled for locally authenticated users.	**Password Policy** 1. Must contain a minimum of 15 characters 2. Must include characters from at least 2 of the following 4 categories: A. Upper case (A through Z);	System > Users > Create User > Save ***User Configuration:*** User Name: <Username> Password: ***** Confirm Password: ***** Maximum Number of Failed Logins: 3 Minimum Password Length: 16 Days Until Password Expiration: 365 Days Before LDA Expiration Warning: 5

			B. Lower case (a through z); C. Digits (0-9); D. Special Characters (!, $, #, %, etc.). 3. Password expiration must be 365days 4. Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word. 5. Not be reused for at least 5 generations 6. Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb. 7. Must not contain three consecutive numbers or letters in any order, such as passwordABC or password321. 8. Must not be identical to the username or the reverse of the username. 9. Account lockout after 5 consecutive failed authentication attempts	Role: Administrator
3.3.5	External Authentication	To secure that only H-Cloud Security Engineers are able to access and make changes to the device configuration through LDAP or RADIUS authentication.	**H-Cloud LDAP Servers IP Address** List of servers to configure for HDC1 devices: 1. 10.244.152.18 [HISADDCVPUTL03.hcloud.healthgrp.com.sg] 2. 10.245.152.19 [HISADDCVPUTL02.hcloud.healthgrp.com.sg] 3. 10.244.152.19 [HISADDCVPUTL04.hcloud.healthgrp.com.sg] [*Optional*] List of servers to configure for HDC2 devices: 1. 10.245.152.19 [HISADDCVPUTL02.hcloud.healthgrp.com.sg] 2. 10.244.152.19 [HISADDCVPUTL04.hcloud.healthgrp.com.sg] 3. 10.244.152.18 [HISADDCVPUTL03.hcloud.healthgrp.com.sg] [*Optional*] Base DN: hcloud,DC=healthgrp,DC=com,DC=sg Port: 636/TCP	System > Users > External Authentication > Add/Delete/Edit External Authentication Object >Save and Apply ***External Authentication Object:*** *Authentication Method:* <LDAP/RADIUS> *Name:* <Authentication Name> *Description:* <Optional> *Server Type:* <MS Active Directory/Oracle Directory/OpenLDAP/Other> ***Primary Server:*** *Host Name/IP Address:* <IP/Hostname> *Port:* Backup Server (Optional) *Host Name/IP Address:* <IP/Hostname> *Port:* ***LDAP-Specific Parameters:*** *Base DN= hcloud,DC=healthgrp,DC=com,DC=sg* *Base Filter = (|(memberOf=CN=IHIS_PAMSECREAD,OU=Hcloud Groups,DC=hcloud,DC=healthgrp,DC=com,DC=sg) (memberOf=CN=IHIS_PAMSECADM,OU=Hcloud Groups,DC=hcloud,DC=healthgrp,DC=com,DC=sg))* *User Name:* <Service Account>

