SNLC Baseline Configuration

Doc. Control Number	Version
SNL-47	0.2

Document Reference

Item	Description
Title	SNLC Baseline Configuration
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	13 June 2024
Revision-Date	13 June 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	13/06/2024

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	13/06/2024

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	18/06/2024

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	14 June 2023	Muhaned Ali	First Release
0.2	13 June 2024	Muhaned Ali	The document has been reviewed

Contents

1. Overview

This document defines the minimal security configuration required for any devices connected to a production network or used in a production capacity at or for SNL.

2. Scope

This policy applies to all of SNLC's informational, technical, and application assets.

3. SNLC Baseline Configuration

3.1 Cisco Routers/Switches

Every router/switch must adhere to the following configuration standards:

1- Access Rules and Configuration.

- Configure Privilege 1 for local users.
- Configure transport ssh for line vty connection.
- Configure no exec for line aux 0.
- Create access -list for use with line vty connection.
- Configure access-class for line vty connection.
- Configure exec-timeout to less than or equal to 10 minutes for line aux 0 connection.
- Configure exec-timeout to less than or equal to 10 minutes for line console 0 connection.
- Configure exec-timeout to less than or equal to 10 minutes for line vty connection.
- Configure transport input non for line aux 0

2- Banner Rules and Configuration.

- Configure the banner-text for banner exec.
- Configure the banner-text for banner login.
- Configure the banner-text for banner motd.

3- Password Rules and Configuration

- Configure password enable secret.
- Configure enable service password-encryption.
- Configure username secret for all local users.

4- SNMP Rules and Configuration.

- Configure no snmp-server to disable SNMP when unused.
- Unset private for snmp-server community.
- Unset public for snmp-server community.
- Configure snmp-server host when using SNMP.
- Configure snmp-server enable traps snmp.
- Configure AES 128 encryption as minimum for snmp-server user when using SNMPv3

5- Control Plane for Global Service Rules and Configuration.

- Setup SSH Version 2
- Setup the hostname.
- Setup the ip domain-name.
- Set modulus to greater or equal 2048 for crypto key generate.
- Set second for ip ssh time timeout.
- Configure no cdp run.
- Configure no ip domain-lookup.
- Configure no ip bootup server.
- Configure no service dhcp.
- Configure no ip identd.
- Configure no service tcp-small service.
- Configure no service udp-small service.
- Configure no feature http-server.
- Configure no ip http secure server.

- Configure no ip finger.
- Configure no service finger.
- Configure transport input ssh.
- Configure no ftp service enable.
- Configure no http server.
- Configure no ip http secure-server.

6- NTP Rules and Configuration.
- Configure Encryption Keys for NTP.
- Configure ntp authenticate.
- Configure ntp authentication-key
- Configure ntp trusted-key.
- Configure key for each ntp server.
- Configure ip address for ntp server.

7- Routing Rules and Configuration.
- Configure no ip source-route.
- Configure no ip proxy-arp
- Configure no interface tunnel.
- Configure verify unicast source reachable-via

8- Border Router Filtering and Configuration.
- Configure ip access-list extended to Forbid Private Source Addresses.
- Configure inbound ip access-group one the External Interface.

9- EIGRP Authentication, require if protocol is used.
- Configure key chain.
- Configure key.
- Configure key-string.
- Configure address-family ipv4 autonomous-system.
- Configure af-interface default.
- Configure authentication key-chain.
- Configure authentication mode md5.
- Configure authentication key-chain eigrp.
- Configure ip authentication mode eigrp.

10- Require OSPF Authentication if Protocol is use.
- Configure authentication message-digest for OSPF area.
- Configure ip ospf message-digest-key md5.

11- Require RIPV2 Authentication if protocol is used.
- Configure Key chain.
- Configure key.
- Configure key-string.
- Configure ip rip authentication key chain.
- Configure ip rip authentication md5

12- Require BGP Authentication if Protocol is used.
- Configure neighbor password.

3.2 FortiGate Firewall

1) Building security into FortiOS
The FortiOS operating system, FortiGate hardware devices, and FortiGate virtual machines (VMs) are built with security in mind, so many security features are built into the hardware and software. Fortinet maintains an ISO:9001 certified software and hardware development processes to ensure that FortiOS and FortiGate products are developed in a secure manner.

2) Boot PROM and BIOS security

The boot PROM and BIOS in FortiGate hardware devices use Fortinet's own FortiBootLoader that is designed and controlled by Fortinet. FortiBootLoader is a secure, proprietary BIOS for all FortiGate appliances. FortiGate physical devices always boot from FortiBootLoader.

3) FortiOS kernel and user processes
   FortiOS is a multi-process operating system with kernel and user processes. The FortiOS kernel runs in a privileged hardware mode while higher-level applications run in user mode. FortiOS is a closed system that does not allow the loading or execution of third-party code in the FortiOS user space. All non-essential services, packages, and applications are removed.
4) Administration access security
   This section describes FortiOS and FortiGate administration access security features.
   As the first step on a new deployment, review default settings such as administrator passwords, certificates for GUI and SSL VPN access, SSH keys, open administrative ports on interfaces, and default firewall policies. As soon as the FortiGate is connected to the internet it is exposed to external risks, such as unauthorized access, man-in-the-middle attacks, spoofing, DoS attacks, and other malicious activities from malicious actors. Either use the startup wizard or manually reconfigure the default settings to tighten your security from the beginning, thereby securing your network to its full potential.
5) Admin administrator account
   All FortiGate firewalls ship with a default administrator account called admin. By default, this account does not have a password, except for FortiGate VMs on public clouds. FortiOS allows administrators to add a password for this account or to remove the account and create new custom super_admin administrator accounts.
6) Secure password storage
   The passwords, and private keys used in certificates, that are stored on the FortiGate are encrypted using a predefined private key and encoded when displayed in the CLI and configuration file.
   Passwords cannot be decrypted without the private key and are not shown anywhere in clear text. The private key is required on other FortiGate's to restore the system from a configuration file. In an HA cluster, the same key should be used on all the units.
   To enhance password security, specify a custom private key for the encryption process. This ensures that the key is only known by you.
   FortiGate models with a Trusted Platform Module (TPM) can store the master encryption password, which is used to generate the master encryption key, on the TPM.
   To configure your own private encryption key:

```
config system global
set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
********************************
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
********************************
        Your private data encryption key is accepted.
```

7) Maintainer account
   Administrators with physical access to a FortiGate appliance can use a console cable and a special administrator account called maintainer to log into the CLI. When enabled, the maintainer account can be used to log in from the console after a hard reboot. The password for the maintainer account is bcpb followed by the FortiGate serial number.
   An administrator has 60 seconds to complete this login.
   The only action the maintainer account has permissions to perform is to reset the passwords of super_admin accounts.

Logging in with the maintainer account requires a hard boot of the FortiGate. FortiOS generates event log messages when you log in with the maintainer account and for each password reset.
The maintainer account is enabled by default; however, there is an option to disable this feature. The maintainer account can be disabled using the following command:

```
config system global
   set admin-maintainer disable
 end
```

8) Administrative access security
Secure administrative access features:

- SSH, Telnet, and SNMP are disabled by default. If required, these admin services must be explicitly enabled on each interface from the GUI or CLI.
- SSHv1 is disabled by default. SSHv2 is the default version.
- SSLv3 and TLS1.0 are disabled by default. TLSv1.1 and TLSv1.2 are the SSL versions enabled by default for HTTPS admin access.
- HTTP is disabled by default, except on dedicated MGMT, DMZ, and predefined LAN interfaces. HTTP redirect to HTTPS is enabled by default.
- The strong-crypto global setting is enabled by default and configures FortiOS to use strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH/TLS/SSL functions.
- SCP is disabled by default. Enabling SCP allows downloading the configuration file from the FortiGate as an
- Alternative method of backing up the configuration file. To enable SCP:

```
config system global
   set admin-scp enable
end
```

