Research hardening a FortiGate firewall.

* **Security Password**
  + Change the default admin password before connecting the firewall to any network.
  + Enable password profile to enforce complex passwords.  Change passwords on a regular scheduled basis.
  + Enable admin profiles and groups to limit access to other administrators.

* **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 FortiGates to restore the system from a configuration file. In an HA cluster, the same key should be used on all units.
  + To enhance password security, specify a custom private key for the encryption process. This ensures that you only know the key.
  + 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. For more information, see [Trusted platform module support](https://docs.fortinet.com/document/fortigate/7.2.66/administration-guide/893277/trusted-platform-module-support).
  + **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.

* **Physical Security**
  + If the FortiGate cannot be physically secured:
    - Disable USB firmware and configuration installation:  
      config system auto-install
    - set auto-install-config disable
    - set auto-install-image disable
* Enable port security (802.1x) to prevent unauthorized devices from forwarding traffic.
* Optionally, disable the maintainer account. Note that doing this will make you unable to recover administrator access using a console connection if all of the administrator credentials are lost.
* **Interface Management Profiles**
  + Do not enable ping, ssh, http/s, etc on firewall interfaces that don't require this service. Also note that the "response pages" may not be necessary on certain interfaces. These are the pages the firewall uses for URL filtering notification, virus block messages, SSL VPN and captive portal.
  + Set up IP based access control on all interfaces that have management profiles. Obviously, this includes the management interface, but also includes any other interfaces that have interface management profiles.
  + Place the management interface into a management VLAN that limits access to authorized personnel. Do not turn on management profiles on interfaces that are accessed by non-authorized personnel.
* **Vulnerability -Monitoring PSIRT**
  + Monitor system and configuration logs on a regular basis to monitor for unauthorized login attempts or changes to configuration settings.
  + Product Security Incident Response Team (PSIRT) continually tests and gathers information about Fortinet hardware and software products.
  + The findings are sent to the Fortinet development teams, and serious issues are described, along with protective solutions, in advisories listed at <https://www.fortiguard.com/psirt>.
  + Set up notifications for system and configuration log messages that indicate modifications of the firewall's operational parameters (these notifications can be sent via email, syslog and/or snmp traps)
  + Set an SNMP community string that is not easy to guess and is preferably not shared by other network equipment.
  + Only enable SNMP on internal interfaces that you need them on.

* **Firmware**
  + Keep the FortiOS firmware up to date. The latest patch release has the most fixed bugs and vulnerabilities and should be the most stable. Firmware is periodically updated to add new features and resolve important issues.
  + Read the release notes. The known issues may include issues that affect your business.
  + Do not use out-of-support firmware. Review the product life cycle and plan to upgrade before the firmware expires.
  + Optionally, subscribe to the Fortinet firmware RSS feed: <https://pub.kb.fortinet.com/rss/firmware.xml>.

* **Encrypted Protocols**
  + Use encrypted protocols whenever possible,
* SNMPv3 instead of SNMP,
* SSH instead of telnet,
* OSPF MD5 authentication,
* SCP instead of FTP or TFTP,
* NTP authentication, and encrypted logging instead of TCP.

.·

* **Strong Ciphers**
  + Force higher levels of encryption and strong ciphers:
    - config system global
    - set strong-crypto enable
    - set ssl-static-key-ciphers disable
    - set dh-params 8192
* **FortiGuard Databases**
  + Ensure that FortiGuard databases, such as AS, IPS, and AV, are updated punctually.
  + Send an alert if they are out of date.
* **Penetration Testing**
  + Test your FortiGate to try to gain unauthorized access, or hire a penetration testing company to verify your work.
* **Denial of Service**
  + DoS policies, which look for anomalous traffic patterns, are checked before the more resource-intensive security policies to help prevent this.
  + These policies can be applied to incoming traffic from your local network or the internet, depending on your particular network. The following guidelines to start with DoS policies:
    - Ensure the FortiGate is receiving regular IPS signature updates from the FortiGuard network through a valid subscription.
    - Enable anomaly logging and keep the action as monitor for some time. This is to observe and understand what expected traffic looks like so that you may tune thresholds to have small margins, and therefore more protection. Keep note of false alarms. If they are too frequent, you should adjust your policy accordingly.
    - Enable the following DoS policy anomalies to help prevent targeted attacks:
* tcp\_syn\_flood
* tcp\_port\_scan
* tcp\_src\_session
* tcp\_dst\_session
* ip\_src\_session
* Ip\_dst\_session
* If you have an idea of your traffic rates for the preceding traffic patterns, you may adjust the threshold. Otherwise, begin with the default and adjust after a period of observing normal traffic. For more information, see [DoS protection](https://docs.fortinet.com/document/fortigate/7.2.99/administration-guide/771644/dos-protection) in the FortiOS Administration Guide.
* Where possible, enable ASIC DoS for offloading using network processor ASICs. The FortiOS Hardware Acceleration Guide contains more information about DoS-related NP6 ASIC features, such as configuring [NP6 anomaly protection](https://docs.fortinet.com/document/fortigate/7.2.99/hardware-acceleration/107867/configuring-individual-np6-processors) and using the [host protection engine (HPE)](https://docs.fortinet.com/document/fortigate/7.2.99/hardware-acceleration/622032/np6-hpe-host-protection-engine) to protect the FortiGate from DoS attacks.