				*Password: ****** *Confirm Password: ******

4 FIREPOWER THREAT DEFENSE (FTD)

4.1 General Security Control List

SN	Controls	Purpose	Required Settings	Configuration Reference
			-All settings are mandatory unless listed as Optional.	-The instructions are purely for reference purpose and may differ across different product versions.
4.1.1	Hostname	Device Hostname should be unique and consistent across H-Cloud <System Name> host names should conform to the H-Cloud Naming Convention.	< DataCenterLocation > - < NetworkZone > - <Institution/cluster>-< DevicePurpose >< Running Numbers >	Login via CLI >configure network hostname <hostname>
4.1.2	Warning Banner	Standard login banner containing the authorized use legal disclaimer are to be configured to all security devices where possible.	Banner Message: *THIS SYSTEM IS SOLELY FOR THE USE OF AUTHORIZED USERS FOR OFFICIAL PURPOSES. YOU HAVE NO EXPECTATION OF PRIVACY IN ITS USE AND TO ENSURE THAT THE SYSTEM IS FUNCTIONING PROPERLY, INDIVIDUALS USING THIS COMPUTER SYSTEMS ARE SUBJECT TO HAVING ALL OF THEIR ACTIVITIES MONITORED AND RECORDED BY SYSTEM PERSONNEL.* *ANY UNAUTHORIZED ACCESS IS LIABLE TO PROSECUTION UNDER THE COMPUTER MISUSE ACT.*	Platform Settings > Platform_HIS_<ZONE> > Banner > Save > Deploy *THIS SYSTEM IS SOLELY FOR THE USE OF AUTHORIZED USERS FOR OFFICIAL PURPOSES. YOU HAVE NO EXPECTATION OF PRIVACY IN ITS USE AND TO ENSURE THAT THE SYSTEM IS FUNCTIONING PROPERLY, INDIVIDUALS USING THIS COMPUTER SYSTEMS ARE SUBJECT TO HAVING ALL OF THEIR ACTIVITIES MONITORED AND RECORDED BY SYSTEM PERSONNEL.* *ANY UNAUTHORIZED ACCESS IS LIABLE TO PROSECUTION UNDER THE COMPUTER MISUSE ACT*
4.1.3	Clock and NTP	Devices must be configured to synchronize with the authorized H-Cloud NTP servers and set to SGT time zone.	**H-Cloud NTP Servers IP Address** All devices in HDC1 and HDC2 to configure the below NTP servers. 1. 10.247.2.11 2. 10.247.2.12 3. 10.247.34.11 4. 10.247.34.12	Platform Settings > Time Synchronization > Set My Clock > via NTP from Management Server > Save
4.1.4	Syslog	All security devices, must be configured to log errors and activity to the H-Cloud syslog servers.	**H-Cloud Syslog Servers IP Address** List of servers to configure for HDC1 devices: 1. 10.247.126.25 UDP/514 Algosec [Optional] 2. 10.247.20.161 TCP/9003 OIP 3. 10.247.0.9 UDP/514 CSA [Optional] List of servers to configure for HDC2 devices: 1. 10.247.126.25 UDP/514 Algosec [Optional]	Platform Settings > Platform_HIS_<ZONE> > Syslog > Deploy ***Logging Setup*** Enable Logging: Yes Enable Logging on the failover standby unit: Yes Memory Size of the Internal Buffer: 4096 Enable Logging to FMC: Yes Logging Level: Informational ***Logging Destinations*** Click Add/Delete/Edit Logging Destination: Syslog Servers

			2. 10.247.32.231 TCP/9003 OIP 3. 10.247.32.9 UDP/514 CSA [Optional]	Event Class: Filter on Severity > Informational Event Class: Syslog Severity Config: Informational Sys: Informational HA: Informational Session: Informational Auth: Informational ***Event Lists*** Click Add/Delete/Edit Name: <Event List Name> Severity/Event Class: Click Add/Delete/Edit and select from the list of events (Optional) Message ID: Click Add/Delete/Edit and select from the list of Message ID ***Syslog Settings***: Facility: Local20 Enable Timestamp on Syslog Messages Timestamp Format: Legacy (MM dd yy HH:mm:ss) Enable Syslog Device ID: Enable > Hostname Syslog Servers: Allow user traffic to pass when TCP syslog server is down > Enable Message Queue Size(messages): 512 ADD Syslog Server: IP Address: <Syslog Server IP Address> Protocol: <TCP/UDP> Port: <Port #> Save

4.2 Health Monitoring

SN	**Controls**	**Purpose**	**Required Settings** -All settings are mandatory unless listed as Optional.	**Configuration Reference** -The instructions are purely for reference purpose and may differ across different product versions.
4.2.1	SNMP Settings	SNMP is an application layer protocol that helps the exchange of management information between the network devices.	**H-Cloud EG, OIP and CSPC Servers IP Address** List of servers to configure for HDC1 devices: 1. 10.247.22.53 2. 10.247.22.54 3. 10.247.22.55 4. 10.247.22.56 5. 10.247.209.10 6. 10.247.20.170 List of servers to configure for HDC2 devices: 1. 10.247.54.53 2. 10.247.54.54 3. 10.247.54.55 4. 10.247.54.56 5. 10.247.218.10 6. 10.247.32.232 Username: <EG Username>	Platform Settings > Platform_HIS_<ZONE> SNMP > Deploy Enable SNMP Serves > Tick Port: 161 **Add Users:** *Security Level:* <NoAuth/Auth/Priv> *Username:* <Username> *Encryption Password Type:* <Cleartext/Encrypted> *Auth Algorithm Type:* <MD5/SHA> Authentication Password: ***** Confirm: ***** **Add SNMP Management Hosts:** IP Address: <SNMP Server IP> SNMP Version: 3 Username: <Username> Enable: Poll and Trap Port: 162