- DHCP is enabled by default on the dedicated MGMT interface and on the predefined LAN port (defined on some FortiGate models).
- The default management access configuration for FortiGate models with dedicated MGMT, DMZ, WAN, and LAN interfaces is shown below. Outside of the interfaces listed below, management access must be explicitly enabled on interfaces – management services are enabled on specific interfaces and not globally.
- Dedicated management interface
  - Ping
  - FMG-Access (fgfm)
  - CAPWAP
  - HTTPS
  - HTTP
- Dedicated WAN1/WAN2 interface
  - Ping
  - FMG-Access (fgfm)
- Dedicated DMZ interface
  - Ping
  - FMG-Access (fgfm)
  - CAPWAP
  - HTTPS
  - HTTP
- Dedicated LAN interface
  - Ping
  - FMG-Access (fgfm)
  - CAPWAP
  - HTTPS

- HTTP

9) Non-factory SSL certificates
Non-factory SSL certificates should be used for the administrator and SSL VPN portals. Your certificate should identify your domain so that remote users can recognize the identity of the server or portal that they are accessing through a trusted CA.
The default Fortinet factory self-signed certificates are provided to simplify initial installation and testing. Using these certificates leaves you vulnerable to man-in-the-middle attacks, where an attacker spoofs your certificate, compromises your connection, and steals your personal information.
It is highly recommended that you purchase a server certificate from a trusted CA to allow remote users to connect to SSL VPN with confidence. Your administrator web portal should also be configured with a server certificate from a trusted CA.

10) Network security
This section describes FortiOS and FortiGate network security features.
   - Network interfaces
     The following are disabled by default on each FortiGate interface:
     - Broadcast forwarding
     - STP forwarding
     - VLAN forwarding
     - L2 forwarding
     - Netbios forwarding
     - Ident accept
   - TCP sequence checking
     FortiOS uses TCP sequence checking to ensure a packet is part of a TCP session. By default, anti-replay protection is strict, which means that if a packet is received with sequence numbers that fall out of the expected range, FortiOS drops the packet. Strict anti-replay checking performs packet sequence checking and ICMP anti-replay checking with the following criteria:
     - The SYN, FIN, and RST bit cannot appear in the same packet.
     - FortiOS does not allow more than 1 ICMP error packet to go through before it receives a normal TCP or UDP packet.
     - If FortiOS receives an RST packet, FortiOS checks to determine if its sequence number in the RST is within the un-ACKed data and drops the packet if the sequence number is incorrect.
     - For each new session, FortiOS checks to determine if the TCP sequence number in a SYN packet has been calculated correctly and started from the correct value.
   - Reverse path forwarding
     FortiOS implements a mechanism called Reverse Path Forwarding (RPF), or Anti Spoofing, to block an IP packet from being forwarded if its source IP does not:
     - belong to a locally attached subnet (local interface), or
     - be in the routing domain of the FortiGate from another source (static route, RIP, OSPF, BGP).
       If those conditions are not met, FortiOS silently drops the packet.

11) FIPS and Common Criteria
FortiOS has received NDPP, EAL2+, and EAL4+ based FIPS and Common Criteria certifications. Common Criteria evaluations involve formal rigorous analysis and testing to examine security aspects of a product or system. Extensive testing activities involve a comprehensive and formally repeatable process, confirming that the security product

functions as claimed by the manufacturer. Security weaknesses and potential vulnerabilities are specifically examined during an evaluation.

12) PSIRT advisories

The FortiGuard Labs Product Security Incident Response Team (PSIRT) continually tests and gathers information about Fortinet hardware and software products, looking for vulnerabilities and weaknesses. Any such findings are fed back to Fortinet's development teams and serious issues are described along with protective solutions.

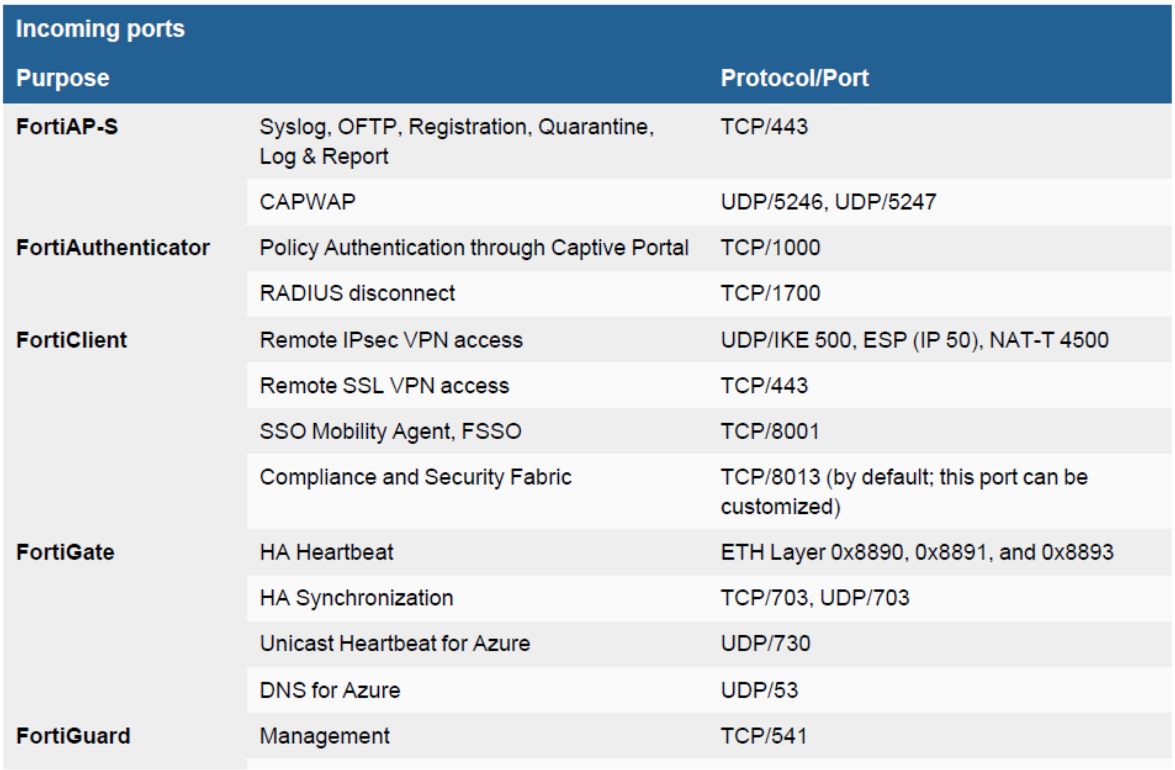
13) FortiOS ports and protocols

Communication to and from FortiOS is strictly controlled and only selected ports are opened for supported functionality such as administrator logins and communication with other Fortinet products or services.

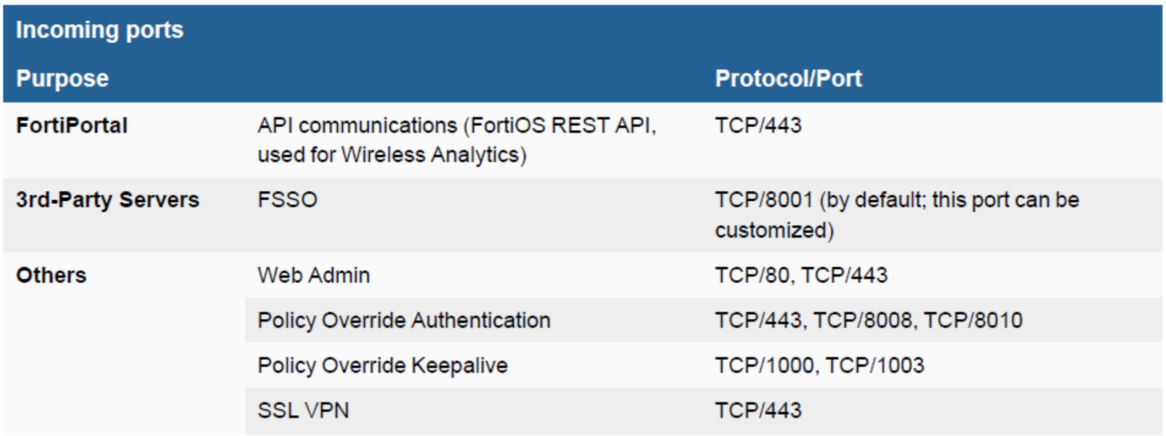
Accessing FortiOS using an open port is protected by authentication, identification, and encryption requirements. Also, ports are only open if the feature using them is enabled.

