



# FortiGate Hardening and Best Practices

Josh Noble  
Network Engineer – LAN Services  
MOREnet  
josh@more.net



# About Me

- Working with Fortinet gear for 7 years.
- IT Professional for 26 years.
- 9 years at MOREnet.
- Proud dad.
- Not a robot.
- Loves Pinball!

# What Are We Doing in Here Today?

- We are going over things that you can do on your FortiGate that don't involve extra products or costs!
- This will be mostly security-focused.
- This will be a live demo, things might break or not go as planned!
- Each section will end with Q and A.

# The Basics – Firmware Versions and Upgrades

- What version of FortiOS are you running?
- Staying up to date with vulnerabilities and patches. <https://www.fortiguard.com/psirt>
- Steps to take prior to upgrading. Read those release notes!
- Fortinet Upgrade Path Tool. Use this! <https://docs.fortinet.com/upgrade-tool>
- Do you have other Fortinet products? This matters, we need to make sure their firmware is compatible. More on that later.
- Fortinet Firmware RSS Feed. <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Subscribe-to-RSS-feeds-for-alerts-on-new-Fortinet/ta-p/248571>

# Firmware Version

- You can find what version you are running in your FortiGate's status dashboard.

The screenshot displays the FortiGate status dashboard. On the left, the 'System Information' section lists various system details. The 'Firmware' entry is highlighted with a red box, showing 'v7.2.6 build1575 (Feature)'. On the right, the 'Licenses' section shows a list of active licenses: FortiCare Support, Firmware & General Updates, IPS, AntiVirus, and Web Filtering. Below the licenses, the 'FortiToken' is shown at 50% usage.

System Information	
Hostname	Noble-FG100E
Serial Number	FG100ETK18031211
Firmware	v7.2.6 build1575 (Feature)
Mode	NAT
System Time	2024/01/17 13:46:48
Uptime	01:05:50:12
WAN IP	[Redacted]

Licenses (173.243.141.6)	
FortiCare Support	✓
Firmware & General Updates	✓
IPS	✓
AntiVirus	✓
Web Filtering	✓

FortiToken 1 / 2  
50%

# Feature vs Mature Firmware

- Most production networks stick to using “Mature” firmware.
- Login to your Fortinet support portal. Go to Support and Firmware Downloads to browse firmware versions.
- Under Release Type, you will see Mature or Feature.
- Your FortiGate will now prompt you that you are going from a mature release to a feature release when upgrading.
- Fortinet’s recommended release for each model of firewall.  
<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Recommended-Release-for-FortiOS/ta-p/227178>

# Firmware Compatibility

- If you do have other Fortinet products, you need to check on FortiOS compatibility.
- FortiAnalyzer always gets upgraded first!
- Check order of other Fortinet devices here:  
<https://docs.fortinet.com/document/fortigate/7.2.6/fortios-release-notes/936594>
- FortiLink Compatibility Matrix (Switches)  
<https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/d756e8a9-6d2d-11e9-81a4-00505692583a/FortiLinkCompatibility.pdf>
- FortiAP Matrix  
<https://docs.fortinet.com/document/fortiap/7.4.0/fortiap-and-fortios-compatibility-matrix/261175/fortiap>
- From your Gate, go to System>Fabric Management for easy firmware upgrades to all Fortinet devices.

Questions about firmware or the  
upgrade process?



# Hardening Basics – Where to Start?

- Let's start with administrative access!
- Who can login to your firewall?
- What do they have access to?
- Where are they logging in from?
- How challenging is it to login?

# Who Can Login to the FortiGate? What Do They Have Access To?

- Go to **System>Administrators** to check on **who** has admin accounts.
- Admin Profiles help us control **what** admins that access to and are very customizable.
- Admin profiles can be set to read-only.
- Changing the admin account that you use to something other than the default “admin” is best practice.
- Check if your admins have logged in recently and remove them if they are unknown or no longer needed.

# Bonus Slide! Extending the Maximum Log Age.

- If your FortiGate has an internal SSD, you can expand the maximum log age.
- If your Gate model ends in "1" you have internal storage.
- Default is 7 days.
- We will change to 180 days.
- If the disk fills, it will purge old logs automatically.
- CLI is the following:

```
config log disk setting  
set maximum-log-age 180  
end
```

# Setup a Login Disclaimer

- CLI for this:






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

- Edit this text here  
System>Replacement Messages
- Click on Extended View in the top right and under Admin choose Post-login Disclaimer Message.