			Password: ****** Version: v3 Authentication Type: SHA Privacy Protocol: AES128	**<u>Delete SNMP Management Hosts:</u>** Select IP Address > Delete
4.2.2	Health Monitor Alerts	Configure an alert response that governs the Firepower Management Center's communication with the SNMP, syslog, or email server where you send the health alert.	Please refer to 3.1.3 for Syslog and 3.2.1 for SNMP Settings.	System > Health > Policy > Save Policy Run Time Interval: 5mins AMP for Endpoints Status: ON AMP for Firepower Status: ON Appliance Heartbeat: ON Automatic Application Bypass Status: ON Backlog Status: ON Card Reset: OFF Cluster/Failover Status: ON CPU Usage Disk Status: ON Disk Usage: ON Critical Threshold %: 90 Warning Threshold %: 85 2HD Critical Threshold %: 99 2HD Warning Threshold %: 97 Hardware Alarms: ON HA Status: ON Health Monitor Process Host Limit: ON Inline Link Mismatch Alarms: ON Interface Status: ON Intrusion and File Event Rate: ON ISE Connection Status Monitor Link State Propagation: ON Local Malware Analysis: ON Memory Usage: Critical Threshold %: 90 Warning Threshold %: 80 Platform Faults Power Supply: ON Process Status: ON Realm Reconfiguring Detection: ON RRD Server Process: ON Security Intelligence: ON Smart License Monitor: ON Threat Data Updates on Devices: ON Time Series Data Monitor: ON Time Synchronization Status: ON URL Filtering Monitor: ON User Agent Status Monitor VPN Status

4.3 Management Access Control List

SN	Controls	Purpose	Required Settings -All settings are mandatory unless listed as Optional.	Configuration Reference -The instructions are purely for reference purpose and may differ across different product versions.
4.3.1	Restrict Remote Access	Access-list is used to secure the management access to the system by IP and port.	**<u>H-Cloud PAM Servers (HTTPS, SSH)</u>** 1. 10.247.22.62 2. 10.247.22.20-10.247.22.22 3. 10.247.22.39-10.247.22.43 4. 10.247.22.126-10.247.22.132 5. 10.247.22.24 6. 10.247.22.77-10.247.22.79	Devices > Platform Settings > Policy Name> Secure Shell > Add/Delete/Edit > Save IP Address: <PAM/Utility Server IP Address> Interface: <diagnostic/management>

			7. 10.247.54.62 8. 10.247.54.20-10.247.54.22 9. 10.247.54.39-10.247.54.43 10. 10.247.54.122-10.247.54.129 11. 10.247.54.24 12. 10.247.54.77-10.247.54.79 13. 10.247.22.80-10.247.22.81 14. 10.247.54.81-10.247.54.82 **H-Cloud Security Utility Servers (HTTPS, SSH)** 1. 10.247.22.4 2. 10.247.54.4 **Security Compliance Server (HTTPS, SSH)** 1. 10.247.17.62 2. 10.247.22.135 **Algosec Server (HTTPS, SSH)** 1. 10.247.126.25-10.247.126.27 [*Optional*] **EVMS Scanner IP (HTTPS, SSH)** 1. 10.247.17.106 2. 10.247.49.98	***Alternate Method: Login to FTD via CLI and Execute below command via clish >configure ssh-access-list <IP Address/Subnet mask> To verify the configuration >show ssh-access-list
4.3.2	Session Timeout	To limit the length of account login to secure the device from unauthorized users to exploit the unattended sessions.	***Browser Settings:*** Browser Session Timeout (Minutes): 15 ***Shell Settings:*** Shell Timeout (Minutes): 15	Devices > Platform Settings > Policy Name> Timeout > 15(mins) > Save
4.3.3	Local Accounts	Local admin accounts used for breakfix. Password strength check must be enabled for locally authenticated users.	**Password Policy** 1. Must contain a minimum of 15 characters 2. Must include characters from at least 2 of the following 4 categories: E. Upper case (A through Z); F. Lower case (a through z); G. Digits (0-9); H. Special Characters (!, $, #, %, etc.). 3. Password expiration must be 365days 4. Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word. 5. Not be reused for at least 5 generations 6. Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb. 7. Must not contain three consecutive numbers or letters	Login to FTD via CLI configure user add <username> <basic/config> • basic—Gives the user basic access. This role does not allow the user to enter configuration commands. • config—Gives the user configuration access. This role gives the user full administrator rights to all commands.