a) FortiOS open ports

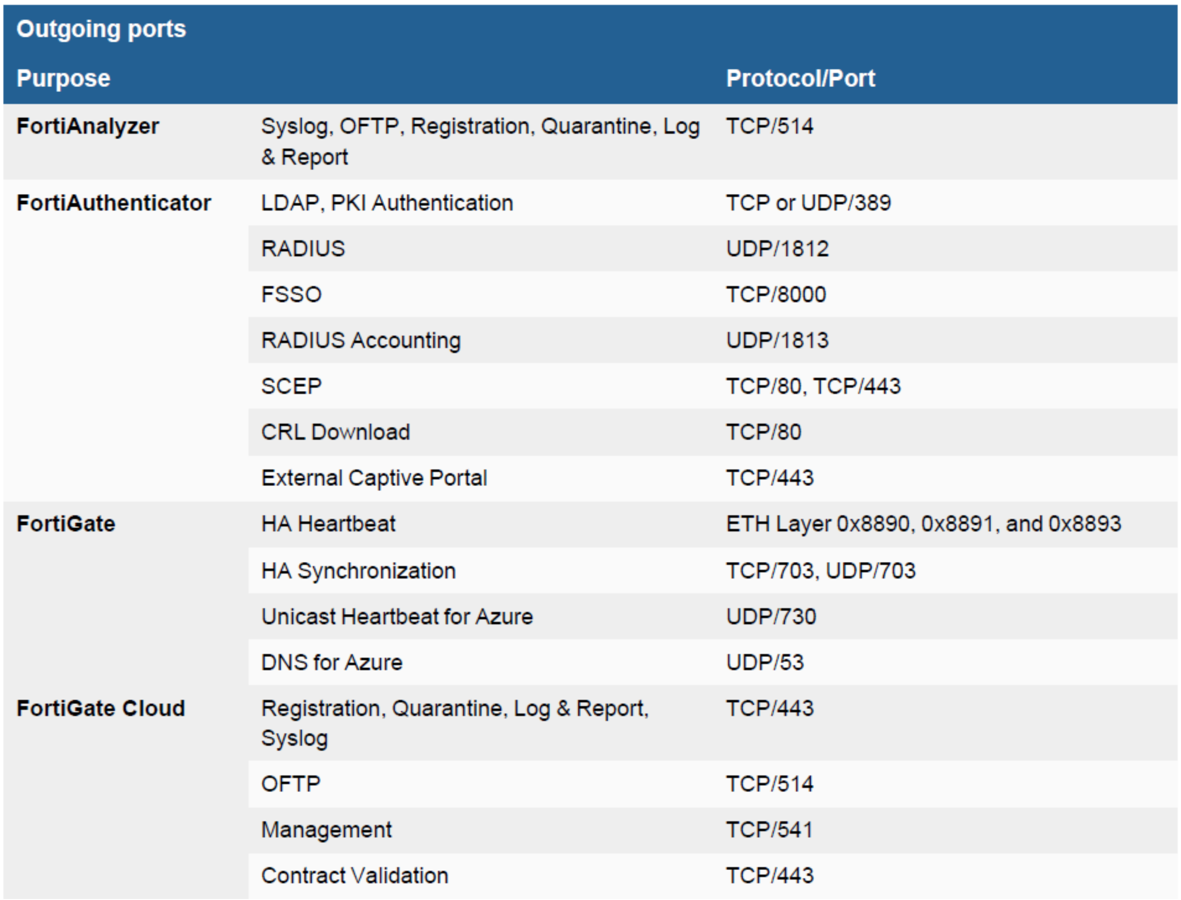
The following tables show the incoming and outgoing ports that are potentially opened by FortiOS.



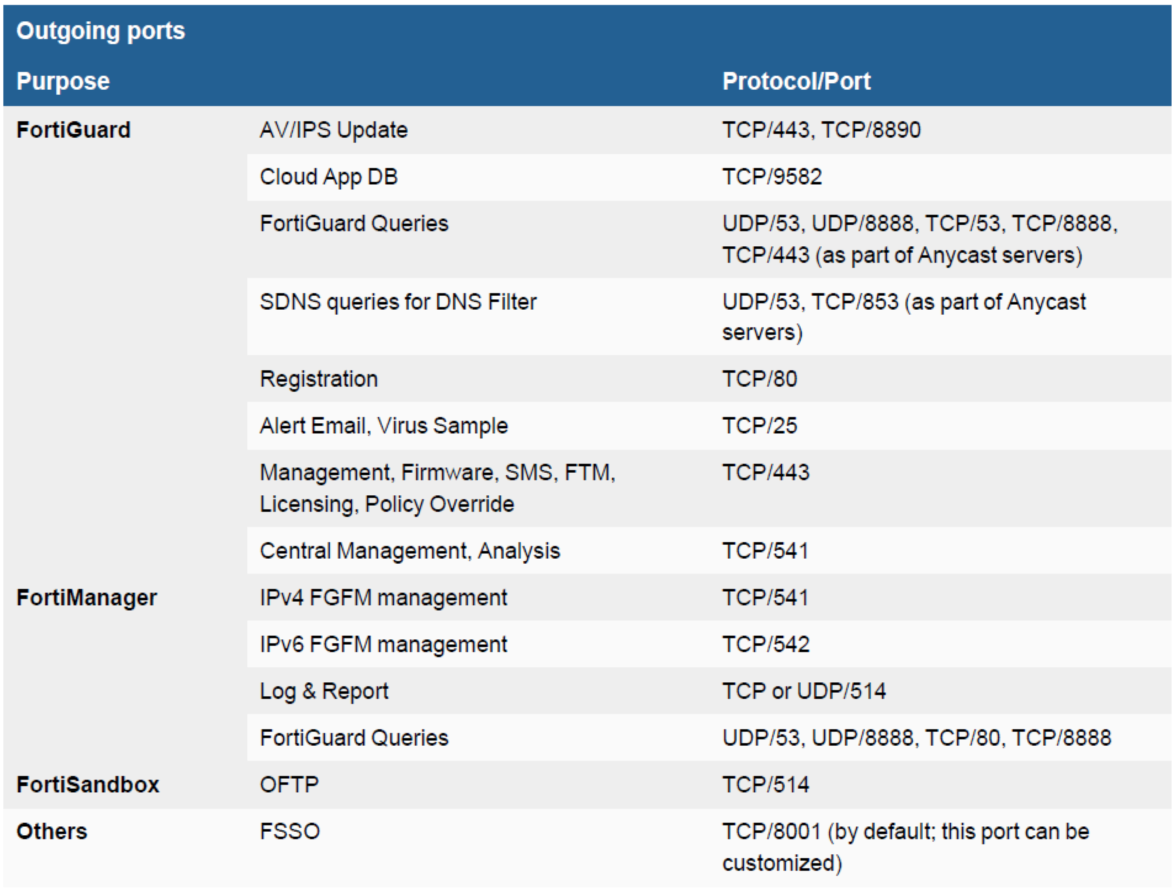
Incoming ports		
Purpose		**Protocol/Port**
FortiAP-S	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/443
	CAPWAP	UDP/5246, UDP/5247
FortiAuthenticator	Policy Authentication through Captive Portal	TCP/1000
	RADIUS disconnect	TCP/1700
FortiClient	Remote IPsec VPN access	UDP/IKE 500, ESP (IP 50), NAT-T 4500
	Remote SSL VPN access	TCP/443
	SSO Mobility Agent, FSSO	TCP/8001
	Compliance and Security Fabric	TCP/8013 (by default; this port can be customized)
FortiGate	HA Heartbeat	ETH Layer 0x8890, 0x8891, and 0x8893
	HA Synchronization	TCP/703, UDP/703
	Unicast Heartbeat for Azure	UDP/730
	DNS for Azure	UDP/53
FortiGuard	Management	TCP/541