# Where Are Your Admins Logging in From?


- Trusted Hosts, Trusted Hosts Trusted Hosts, please use this!!!
- Restrict access to your management LAN or specific workstation IP addresses or ranges if possible.
- Make sure every admin account has trusted hosts enabled.

# WAN Admin Access

Name	 wan1
Alias	<input type="text"/>
Type	 Physical Interface
Role 	WAN 
Estimated bandwidth 	<input type="text" value="0"/> kbps Upstream
	<input type="text" value="0"/> kbps Downstream



---

### Address

Addressing mode	<input type="button" value="Manual"/> <input checked="" type="button" value="DHCP"/> <input type="button" value="PPPoE"/>
Status	 Connected
Obtained IP/Netmask	10.10.11.101/255.255.255.0 <input type="button" value="Renew"/>
Expiry Date	2024/01/25 07:59:39
Acquired DNS	8.8.8.8
Default gateway	10.10.11.1
Retrieve default gateway from server	<input type="checkbox"/>
Distance	<input type="text" value="5"/>
Override internal DNS	<input type="checkbox"/>

---

### Administrative Access

IPv4	<input checked="" type="checkbox"/> HTTPS	<input type="checkbox"/> HTTP 	<input checked="" type="checkbox"/> PING
	<input checked="" type="checkbox"/> FMG-Access	<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP
	<input type="checkbox"/> FTM	<input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> Security Fabric Connection 
	<input type="checkbox"/> Speed Test		

## WAN Admin Access cont.

- If you or another admin needs admin access from outside of your LAN, use a VPN or another secure remote desktop application.
- Your FortiGate has VPN built in at no extra charge.
- We will talk about a little about SSL-VPN access later.

# How Challenging is it to Login?

- If we go to **System>Settings** we can check HTTPS port (change this and document).
- We can also set a password policy here (Good idea!)
- SSH Port can be changed.
- Don't use telnet please!
- Idle Timeout is how long your FortiGate will stay logged in without activity. Default is 5 minutes.
- Yay, you can change your theme in here too!



# How Challenging is it to Login cont.

- Change the admin timeout from 30 seconds to 300 seconds (5 minutes)

- This is done in CLI:

```
config system global  
set admin-lockout-duration 300  
end
```

# 2FA With FortiToken

- You get two FortiTokens for free.
- You might as well use them!
- If you need more, you can purchase them in packs of 5, 10, 25, 50, 100, 200 etc.
- Licenses are perpetual, so if someone doesn't need one anymore, you get that one back to use elsewhere.
- To access your tokens: **User & Authentication > FortiTokens**
- You will need FortiToken Mobile application for your phone. It is a free app.
- Add your tokens to your admins under **System > Administrators**



Welcome to FortiToken Mobile

Scan or enter the key to add token

SCAN BARCODE

ENTER MANUALLY



# Questions About Admin Access?

# Firewall Policy Fun!

- Let's discuss some policy best practices and tips in this section.
- You can check how many policies your firewall can support on its specific product data sheet or the Fortinet Product Matrix.

[https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet\\_Product\\_Matrix.pdf](https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf)

# Flow-Based vs Proxy-Based

- Flow-based will not be buffered by the FortiGate
- Flow-based inspection takes a snapshot of content packets and uses pattern matching to identify security threats in the content.
- Use flow-based policies for things like streaming, VOIP, etc.
- Best performance.
- Fast Pass

# Flow-Based vs Proxy-Based

- Proxy-based inspection reconstructs content that passes through the FortiGate and inspects the content for security threats.
- Packets held by the FortiGate until the entire payload is inspected for violations such as virus, spam, or malicious web links.
- Uses more of the FortiGate's resources.
- Full blown border patrol car search.