			in any order, such as passwordABC or password321. 8. Must not be identical to the username or the reverse of the username. 9. Account lockout after 5 consecutive failed authentication attempts	
4.3.4	External Authentication	To secure that only H-Cloud Security Engineers are able to access and make changes to the device configuration through LDAP or RADIUS authentication.	**H-Cloud LDAP Servers IP Address** List of servers to configure for HDC1 devices: 1. 10.244.152.18 [HISADDCVPUTL03.hcloud.healthgrp.com.sg] 2. 10.245.152.19 [HISADDCVPUTL02.hcloud.healthgrp.com.sg] 3. 10.244.152.19 [HISADDCVPUTL04.hcloud.healthgrp.com.sg] [*Optional*] List of servers to configure for HDC2 devices: 1. 10.245.152.19 [HISADDCVPUTL02.hcloud.healthgrp.com.sg] 2. 10.244.152.19 [HISADDCVPUTL04.hcloud.healthgrp.com.sg] 3. 10.244.152.18 [HISADDCVPUTL03.hcloud.healthgrp.com.sg] [*Optional*] Base DN: hcloud,DC=healthgrp,DC=com,DC=sg Port: 636/TCP	Devices > Platform Settings > Policy Name> External Authentication Select the External Authentication Profile: Enable For Authentication Profile, refer to FMC External Authentication Settings.

5 FIREPOWER CHASSIS MANAGER (FCM)

5.1 General Security Control List

SN	Controls	Purpose	Required Settings -All settings are mandatory unless listed as Optional.	Configuration Reference -The instructions are purely for reference purpose and may differ across different product versions.
5.1.1	Hostname	Device Hostname should be unique and consistent across H-Cloud <System Name> host names should conform to the H-Cloud Naming Convention.	< DataCenterLocation > - < NetworkZone > - <Institution/cluster>-< DevicePurpose >< Running Numbers >	Login via CLI Firepower-chassis-A# scope system Firepower-chassis-A /system # set name <hostname> Firepower-chassis-A /system* # commit-buffer
5.1.2	Warning Banner	Standard login banner containing the authorized use legal disclaimer are to be configured to	Banner Message: *THIS SYSTEM IS SOLELY FOR THE USE OF AUTHORIZED USERS FOR OFFICIAL*	Firepower-chassis# scope security Firepower-chassis /security # scope banner Firepower-chassis /security/banner # create pre-login-banner