**Research hardening Windows 10.**

Using built in features

* Windows defender
* Microsoft smartscreen
* Windows sandbox

Windows defender is a built in antivirus that requires no manual configuration

|  |  |
| --- | --- |
| Includes - | exploit guard (anti-malware) |
|  | Device guard (cod integrity) |
|  | Application Guard (built into microsoft edge to protect from malicious activity) |
|  | Credential guard (isolates login info from the overall operating system) |

Microsoft Smart screen

* provides anti-phishing and anti-malware support, reputation-based URL and app protection, operating system integration.

Windows Sandbox

* operates like a VM for install of new applications to ensure no back-end issues.

Windows Secure boot

* Safeguards users BIOS and protects against ransomware.

Windows BitLocker encryption

* Allows you to encrypt data or even entire drives so they can’t be accessed unless individual has appropriate key

Best Practices

* Application management
* Application control
* Disabling remote access
* Enable auto-updates for OS
* Enable file backups
* Host based Intrusion prevention system

**Research hardening Windows Server 2012r2.**

* The operating system should be protected from hostile network traffic until such time the system is installed and hardened.
* Harden the server- The operating system should be hardened at the earliest prior connecting it to the corporate network.
* After completing the security hardening, the server can be connected to the internet in order to get the latest service packs and hotfixes from the Microsoft Update servers.
* Configure Automatic Updates from the Automatic Updates control panel.
* The server should be properly placed within the corporate network according to the service requirements.
* Set proper file system permissions- File systems permissions should be reviewed and enabled on a required basis. Each data folder should only be allowed to personnel who have required clearance levels to access that information.
* Setting network time protocol to a single time and date source is extremely important to co-relate events and Maintenance of proper malware protection is of utmost importance for a secure windows environment.
* The integrity of critical operating system files and application configuration files should be monitored and verified against the change management requests of the organization.
* Set Minimum password length, deploy a proper account lockout policy, Disable or delete unused users.
* Ensure that access to any network setting by anonymous users is disabled.
* Enable the windows firewall or any relevant firewall to all the profiles of the server (Domain, Private , Public ).
* Configure Event Log retention size- The maximum log file size can be configured between 1 mb and 2 tb.\
* Set a BIOS/Firmware password to prevent alterations in system startup settings, disable automatic administrative login to recovery console, Do not allow the system to be shut down without having to log on, Configure the device boot order to prevent unauthorized booting from alternate media, Configure a screen-saver to lock the console's screen automatically if the host is left unattended.

**Research hardening Ubuntu server 18.04.**

* Make sure to regularly update server:
  + sudo apt update && sudo apt dist-upgrade && sudo apt autoremove
* Setup/Require an Authentication Key Pair for SSH login
* Install Fail2Ban to reduce the rate of incorrect authentications attempts.
  + sudo apt-get install fail2ban
  + sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
  + sudo nano /etc/fail2ban/jail.local
* Change sshd\_config file in order to:
  + Turn off SSH Password Authentication
  + Turn off SSH Root Login
  + Implement Idle Session Timer (100 second interval, 4 checks)
  + "Password Authentication" = no
  + "PermitRootLogin" = no
  + "ClientAliveInterval" = 100
  + "ClientAliveCountMax" = 4
* Whitelist allowed SSH users
  + AllowUsers <usernames>
* Change the default SSH port
* Utilize the UFW firewall
  + sudo ufw allow ssh
  + sudo ufw enable

*Also use these to allow http/https traffic:*

* sudo ufw allow http
* sudo ufw allow https

*Check status*

* sudo ufw status verbose
* Setup regular server backups as a Disaster Recovery Solution (Mondo Rescue or Déjà Dup)

Sources

Fortigate:

<https://docs.fortinet.com/document/fortigate/6.4.0/hardening-your-fortigate/612504/hardening-your-fortigate>

Windows 10 Hardening:

<https://perception-point.io/guides/os-isolation/windows-10-hardening-19-ways-to-secure-your-workstations>

Windows Server 2012:

<https://www.fincsirt.lk/pdf/FINCSIRT_Windows_2012_R2_Hardening_V1_0.pdf>

Ubuntu Server 18.04:

<https://help.ubuntu.com/community/BackupYourSystem>

<https://medium.com/@BaneBiddix/how-to-harden-your-ubuntu-18-04-server-ffc4b6658fe7>

<https://www.civo.com/learn/harden-your-virtual-private-server-against-attackers>