Incoming ports		
Purpose		**Protocol/Port**
FortiPortal	API communications (FortiOS REST API, used for Wireless Analytics)	TCP/443
3rd-Party Servers	FSSO	TCP/8001 (by default; this port can be customized)
Others	Web Admin	TCP/80, TCP/443
	Policy Override Authentication	TCP/443, TCP/8008, TCP/8010
	Policy Override Keepalive	TCP/1000, TCP/1003
	SSL VPN	TCP/443



Outgoing ports		
Purpose		**Protocol/Port**
FortiAnalyzer	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
FortiAuthenticator	LDAP, PKI Authentication	TCP or UDP/389
	RADIUS	UDP/1812
	FSSO	TCP/8000
	RADIUS Accounting	UDP/1813
	SCEP	TCP/80, TCP/443
	CRL Download	TCP/80
	External Captive Portal	TCP/443
FortiGate	HA Heartbeat	ETH Layer 0x8890, 0x8891, and 0x8893
	HA Synchronization	TCP/703, UDP/703
	Unicast Heartbeat for Azure	UDP/730
	DNS for Azure	UDP/53
FortiGate Cloud	Registration, Quarantine, Log & Report, Syslog	TCP/443
	OFTP	TCP/514
	Management	TCP/541
	Contract Validation	TCP/443



Outgoing ports		
Purpose		**Protocol/Port**
FortiGuard	AV/IPS Update	TCP/443, TCP/8890
	Cloud App DB	TCP/9582
	FortiGuard Queries	UDP/53, UDP/8888, TCP/53, TCP/8888, TCP/443 (as part of Anycast servers)
	SDNS queries for DNS Filter	UDP/53, TCP/853 (as part of Anycast servers)
	Registration	TCP/80
	Alert Email, Virus Sample	TCP/25
	Management, Firmware, SMS, FTM, Licensing, Policy Override	TCP/443
	Central Management, Analysis	TCP/541
FortiManager	IPv4 FGFM management	TCP/541
	IPv6 FGFM management	TCP/542
	Log & Report	TCP or UDP/514
	FortiGuard Queries	UDP/53, UDP/8888, TCP/80, TCP/8888
FortiSandbox	OFTP	TCP/514
Others	FSSO	TCP/8001 (by default; this port can be customized)

b) Closing open ports

You can close open ports by disabling the feature that opens them. For example, if FortiOS is not managing a FortiAP then the CAPWAP feature for managing FortiAPs can be disabled, closing the CAPWAP port.

The following sections of this document described several options for closing open ports:

- Use local-in policies to close open ports or restrict access.
- Disable unused protocols on interfaces.

14) Security best practices

This section describes some techniques and best practices that you can use to improve FortiOS security.

1- Install the FortiGate unit in a physically secure location.

A good place to start with is physical security. Install your FortiGate in a secure location, such as a locked room or one with restricted access. A restricted location prevents unauthorized users from getting physical access to the device. If unauthorized users have physical access, they can disrupt your entire network by disconnecting your FortiGate (either by accident or on purpose). They could also connect a console cable and attempt to log into the CLI. Also, when a FortiGate unit reboots, a person with physical access can interrupt the boot process and install different firmware.

2- Register your product with Fortinet Support

You need to register your Fortinet product with Fortinet Support to receive customer services, such as firmware updates and customer support. You must also register your product for FortiGuard services, such as up-to-date antivirus and IPS signatures.

3- Keep your FortiOS firmware up to date

Always keep FortiOS up to date. The most recent version is the most stable and has the most bugs fixed, and vulnerabilities removed. Fortinet periodically updates the FortiGate firmware to include new features and resolve important issues.

After you register your FortiGate, you can receive notifications on FortiGate GUI about firmware updates. You can update the firmware directly from GUI or by downloading firmware updates from the Fortinet Support website.

Before you install any new firmware, be sure to follow these steps:

- Review the release notes for the latest firmware release.
- Review the Upgrade Path tool to determine the best path to take from your current version of FortiOS to the latest version.
- Back up the current configuration.

Only FortiGate administrators who have read and write privileges can upgrade the FortiOS firmware.

15) System administrator best practices

This section describes a collection of changes you can implement to make administrative access to the GUI and CLI more secure.

1- Disable administrative access to the external (Internet-facing) interface.

When possible, don’t allow administration access on the external (Internet-facing) interface.

To disable administrative access, go to Network > Interfaces, edit the external interface and disable HTTPS, PING, HTTP, SSH, and TELNET under Administrative Access.

From the CLI:

```
config system interface
   edit <external-interface-name>
   unset allowaccess
 end
```

2- Allow only HTTPS access to the GUI and SSH access to the CLI

For greater security never allow HTTP or Telnet administrative access to a FortiGate interface, only allow HTTPS and SSH access. You can change these settings for individual interfaces by going to Network > Interfaces and adjusting the administrative access to each interface.

From the CLI:

```
config system interface
   edit <interface-name>
   set allowaccess https ssh
 end
```

3- Require TLS 1.2 for HTTPS administrator access

Use the following command to require TLS 1.2 for HTTPS administrator access to the GUI:

```
 config system global
   set admin-https-ssl-versions tlsv1-2
 end
```

TLS 1.2 is currently the most secure SSL/TLS supported version for SSL-encrypted administrator access.

4- Re-direct HTTP GUI logins to HTTPS

Go to System > Settings > Administrator Settings and enable Redirect to HTTPS to make sure that all attempted HTTP login connections are redirected to HTTPS.

From the CLI:

```
config system global
   set admin-https-redirect enable
 end
```

5- Change the HTTPS and SSH admin access ports to non-standard ports

Go to System > Settings > Administrator Settings and change the HTTPS and SSH ports.

You can change the default port configurations for HTTPS and SSH administrative access for added security. To connect to a non-standard port, the new port number must be included in the collection request. For example:

- If you change the HTTPS port to 7734, you will browse to `https://<ip-address>:7734.`
- If you change the SSH port to 2345, you will connect to `ssh admin@<ip-address>:2345`

To change the HTTPS and SSH login ports from the CLI:

```
config system global
   set admin-sport 7734
   set admin-ssh-port 2345
 end
```

If you change to the HTTPS or SSH port numbers, make sure your changes do not conflict with ports used for other services.

6- Maintain short login timeouts

Set the idle timeout to a short time to avoid the possibility of an administrator walking away from their management computer and leaving it exposed to unauthorized personnel.

To set the administrator idle timeout, go to System > Settings and enter the amount of time for the Idle timeout. The best practice is to keep the default time of 5 minutes.

To set the administrator idle timeout from the CLI:

```
 config system global
     set admintimeout 5
end
```

You can use the following command to adjust the grace time permitted between making an SSH connection and authenticating. The range can be between 10 and 3600 seconds, the default is 120 seconds (minutes). By shortening this time, you can decrease the chances of someone attempting a brute force attack a from being successful. For example, you could set the time to 30 seconds.

```
 config system global
     set admin-ssh-grace-time 30
end
```

7- Restrict logins from trusted hosts

Setting up trusted hosts for an administrator limits the addresses from where they can log into FortiOS. The trusted hosts configuration applies to most forms of administrative access including HTTPS, SSH, and SNMP. When you identify a trusted host for an administrator account, FortiOS accepts that administrator's login only from one of the trusted hosts. A login, even with proper credentials, from a non-trusted host is dropped.

To identify trusted hosts, go to System > Administrators, edit the administrator account, enable Restrict login to trusted hosts, and add up to ten trusted host IP addresses.