		all security devices where possible.	*PURPOSES. YOU HAVE NO EXPECTATION OF PRIVACY IN ITS USE AND TO ENSURE* *THAT THE SYSTEM IS FUNCTIONING PROPERLY, INDIVIDUALS USING THIS COMPUTER SYSTEM ARE SUBJECT TO HAVING ALL OF THEIR ACTIVITIES MONITORED AND RECORDED BY SYSTEM PERSONNEL.* *ANY UNAUTHORIZED ACCESS IS LIABLE TO PROSECUTION UNDER THE COMPUTER MISUSE ACT.*	Firepower-chassis /security/banner/pre-login-banner* # set message Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort. Enter prelogin banner: >THIS SYSTEM IS SOLELY FOR THE USE OF AUTHORIZED USERS FOR OFFICIAL >PURPOSES. YOU HAVE NO EXPECTATION OF PRIVACY IN ITS USE AND TO ENSURE >THAT THE SYSTEM IS FUNCTIONING PROPERLY, INDIVIDUALS USING THIS >COMPUTER SYSTEM ARE SUBJECT TO HAVING ALL OF THEIR ACTIVITIES >MONITORED AND RECORDED BY SYSTEM PERSONNEL. > >ANY UNAUTHORIZED ACCESS IS LIABLE TO PROSECUTION UNDER THE COMPUTER MISUSE ACT. >ENDOFBUF Firepower-chassis /security/banner/pre-login-banner* # commit-buffer Firepower-chassis /security/banner/pre-login-banner #
5.1.3	Clock and NTP	Devices must be configured to synchronize with the authorized H-Cloud NTP servers and set to SGT time zone.	**H-Cloud NTP Servers IP Address** All devices in HDC1 and HDC2 to configure the below NTP servers. 1. 10.247.2.11 2. 10.247.2.12 3. 10.247.34.11 4. 10.247.34.12	Platform Settings > NTP > Time Synchronization > Use NTP Server > Add >Save <NTP Server IP Address>
5.1.4	Syslog	All security devices, must be configured to log errors and activity to the H-Cloud syslog servers.	**H-Cloud Syslog Servers IP Address** List of servers to configure for HDC1 devices: 1. 10.247.20.161 OIP List of servers to configure for HDC2 devices: 1. 10.247.32.231 OIP	Platform Settings > Syslog > Remote Destinations > Save Server1 Admin State: Enable Level: Information Hostname/IP Address: <Syslog Server IP Address> Facility: Local7

5.2 Health Monitoring

SN	Controls	Purpose	Required Settings -All settings are mandatory unless listed as Optional.	Configuration Reference -The instructions are purely for reference purpose and may differ across different product versions.
5.2.1	SNMP Settings	SNMP is an application layer protocol that helps the exchange of management information between the network devices.	**H-Cloud EG Servers IP Address** List of servers to configure for HDC1 devices: 1. 10.247.22.53 2. 10.247.22.54 3. 10.247.22.55 4. 10.247.22.56 5. 10.247.20.170 List of servers to configure for HDC2 devices: 1. 10.247.54.53 2. 10.247.54.54 3. 10.247.54.55 4. 10.247.54.56	Devices > Platform Settings > SNMP > Save Admin State: Enable **Add User** *Username:* <Username> *Auth Type: SHA* *Encryption Password Type:* Use AES-128: Enable Password: ***** Confirm Password: ***** Privacy Password: ***** Confirm Privacy Password: ***** **Add SNMP Traps:** Hostname/IP Address: 2.2.2.2

			5. 10.247.32.232 Username: <EG Username> Password: ****** Version: v3 Authentication Type: SHA Privacy Protocol: AES128	Community/Username: <Username> Port: 162 Version: V3 Type: <Traps/Informs> V3 Privilege: <Auth/NoAuth/Priv> Save

5.3 Management Access Control List

SN	**Controls**	**Purpose**	**Required Settings** -All settings are mandatory unless listed as Optional.	**Configuration Reference** -The instructions are purely for reference purpose and may differ across different product versions.
5.3.1	Restrict Remote Access	Access-list is used to secure the management access to the system by IP and port.	**H-Cloud PAM Servers (HTTPS, SSH)** 1. 10.247.22.62 2. 10.247.22.20-10.247.22.22 3. 10.247.22.39-10.247.22.43 4. 10.247.22.126-10.247.22.132 5. 10.247.22.24 6. 10.247.22.77-10.247.22.79 7. 10.247.54.62 8. 10.247.54.20-10.247.54.22 9. 10.247.54.39-10.247.54.43 10. 10.247.54.122-10.247.54.129 11. 10.247.54.24 12. 10.247.54.77-10.247.54.79 13. 10.247.22.80-10.247.22.81 14. 10.247.54.81-10.247.54.82 **H-Cloud Security Utility Servers (HTTPS, SSH)** 1. 10.247.22.4 2. 10.247.54.4 **Security Compliance Server (HTTPS, SSH)** 1. 10.247.17.62 2. 10.247.22.135 **EVMS Scanner IP (HTTPS, SSH)** 1. 10.247.17.106 2. 10.247.49.98	Devices > Platform Settings > Access-list > Add > Save IP Address: <PAM/Utility Server IP Address> Prefix Length: /32 Protocol: <https/ssh/snmp>
5.3.2	Session Timeout	To limit the length of account login to secure the device from unauthorized users to exploit the unattended sessions.	***Browser Settings:*** Browser Session Timeout (Minutes): 15 ***Shell Settings:*** Shell Timeout (Minutes): 15	Firepower-chassis # scope security Firepower-chassis /security # scope default-auth Firepower-chassis /security/default-auth # set session-timeout seconds 900 Firepower-chassis /security/default-auth # commit-buffer
5.3.3	Web GUI	By default, the device uses a default self-signed certificate. To secure the information between GUI and your jump host, it is recommended to replace the certificate with a trusted certificate authority.	***Country Name:*** SG ***State of Province:*** SG ***Locality or City:*** SG ***Organization:*** SYNAPXE ***Organizational Unit:*** H-CLOUD ***Common Name:*** <Hostname>. H-Cloud.healthgrp.com.sg *Note: Certificates generated before 01 September 2023 may use*	Firepower-chassis # scope security Firepower-chassis /security # create trustpoint firepower_chain Firepower-chassis /security # set certchain Copy and paste the CA Cert Binary one line at a time enter "ENDOFBUF" at the end of the line Firepower-chassis /security # commit-buffer