# Links for More Info on Inspection Types

- <https://docs.fortinet.com/document/fortigate/6.4.0/parallel-path-processing-life-of-a-packet/993346/comparison-of-inspection-types>
- <https://docs.fortinet.com/document/fortigate/7.2.6/administration-guide/721410>



# Policies and What to Allow

- So, you want to limit outbound traffic?
- Where do we start?
- Let's create a web access policy for HTTP and HTTPS
- Do you just want your local clients to use your internal DNS?
- We would need to create a policy for your local DNS servers to get access to their DNS forwarders
- Let's create a policy for DNS service.

# Determining What Else to Allow

- This process takes time and log monitoring.
- Start with what you know is needed and create policies.
- Think about NTP, SMTP, Azure etc.
- Once you remove your blanket policy, turn logging on for the implicit deny policy to see if anything was missed.
- Create service groups for similar services such as LDAP, VOIP

# Policies with Internet Service Database (ISDB)

- ISDB is a living database for many common services.
- Combines IP addresses, service ports, etc.
- Fortinet updates this for us.
- To check the last time the ISDB was updated, go to **System>FortiGuard>Firmware and General Updates** or the command below:

```
diag autoupdate versions | grep  
'Internet-service' -A6
```

# ISDB Resource Usage

- If your FortiGate has under 2GB of system memory, ISDB can affect performance or trigger conserve mode
- Command to see system memory and how much memory is free:

*diagnose hardware sysinfo memory*

- You can setup the system to auto update to at a specific time that is outside of school hours with this command:

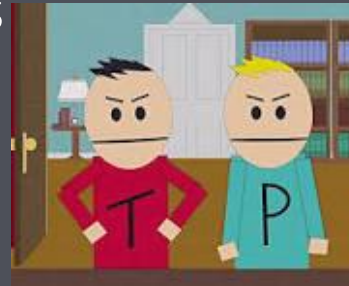
*config system autoupdate schedule  
set status enable  
set frequency daily  
set time 01:00*

More info and options here:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Low-end-FortiGate-models-with-RAM-2GB-entering/ta-p/295489>

# Geo-Blocking

- Fortinet has an IP Geography database that contain IPs and their geographic location.
- Do you want to block certain countries altogether?
- First, we need to create address objects for the countries.
- Then we will create an address group for the objects.
- When troubleshooting issues, remember that you set this up.
- If you have any VIPs, you may to need create a rule with source "Blocked Countries" to the destination of each of your VIPs
- We're going to pick on Canada



# Geo-Blocking Extras

- Find out what country an IP is registered:

```
diagnose geoip geoip-query <public ip>
```

- Fortinet article on setting Geo-blocking:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-block-by-country-or-geolocation/tap/196741>

# Security Profiles

- Come with your FortiGuard subscription.
- Compare Bundles here:
- <https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/fortigate-security-bundles#:~:text=The%20Enterprise%20Protection%20bundle%20builds,surface%20assessment%20and%20monitoring%20service>

# Application Control

- Uses application sensors or signatures to detect application traffic even if the traffic uses non-standard ports or protocols.
- Signatures are automatically updated through FortiGuard.
- If an application was written to tunnel through port 443 (https,) app control can determine that this is non-standard https traffic and block/monitor.
- Runs at layer 7 of the OSI model.
- Works best with DPI but mostly for Cloud-based applications.



# Questions About Policies?

# Automation Stitches

- Triggers can be setup to notify you for certain firewall events
- Any event can be triggered to send a notification or action.
- By default, this uses a Fortinet SMTP server, and it doesn't always work...
- Useful ones are firewall reboot, license expiry, conserve mode
- Let's setup a Teams notification!
- Teams Setup Link  
<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/72623/microsoft-teams-notification-action>

# Local-in Policies with Automation Stitches

- These are to the Gate, not through the Gate.
- Similar to administrative access that we discussed earlier.
- Need to be enabled in Feature Visibility **System>Feature Visibility>Local-in Policies**
- Can be applied to any interface, so WAN-side or LAN-side.
- CLI is where we configure these.
- Let's setup a stitch that will block disabled admin login attempts both externally and internally!