To add two trusted hosts from the CLI:

```
config system admin
   edit <administrator-name>
      set trustedhost1 172.25.176.23 255.255.255.255
      set trustedhost2 172.25.177.0 255.255.255.0
 end
```

8- Trusted host IP addresses can identify individual hosts or subnets.

Just like firewall policies, FortiOS searches through the list of trusted hosts in order and acts on the first match it finds. When you configure trusted hosts, start by adding specific addresses at the top of the list. Follow with more general IP addresses. You don't have to add addresses to all the trusted hosts as long as all specific addresses are above all of the 0.0.0.0 0.0.0.0 addresses.

9- Set up two-factor authentication for administrators

FortiOS supports FortiToken and FortiToken Mobile 2-factor authentication. FortiToken Mobile is available for iOS and

Android devices from their respective application stores.

Every registered FortiGate unit includes two trial tokens for free. You can purchase additional tokens from your reseller or from Fortinet.

To assign a token to an administrator, go to System > Administrators and select Enable Two-factor Authentication for each administrator.

10- Create multiple administrator accounts

Rather than allowing all administrators to access ForiOS with the same administrator account, you can create accounts for each person or each role that requires administrative access. This configuration allows you to track the activities of each administrator or administrative role.

If you want administrators to have different functions, you can add different administrator profiles. Go to System > Admin Profiles and select Create New.

11- Modify administrator account lockout duration and threshold values

By default, FortiGate sets the number of passwords retries at three, allowing the administrator a maximum of three attempts to log into their account before locking the account for a set amount of time.

Both the number of attempts (`admin-lockout-threshold`) and the wait time before the administrator can try to enter a password again (`admin-lockout-duration`) can be configured within the CLI.

To configure the lockout options:

```
config system global
   set admin-lockout-threshold <failed_attempts>
   set admin-lockout-duration <seconds>
end
```

The default value of admin-lockout-threshold is 3 and the range of values is between 1 and 10. The adminlockout-duration is set to 60 seconds by default and the range of values is between 1 and 4294967295 seconds.

Keep in mind that the higher the lockout threshold, the higher the risk that someone may be able to break into the FortiGate.

12- Add administrator disclaimers

FortiOS can display a disclaimer before or after logging into the GUI or CLI (or both). In either case the administrator must read and accept the disclaimer before they can proceed.

Use the following command to display a disclaimer before logging in:

```
config system global
   set pre-login-banner enable
end
```

Use the following command to display a disclaimer after logging in:

```
config system global
   set post-login-banner enable
end
```

You can customize the replacement messages for these disclaimers by going to System > Replacement Messages. Select Extended View to view and edit the Administrator replacement messages.

From the CLI:

```
config system replacemsg admin pre_admin-disclaimer-text
config system replacemsg admin post_admin-disclaimer-text
```

16) Global commands for stronger and more secure encryption

This section describes some best practices for employing stronger and more secure encryption.

1- Turn on global strong encryption

Enter the following command to configure FortiOS to use only strong encryption and allow only strong ciphers (AES,3DES) and digest (SHA1) for HTTPS, SSH, TLS, and SSL functions.

```
config system global
  set strong-crypto enable
end
```

2- Disable MD5 and CBC for SSH

In some cases, you may not be able to enable strong encryption. For example, your FortiGate may be communicating with a system that does not support strong encryption. With `strong-crypto` disabled you can use the following options to prevent SSH sessions with the FortiGate from using less secure MD5 and CBC algorithms:

```
 config system global
    set ssh-hmac-md5 disable
    set ssh-cbc-cipher disable
end
```

3- Disable static keys for TLS

You can use the following command to prevent all TLS sessions that are terminated by FortiGate from using static keys (AES128-SHA, AES256-SHA, AES128-SHA256, AES256-SHA256):

```
 config system global
     set ssl-static-key-ciphers disable
end
```

4- Require larger values for Diffie-Hellman exchanges

Larger Diffie-Hellman values result in stronger encryption. Use the following command to force Diffie-Hellman exchanges to use 8192 bit values (the highest configurable DH value).

```
config system global
    set dh-params 8192
 end
```

5- Disable auto USB installation

If USB installation is enabled, an attacker with physical access to a FortiGate could load a new configuration or firmware on the FortiGate using the USB port. You can disable USB installation by entering the following from the CLI:

```
config system auto-install
   set auto-install-config disable
   set auto-install-image disable
end
```

6- Set system time by synchronizing with an NTP server

For accurate time, use an NTP server to set system time. Synchronized time facilitates auditing and consistency between expiry dates used in expiration of certificates and security protocols.

From the GUI go to System > Settings > System Time and select Synchronize with NTP Server. By default, this causes FortiOS to synchronize with Fortinet's FortiGuard secure NTP server.

From the CLI you can use one or more different NTP servers:

```
 config system ntp
     set type custom
     set ntpsync enable
       config ntpserver
         edit 1
           set server <ntp-server-ip>
       next
       edit 2
          set server <other-ntp-server-ip>
   end
```

7- Disable the maintainer admin account

Administrators with physical access to a FortiGate appliance can use a console cable and a special administrator account called maintainer to log into the CLI.

The maintainer account allows you to log into a FortiGate if you have lost all administrator passwords.

- Once you have logged in with the maintainer account you can:
  Change the password of the admin administrator account (if it exists).
- Reset the FortiGate to the factory default configuration using the `execute factoryreset` command. This is the only way to get access to FortiGate if you have deleted the admin administrator account.

The methodology for using the maintainer account is publicly available. As long as someone with physical access to the device has the serial number of the device, which is labeled on the device, they can change the admin administrator account password and access the FortiGate. This may be an unacceptable risk in some circumstances, especially where the hardware is not physically secured. As an added security measure, the maintainer account can be disabled using the following setting:

```
config system global
    set admin-maintainer disable
end
```

8- Enable password policies

Go to System > Settings > Password Policy, to create a password policy that all administrators must follow. Using the available options you can define the required length of the password, what it must contain (numbers, upper and lower case, and so on) and an expiry time.

Use the password policy feature to make sure all administrators use secure passwords that meet your organization's requirements.

9- Configure auditing and logging

For optimum security go to Log & Report > Log Settings enable Event Logging. For the best results send log messages to FortiAnalyzer or FortiCloud.

From FortiAnalyzer or FortiCloud, you can view reports or system event log messages to look for system events that may indicate potential problems. You can also view system events by going to FortiView > System Events.

Establish an auditing schedule to routinely inspect logs for signs of intrusion and probing.

10- Encrypt logs sent to FortiAnalyzer/FortiManager

To keep information in log messages sent to FortiAnalyzer private, go to Log & Report > Log Settings and when you configure Remote Logging to FortiAnalyzer/FortiManager select Encrypt log transmission.

From the CLI.

```
config log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
   set enc-algorithm high
end
```

11- Disable unused interfaces

To disable an interface from the GUI, go to Network > Interfaces. Edit the interface to be disabled and set Interface State to Disabled.