			Integrated Health Information Systems for "Organization".	Firepower-chassis /security # scope keyring firepower_cert Firepower-chassis /security # set trustpoint firepower_chain #set cert Copy and paste the Signed Cert Binary one line at a time enter "ENDOFBUF" at the end of the line #commit-buffer #scope system #scope services #set https keyring firepower_cert #commit buffer
5.3.4	Local Accounts	Local admin accounts used for breakfix. Password strength check must be enabled for locally authenticated users.	**Password Policy** 1. Must contain a minimum of 15 characters 2. Must include characters from at least 2 of the following 4 categories: I. Upper case (A through Z); J. Lower case (a through z); K. Digits (0-9); L. Special Characters (!, $, #, %, etc.). 3. Password expiration must be 365days 4. Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word. 5. Not be reused for at least 5 generations 6. Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb. 7. Must not contain three consecutive numbers or letters in any order, such as passwordABC or password321. 8. Must not be identical to the username or the reverse of the username. 9. Account lockout after 5 consecutive failed authentication attempts	System > Users > Add/Delete/Edit User > Save ***User Configuration:*** User Name: First Name: Last Name: Email: example@example.com (Optional) Phone Number: +XXXXXXXXXX (Optional) Password: ***** Confirm Password: ***** Account Status: <Active/Inactive> User Role: Read-Only Admin Operations AAA Account Expires: (Optional) Expiry Date: (mm/dd/yyyy) 12months
5.3.5	External Authentication	To secure that only H-Cloud Security Engineers are able to access and make changes to the device configuration through LDAP or RADIUS authentication.	**H-Cloud LDAP Servers IP Address** List of servers to configure for HDC1 and HDC2 devices: 1. 10.247.0.11 2. 10.247.32.11 Port: 1812	Platform Settings > AAA > LDAP/RADIUS/TACACS > Add/Delete/Edit > Save **Add RADIUS Servers** IP addreses: <Pri NPS IP> Order: 1 Key: xxxx Confirm Key: xxxx

				Authorization: 1812 Timeout: 5 Retires: 1 IP addreses: <Sec NPS IP> Order: 1 Key: xxxx Confirm Key: xxxx Authorization: 1812 Timeout: 5 Retires: 1 Save **Set Authentication to Radius as Primary** System > User Management > Settings Default Authentication : RADIUS Save

6 References/Records

The following is the list of references used for this document:

- FirePower Management Centre

Firepower Management Centre Configuration Guide Version 7.2

Last Modified: 01 September 2022

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72.html

- FirePower Chassis Manager

Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide Version 2.12

Last Modified: 09 December 2022

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/2120/web-guide/b_GUI_FXOS_ConfigGuide_2120.html

- ICT Security Policy

HIM-ICT Security Policy Version 1.5
Last Modified: 29 Nov 2023
https://healthtech-im.intranet.ihis/Pages/HIM-ISP/Purpose.aspx