# Automation Stitch – Block Disabled Admin

- Create new address group – “Admin Failed Login”
- Create Trigger for Event Logs pertaining to Admin login disabled
- Add Action – CLI Script
- Create stitch with our trigger and action
- Create local-in policy with our admin address group
- <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Block-FortiGate-Administrator-Login-with-an/ta-p/291355#:~:text=an%20automation%20stitch.-,In%20the%20GUI%3A,Select%20OK%20-%3E%20Select%20Apply>

# NO NETWORK FOR YOU!

- Now that we have prevented this user from having the ability get a login prompt, let's cut them off!
- Create a regular IPv4 policy with the source of our Admin\_Login\_Failed address group.
- Destination can be any interface or multiple interfaces.
- DENY ALL!
- If this is an internal user, we can look up their MAC address in device inventory as well and block that.

# Audience Participation

- What are some items that you currently use automation stitches for?
- What are some things that you can envision being helpful?

# SSL-VPN Best Practices for Remote Users

- To prevent brute force attacks we can limit login attempts and configure the block duration

```
config vpn ssl settings
```

```
set login-attempt-limit 3
```

```
set login-block-time 300
```

This gives us 3 attempts, after 3 attempts you must wait 5 minutes before trying again.

# SSL-VPN Best Practices for Remote Users, cont.

- Let's change the Listen on Port from 443 to 14443
- Document this change, it will be needed by your end users that connect to VPN.

The screenshot displays the 'SSL-VPN Settings' configuration page. On the left, a navigation menu includes 'VPN', 'Overlay Controller VPN', 'IPsec Tunnels', 'IPsec Wizard', 'IPsec Tunnel Template', 'SSL-VPN Portals', 'SSL-VPN Settings' (highlighted with a star), and 'SSL-VPN Clients'. The main content area is titled 'Connection Settings' and features a toggle for 'Enable SSL-VPN' which is turned on. Below this, the 'Listen on Interface(s)' field contains 'wan1'. The 'Listen on Port' field is set to '14443'. A blue information box at the bottom right states: 'Web mode access will be listening at <https://10.10.11.101:14443>'.



# SSL-VPN Questions to Ask

- Who needs access to VPN?
- What do they need access to?
- Where can they access it from?
- When do they need access?
- How long do they need access?

# Who Needs Access to VPN?

- If it is internal staff, you can authenticate through RADIUS, local user (created on firewall,) LDAP, etc.
- You can do 2FA with FortiToken or other 2FA products

# What Will They Need Access to Over the VPN?

- Certain PC?
- Camera System?
- File Server?
- Certain VLAN?
- HVAC?
- Limit their access to only what they need. Be as specific as possible.

# Where Are They Accessing From?

- At the very least, create a Geo-address for the USA and restrict to that.
- Ideally, we can set a static IP in here for other businesses that need access.

# SSL-VPN Questions?

# More Ways to Harden

- Disable SSHv1

```
config system global  
set admin-ssh-v1 disable
```

- Disable Telnet

```
Config system global  
Set admin-telnet disable
```

## Use Certificates Signed by a Trusted CA

- Fortinet recommends using the built-in self signed certs for initial installation and testing only.
- To see the local certs installed on your Gate, you must turn the feature on first. **System>Feature Visibility** and tick Certificates. There are lots of other features in here that are turned off.
- Purchase and import a signed SSL cert:  
<https://docs.fortinet.com/document/fortigate/7.2.6/administration-guide/825073>
- Certificates are needed to do deep packet inspection!

# Quick Look at SSL Profiles

- This is where the deep packet inspection fun begins
- **Security Profiles > SSL/SSH Inspection**
- Note that you can exclude certain web categories like Finance and Banking, Health and Wellness, etc.
- Required for DLP (Data Leak Prevention)



# Physical Security

- This one always seems obvious, but make sure your firewall is in a locked room with restricted access.
- Someone could unplug your Gate, hook a console cable to it, and interrupt the boot process.
- Disable physical interfaces that aren't in use.

Questions or Anything That You  
Have Found That You Want to  
Share?

# Useful Links

- <https://www.fortiguard.com/psirt>
- <https://docs.fortinet.com/document/fortigate/7.4.0/best-practices/555436/hardening>
- <https://training.fortinet.com/>
- <https://docs.fortinet.com/upgrade-tool>
- <https://docs.fortinet.com/>
- <https://www.more.net/solutions/network-solutions/lan-services/>



Thank You for Attending Tech Summit 2024. See you at the MOREnet Conference down in Branson in October!



(800) 509-6673  
www.more.net