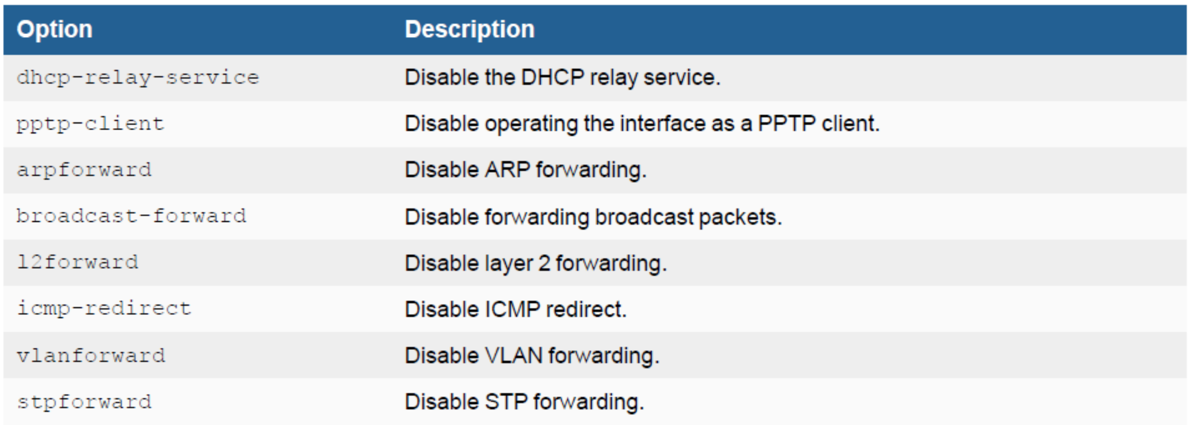
From the CLI, to disable the port21 interface:

```
config system interface
  edit port21
    set status down
end
```

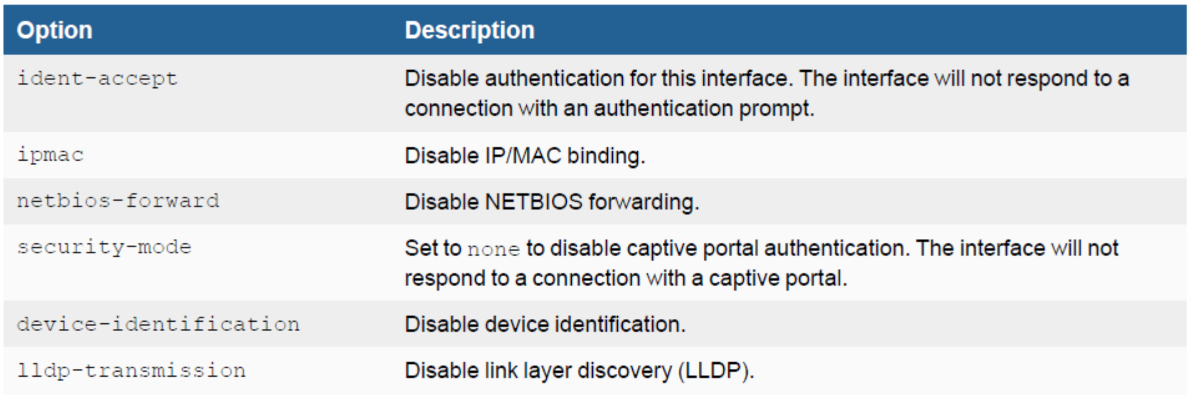
12- Disable unused protocols on interfaces

You can use the config system interface command to disable unused protocols that attackers may attempt to use to gather information about a FortiGate unit. Many of these protocols are disabled by default. Using the config system interface command, you can see the current configuration of each of these options for the selected interface and then choose to disable them if required.

```
config system interface
   edit <interface-name>
      set dhcp-relay-service disable
      set pptp-client disable
      set arpforward disable
      set broadcast-forward disable
      set l2forward disable
      set icmp-redirect disable
      set vlanforward disable
      set stpforward disable
      set ident-accept disable
      set ipmac disable
      set netbios-forward disable
      set security-mode none
      set device-identification disable
      set lldp-transmission disable
   end
```



Option	Description
dhcp-relay-service	Disable the DHCP relay service.
pptp-client	Disable operating the interface as a PPTP client.
arpforward	Disable ARP forwarding.
broadcast-forward	Disable forwarding broadcast packets.
l2forward	Disable layer 2 forwarding.
icmp-redirect	Disable ICMP redirect.
vlanforward	Disable VLAN forwarding.
stpforward	Disable STP forwarding.



Option	Description
ident-accept	Disable authentication for this interface. The interface will not respond to a connection with an authentication prompt.
ipmac	Disable IP/MAC binding.
netbios-forward	Disable NETBIOS forwarding.
security-mode	Set to none to disable captive portal authentication. The interface will not respond to a connection with a captive portal.
device-identification	Disable device identification.
lldp-transmission	Disable link layer discovery (LLDP).

17) Use local-in policies to close open ports or restrict access

You can also use local-in policies to close open ports or otherwise restrict access to FortiOS.

1- Close ICMP ports

Use the following command to close all ICMP ports on the WAN1 interface. The following example blocks traffic that matches the ALL_ICMP firewall service.

```
config firewall local-in-policy
   edit 1
      set intf wan1
      set scraddr all
      set dstaddr all
      set action deny
      set service ALL_ICMP
      set schedule always
  end
```

2- Close the BGP port

Use the following command to close the BGP port on the wan1 interface. The following example blocks traffic that matches the BGP firewall service.

```
    config firewall local-in-policy
       edit 1
         set intf wan1
         set scraddr all
         set dstaddr all
         set action deny
         set service BGP
         set schedule always
end
```

3.3 Windows 10, 11

Every Windows 10,11 adhere to the following configuration standards.

1- Password Policy Configurations.
   - Ensure Enforce password history is to 12 passwords.
   - Ensure Maximum password age is to 90.
   - Ensure Minimum password age is to 1 or more days.
   - 'Minimum password length' is set to 8 or more character.
   - Ensure Password must meet the complexity requirements is set to enabled.
   - Ensure Relax minimum password length limits is set to Enabled.
   - Ensure Store password using reversible encryption is set to Disabled.

2- Account Lockout Policy.
   - Ensure Account lockout duration is set to 15 minutes or more.
   - Ensure Account lockout threshold is set to 5 or fewer invalid logon attempts.
   - Ensure Allow Administrator account lockout is set to Enabled.
   - Ensure Reset account lockout counter after is set to 14 or more minutes.

3- Local Policies.
   - Ensure allow log on locally is set to Administrator Users.
   - Ensure Allow log on through Remote Desktop Services is set to Administrator Remote desktop user.
   - Ensure Backup files and directories is set to Administrator.
   - Ensure Change the system time is set to Administrator.
   - Ensure Change the time zone is set to Administrator.
   - Ensure Create a page file is set to Administrator.
   - Ensure Create permanent shared objects is to No One.
   - Ensure Debug programs is set to Administrator.
   - Ensure Force Shutdown from a remote is set to Administrators.

- Ensure Generate security audits is set to LOCAL SERVICE NETWORK SERVICE.
- Ensure Load and unload device drivers is set to administrators.
- Ensure Manage auditing and security log is set Administrators.
- Ensure Modify in Object label is set to No One.
- Ensure Modify firmware environment values is set to Administrators.
- Ensure perform volume task is set to Administrator.
- Ensure Restore files and directories are set to administrator.
- Ensure Shutdown the system is set to Administrator.

4- Security Options of Account.
- Ensure Account: Block Microsoft account is set Users can not add or log on with Microsoft account.
- Ensure Account: Guest Account status is set to Disabled.
- Configure Account: Rename Administrator account.

5- Audit.
- Ensure Audit: Force audit policy subcategory setting (windows vista or later to override audit policy settings is set to Enabled.
- Ensure Audit: Shutdown system immediately if unable to log security audits is set to Disabled.

6- Devices.
- Ensure Devices: Prevent users from installing printer drivers is set to Enabled.

7- Interactive logon
- Ensure interactive logon: Do not require CTRL+ALT+DEL is set to Disabled.
- Ensure interactive logon: Don not display last signed-in is set to Enabled.
- Ensure interactive logon: Machine account lockout threshold is set to 5 or fewer invalid logon attempts but not 0.
- Configure interactive logon: Message text for users attempting to log on.
- Ensure interactive logon: prompt user to change password before expiration is set between t5 and 14 days.

8- Microsoft Network Client.
- Ensure Microsoft network client: Digitally sign communication always is set to Enabled.
- Ensure Microsoft network client: Digitally sign communication if server agrees is set to Enabled.
- Ensure Microsoft network client: Send unencrypted password to third-parties SMB servers is set to Disabled.