7 Revision History

Document Title:	Security Hardening Benchmark for Cisco FirePower Devices
Document ID:	STND-78-2143- Security Hardening Benchmark for Cisco FirePower Devices
Document Owner:	Cloud, Platform Services
Document Approver:	Head of Department (HOD), Cloud Enablement Services (CES)
Information Classification:	Restricted, Sensitive (Normal)
Special Instructions:	NA

Version	Revision Date	Summary of Changes	Documented By	Reviewed By
1.0	23-Jul-2021	Initial Document	– Marie Ann Cadiz – Sam Lee	Ho Bee Huat
1.1	16-Aug-2021	Update: -Restrict Remote Access: added HDC1 and HDC2 Jump Host IPs. -Local Accounts 1.Password expiration must be 365days 2.Not be reused for at least 5 generations	-Marie Ann Cadiz -Sam Lee	Ho Bee Huat
1.2	15-Sep-2021	Update: -Restrict Remote Access: added HDC1 and HDC2 Jump Host IPs. - Syslog: removed old MSS IP and updated to use TCP/514 for ELK and Splunk.	-Marie Ann Cadiz -Sam Lee	Ho Bee Huat
1.3	10-Oct-2021	Update: -Restrict Remote Access - Syslog	-Marie Ann Cadiz -Sam Lee	Ho Bee Huat
1.4	24-Jan-2022	Update: -Document Approver -4.2 Health Policy updated Configuration/Variable with the alert modules. -5.1 Restrict Remote Access, added EG Server IPs and management ports -5.2 Session Timeout, updated Browser and Shell Timeout to 15mins. -5.5 External Authentication, Added Radius Servers.	-Marie Ann Cadiz -Sam Lee	Kenneth Chew
1.5	20-May-2022	Update: -Individual Hardening Guide for FMC, FTD and FCM. -4.1.3 Added Event Lists	-Marie Ann Cadiz -Sam Lee	Kenneth Chew
1.6	1-Aug-2022	Update: -3.3.1 Restrict Remote Access, Updated PAM Servers and added Algosec Servers -3.3.5 External Authentication, updated 3rd LDAPS Server as Optional.	-Marie Ann Cadiz -Sam Lee	-Kenneth Chew -Stephen Tan

Version	Revision Date	Summary of Changes	Documented By	Reviewed By
		-4.3.1 Restrict Remote Access, added Algosec Servers -4.3.4 External Authentication, updated 3rd LDAPS Server as Optional.		
1.7	13-Jan-2023	-Annual Review Completed Update: -3.3.1 Restrict Remote Access, added EVMS Scanner IP -3.1.3 Syslog, Syslog Configuration via eStreamer -4.3.1 Restrict Remote Access, Added EVMS Scanner IP and alternative Method via CLI -5.3.1 Restrict Remote Access, Added EVMS Scanner IP	-Mohamed Refain -Marie Ann Cadiz	-Connie Tham -Stephen Tan -Terence Lee
1.8	01-Aug-2023	-Annual Review Completed Update: -Synapxe Template -Document Approver	-Kaiden Tan -Marie Ann Cadiz	-Connie Tham -Stephen Tan -Terence Lee
1.9	16-May-2024	Annual Review Completed Updated: -3.1.3 FMC Clock and NTP - Updated Configuration Reference to include Authentication Settings. -3.1.4 FMC Syslog - Added ASOC/OIP and removed ELK syslog servers. -3.3.3 FMC Web Gui - Updated Organization. -4.1.3 FTD Clock and NTP - Updated Configuration Steps. -4.1.4 FTD Syslog - Added OIP/CSA and removed ELK/Splunk syslog servers. -4.2.1 FTD SNMP Settings - Added OIP/CSPC Servers. -5.1.4 FCM Syslog - Added OIP and removed ELK/Splunk syslog servers. -5.2.1 FCM SNMP Settings - Added OIP Servers. -5.3.3 FCM Web Gui - Updated Organization. -5.3.5 FCM External Authentication - Updated LDAP Servers. -6 References – Updated HIM-ICT Security Policy Version 1.5.	-Mohamed Refain -Chiu Yih Tah	-Connie Tham -Stephen Tan