9- Network Access.
- Allow anonymous SID/Name translation is set to Disabled.
- Do not allow anonymous enumeration of SAM accounts and shares is set to Enabled.
- Do not allow anonymous enumeration of SAM accounts is set to Enabled.
- Do not allow storage of passwords and credentials for network authentication is set to Enabled.
- Let Everyone permission apply to anonymous users is set to Disabled.
- Restricting anonymous access to Named pipes and shares is set to Enabled.
- Share that can be accessed anonymously is set to None.

10- User Account Control.
- Admin approval mode for the Built-in Administrator Account is set to Enabled.
- Detect Applications installation and prompt for elevation is set enabled.
- Virtualize file and registry write failures to per-user locations is set to enabled.
- Run All administrators in admin approval mode are to enabled.

11- System Services.
- Ensure Bluetooth and Audio Gateway Service is set Disable.
- Ensure 'Bluetooth Support Service (bthserv)' is set to 'Disabled'.

- Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed'
- Ensure 'Downloaded Maps Manager (MapsBroker)' is set to 'Disabled.
- Ensure 'Geolocation Service (lfsvc)' is set to 'Disabled.
- Ensure 'IIS Admin Service (IISADMIN)' is set to 'Disabled' or 'Not Installed.
- Ensure 'Infrared monitor service (irmon)' is set to Disabled' or 'Not Installed.
- Ensure 'Internet Connection Sharing (ICS) (SharedAccess)' is set to 'Disabled.
- Ensure 'Link-Layer Topology Discovery Mapper (lltdsvc)' is set to 'Disabled.
- Ensure 'LxssManager (LxssManager)' is set to 'Disabled' or 'Not Installed.
- Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Disabled' or 'Not Installed.
- Ensure 'Microsoft iSCSI Initiator Service (MSiSCSI)' is set to 'Disabled.
- Ensure 'OpenSSH SSH Server (sshd)' is set to 'Disabled' or 'Not Installed.
- Ensure 'Peer Name Resolution Protocol (PNRPsvc)' is set to 'Disabled.
- E Ensure 'Peer Networking Identity Manager (p2pimsvc)'
- is set to 'Disabled nsure 'Peer Networking Grouping (p2psvc)' is set to 'Disabled'.
- Ensure 'PNRP Machine Name Publication Service (PNRPAutoReg)' is set to 'Disabled.
- Ensure 'Print Spooler (Spooler)' is set to 'Disabled.
- Ensure 'Problem Reports and Solutions Control Panel Support (wercplsupport)' is set to 'Disabled.
- Ensure 'Remote Access Auto Connection Manager (RasAuto)' is set to 'Disabled.
- Ensure 'Remote Desktop Configuration (SessionEnv)' is set to 'Disabled.
- Ensure 'Remote Desktop Services (TermService)' is set to 'Disabled.
- Ensure 'Remote Desktop Services UserMode Port Redirector (UmRdpService)' is set to 'Disabled.
- Ensure 'Remote Procedure Call (RPC) Locator (RpcLocator)' is set to 'Disabled.
- Ensure 'Remote Registry (RemoteRegistry)' is set to 'Disabled.
- Ensure 'Routing and Remote Access (RemoteAccess)' is set to 'Disabled.
- Ensure 'Simple TCP/IP Services (simptcp)' is set to Disabled' or 'Not Installed.
- Ensure 'SNMP Service (SNMP)' is set to 'Disabled' or 'Not Installed.
- Ensure 'Special Administration Console Helper (sacsvr)'is set to 'Disabled' or 'Not Installed.
- Ensure 'SSDP Discovery (SSDPSRV)' is set to Disabled.
- Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled.
- Ensure 'Web Management Service (WMSvc)' is set to 'Disabled' or 'Not Installed.
- Ensure 'Windows Error Reporting Service (WerSvc)' is set to 'Disabled.
- Ensure 'Windows Event Collector (Wecsvc)' is set to 'Disabled.
- Ensure 'Windows Media Player Network SharingService (WMPNetworkSvc)' is set to 'Disabled' or 'Not Installed.
- Ensure 'Windows Mobile Hotspot Service (icssvc)' is set to 'Disabled.
- Ensure 'Windows Push Notifications System Service (WpnService)' is set to 'Disabled.
- Ensure 'Windows PushToInstall Service (PushToInstall)' is set to 'Disabled.
- Ensure 'Windows Remote Management (WS-Management) (WinRM)' is set to 'Disabled.
- Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled.

12- Windows Defender Firewall with Advanced Security.

- Private Settings.
- Ensure 'Windows Firewall: Private: Firewall state,' is set to 'On.
- Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block.
- Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow.
- Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log.
- Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater.
- Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes.

- Public Settings.
- Ensure 'Windows Firewall: Public: Firewall state,' is set to 'On.
- Ensure 'Windows Firewall: Public: Inbound connections’ is set to 'Block.
- Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow.
- Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No.
- nsure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No.
- Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log.
- Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater.
- Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes.

13- Bit Locker Drive Encryptions.

- Ensure 'Allow access to BitLocker-protected fixed data drives from earlier versions of Windows' is set to 'Disabled.
- Ensure 'Choose how BitLocker-protected fixed drives can be recovered' is set 'Enabled'.
- Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Allow data recovery agent' is set to'Enabled: True'.
- Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Recovery Password' is set to 'Enabled: Allow 48-digit recovery password.
- Operating System Drives.
- Ensure 'Allow enhanced PINs for startup' is set to 'Enabled.
- Ensure 'Allow Secure Boot for integrity validation' is set to 'Enabled.
- Ensure 'Choose how BitLocker-protected operating system drives can be recovered' is set to 'Enabled.
- Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Allow data recover agent' is set to 'Enabled: False.
- Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Recovery Password' is set to 'Enabled: Require 48-digit recovery password.

14- Windows Update.

- Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled.
- Ensure 'Configure Automatic Updates' is set to 'Enabled.
- Ensure 'Configure Automatic Updates' is set to 'Enabled.
- Ensure 'Remove access to “Pause updates” feature' is set to 'Enabled.
- Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days.

15- Camera

- Ensure 'Allow Use of Camera' is set to 'Disabled.

16- Event Log Service.

- Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'.
- Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater.
- Security.
- Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled.
- Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater.
- Setup.
- Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled.

- Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater.
- System.
- Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled.
- Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater.

17- Microsoft Defender Antivirus.

- Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'.
- Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured.
- Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block.
- Ensure 'Enable file hash computation feature' is set to 'Enabled.
- Ensure 'Scan all downloaded files and attachments' is set to 'Enabled.
- Ensure 'Turn off real-time protection' is set to 'Disabled.
- Ensure 'Turn on behavior monitoring' is set to 'Enabled.
- Ensure 'Turn on script scanning' is set to 'Enabled'.
- Ensure 'Scan removable drives' is set to 'Enabled'.
- Ensure 'Turn on e-mail scanning' is set to 'Enabled'.
- Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block.
- Ensure 'Turn off Microsoft Defender Antivirus' is set to 'Disabled.

18- Microsoft Defender Application Guard.

- Ensure 'Allow auditing events in Microsoft Defender Application Guard' is set to 'Enabled.
- Ensure 'Allow auditing events in Microsoft Defender Application Guard' is set to 'Enabled.
- Ensure 'Allow auditing events in Microsoft Defender Application Guard' is set to 'Enabled.
- Ensure 'Allow files to download and save to the host operating system from Microsoft Defender Application Guard' is set to 'Disabled'.
- Ensure 'Enable news and interests on the taskbar' is set to 'Disabled.
- Ensure 'Turn off Push to Install service' is set to Enabled.

3.4 Windows Server

Windows Server must adhere to the following configuration standards.

1- Password Policy Configurations.

- Ensure Enforce password history is to 24 or more passwords.
- Ensure Maximum password age is to 90 or fewer days but not 0.
- Ensure Minimum password age is to 1 or more days.
- 'Minimum password length' is set to '14 or more character.
- Ensure Password must meet the complexity requirements is set to enabled.
- Ensure Relax minimum password length limits is set to Enabled.
- Ensure Store password using reversible encryption is set to Disabled.

2- Account Lockout Policy.

- Ensure Account lockout duration is set to 15 minutes or more.
- Ensure Account lockout threshold is set to 5 or fewer invalid logon attempts.
- Ensure Allow Administrator account lockout is set to Enabled.
- Ensure Reset account lockout counter after is set to 14 or more minutes.

3- Local Policies.

- Ensure 'Access Credential Manager as a trusted caller' is set to 'No One.

- Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users.
- Ensure 'Act as part of the operating system' is set to 'No One'.
- Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVIC .
- Ensure 'Allow log on locally' is set to 'Administrators.
- Ensure 'Allow log on locally' is set to 'Administrators.
- Ensure 'Back up files and directories' is set to 'Administrators'.
- Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE.
- Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE.
- Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVIC.
- Ensure 'Create a pagefile' is set to 'Administrators'.
- Ensure 'Create a token object' is set to 'No One.
- Ensure Debug programs is set to Administrator.
- Ensure Force Shutdown from a remote is set to Administrators.
- Ensure Generate security audits is set to LOCAL SERVICE NETWORK SERVICE.
- Ensure Load and unload device drivers is set to administrators.
- Ensure Manage auditing and security log is set Administrators.
- Ensure Modify in Object label is set to No One.
- Ensure Modify firmware environment values is set to Administrators.
- Ensure perform volume task is set to Administrator.
- Ensure Restore files and directories are set to administrator.
- Ensure Shutdown the system is set to Administrator.

4- Security Options of Account.
- Ensure Account: Block Microsoft account is set Users can not add or log on Microsoft account.
- Ensure Account: Guest Account status is set to Disabled.
- Configure Account: Rename Administrator account.
- Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled.

5- Audit.
- Ensure Audit: Force audit policy subcategory setting (windows vista or later to override audit policy settings is set to Enabled.
- Ensure Audit: Shutdown system immediately if unable to log security audits is set to Disabled.

6- Interactive logon
- Ensure interactive logon: Do not require CTRL+ALT+DEL is set to Disabled.
- Ensure interactive logon: Don not display last signed-in is set to Enabled.
- Ensure interactive logon: Machine account lockout threshold is set to 5 or fewer invalid logon attempts but not 0.
- Configure interactive logon: Message text for users attempting to log on.
- Ensure interactive logon: prompt user to change password before expiration is set between t5 and 14 days.

7- Network Access.
- Allow anonymous SID/Name translation is set to Disabled.
- Do not allow anonymous enumeration of SAM accounts and shares is set to Enabled.
- Do not allow anonymous enumeration of SAM accounts is set to Enabled.
- Do not allow storage of passwords and credentials for network authentication is set to Enabled.
- Let Everyone permission apply to anonymous users is set to Disabled.
- Restricting anonymous access to Named pipes and shares is set to Enabled.
- Share that can be accessed anonymously is set to None.

8- Devices.
- Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators.

- Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled.

9- Microsoft network server.
- 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute.
- Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher.

10- Shutdown.
- Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled.

11- System Services.
- Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Not Installed.
- Peer Name Resolution Protocol (PNRPsvc)' is set to 'Not Installed.
- Ensure 'Print Spooler (Spooler)' is set to 'Disabled'.
- Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Not Installed.

12- Bit Locker Drive Encryptions.
- Ensure 'Allow access to BitLocker-protected fixed data drives from earlier versions of Windows' is set to 'Disabled.
- Ensure 'Choose how BitLocker-protected fixed drives can be recovered' is set 'Enabled'.
- Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Allow data recovery agent' is set to ‘Enabled: True'.
- Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Recovery Password' is set to 'Enabled: Allow 48-digit recovery password.

13- Microsoft Defender Antivirus.
- Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'.
- Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured.
- Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block.
- Ensure 'Enable file hash computation feature' is set to 'Enabled.
- Ensure 'Scan all downloaded files and attachments' is set to 'Enabled.
- Ensure 'Turn off real-time protection' is set to 'Disabled.
- Ensure 'Turn on behavior monitoring' is set to 'Enabled.
- Ensure 'Turn on script scanning' is set to 'Enabled’.
- Ensure 'Scan removable drives' is set to 'Enabled'.
- Ensure 'Turn on e-mail scanning' is set to 'Enabled'.
- Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block.

3.5 ESXi 7

ESXi 7 must adhere to the following configuration standards.

1- Installation.
- Ensure ESXi is properly patched.
- Ensure the Image Profile VIB acceptance level is configured properly.
- Ensure no unauthorized kernel modules are loaded on the host.

2- Communication.
- Ensure NTP time synchronization is configured properly.
- Ensure the ESXi host is configured to restrict access to services running on the host.
- Ensure Managed Object Browser is disabled.
- Ensure default self-signed certificate for ESXi communication is not used.
- Ensure SNMP is properly configured.
- Ensure dvfilter API is not configured if not used.

- Ensure expired and revoked SSL certificates are removed from ESXi server.
- Ensue VDS health check is disabled.

3- Logging.

- Ensure a centralized location is configured to collect ESXi host core dumps.
- Ensure persistent logging is configured for all ESXi hosts.
- Ensure remote logging is configured for ESXi hosts.

4- Access.

- Ensure a not-root account exists for local admin access.
- Ensure passwords are required to be complex.
- Ensure the maximum failed login attempts is set to 3.
- Ensure account lockout is set to 15 minutes.
- Ensure previous 5 password is prohibited.
- Ensure only authorized users and groups belong to esxAdminsGroup group.
- Ensure the Exception is properly configured.

5- Console.

- Ensure the DCUI timeout is set to 600 seconds or less.
- Ensure the ESXi shell is disabled.
- Ensure Normal Lockdown mode is enabled.
- Ensure idle ESXi shell and SSH sessions time out after 300 seconds or less.
- Ensure the shell services timeout is set 1 hour or less.
- Ensure DCUI has a trusted users list for lockdown mode.
- Ensure contents of exposed configuration files have not been modified.

6- Storage.

- Ensure bidirectional CHAP authentication for iSCSI traffic is enabled.
- Ensure the uniqueness of CHAP authentication secrets for iSCSI traffic.
- Ensure storage area network (SAN) resources are segregated properly.

7- vNetwork.

- Ensure the vSwitch Forged Transmits Policy is set to be rejected.
- Ensure the vSwitch MAC Address Change policy is set to be rejected.
- Ensure the vSwitch Promiscuous Mode policy is set to reject.
- Ensure port groups are not configured to the value of native VLAN.
- Ensure Virtual Distributed Switch NetFlow is sent to an authorized collector.
- Ensure ports-level configuration overrides are disabled.

8- Devices.

- Ensure Unnecessary CD/DVD devise are disconnected.
- Ensure parallel ports are disconnected.
- Ensure unnecessary serial ports are disconnected.
- Ensure unnecessary USB devices are disconnected.
- Ensure unauthorize modifications and disconnection of devices are disconnected.
- Ensure unauthorized connections of devices is disabled.
- Ensure PCI and PCIe devices passthrough is disabled.

9- Guest.

- Ensure use of the VM console is limited.
- Ensure secure protocols are used for virtual serial port access.

10- Monitor.

- Ensure Autologon is disabled.
- Ensure BIOS BBS is disabled.
- Ensure Guest Host Interaction Protocol Handler is set to disabled.
- Ensure Unity Taskbar is disabled.
- Ensure Unity Window Content is disabled.
- Ensure Unity Push Update is disabled.

- Ensure Shell Action is disabled.
- Ensure Request Disk Topology is disabled.
- Ensure Trash Folder State is disabled.
- Ensure Unity is disabled.
- Ensure Unity Interlock is disabled.

11- Resources.

- Ensure VM limits are configured correctly.
- Ensure hardware-based #D Acceleration is disabled.

12- Storage.

- Ensure nonresistant disks are limited.
- Ensure virtual disk shirking is disabled.
- Ensure virtual disk wiping is disabled.

13- Tools.

- Ensure the number of VM log files is configured properly.
- Ensure host information is sent to guests.
- Ensure VM log files size is limited.