

AI-03155 pfSense Deployment

Owner	Ⓒ Rigel Arcayan
Tags	Project
Created time	@November 11, 2025 11:24 AM

I have a pfsense installed as a hyper-vm on my laptop Dell latitude e4310 with a wifi and lan connection. Help me configure the pfsense so that it can connect to my lte hotspot and then the lan provide an internet connection to the 8 port Poe switch

Got it! You want to use your Dell Latitude E4310's Wi-Fi (connected to an LTE hotspot) as the internet source for a **pfSense VM** in Hyper-V, then have pfSense share that internet over **LAN** to an 8-port PoE switch. Let's break this down carefully.

Direct Answer: Setup Overview

1. **Wi-Fi (Hotspot) → pfSense WAN**
2. **pfSense LAN → Laptop NIC → PoE Switch → Devices**

Key Steps

1. Hyper-V Network Setup

- **Create two virtual switches in Hyper-V:**
 1. **WAN Switch (External)**
 - Binds to **your laptop Wi-Fi adapter**.
 - This lets the pfSense VM access the LTE hotspot.
 2. **LAN Switch (Internal)**
 - Internal only (connects VM to host and LAN NIC).
 - This will forward traffic from pfSense to your LAN adapter.

- Assign in pfSense VM:
 - **WAN** → connected to the **Wi-Fi virtual switch**.
 - **LAN** → connected to the **LAN virtual switch**.
-

2. pfSense WAN Configuration

- Go to **Interfaces** → **WAN**.
 - Select **DHCP** (since LTE hotspot usually provides dynamic IP).
 - Save and apply.
 - Test **WAN connectivity** by pinging 8.8.8.8 from pfSense Diagnostics → Ping.
-

3. pfSense LAN Configuration

- Go to **Interfaces** → **LAN**.
 - Assign **static IP**, e.g., `192.168.100.1/24`.
 - Enable **DHCP Server** on LAN so connected devices can get IPs automatically.
-

4. Bind LAN to Laptop NIC

- On your host laptop, make sure the LAN adapter is **bridged or assigned** to the Hyper-V Internal switch.

Option 1: Internet via NAT (simpler)

- Leave LAN as internal virtual switch. pfSense handles DHCP/NAT.
- Devices plugged into your PoE switch will get IPs from pfSense.

Option 2: Bridge mode (advanced)

- Less recommended unless you want devices on same subnet as LTE hotspot.
-

5. Physical Setup

1. Laptop NIC → **PoE switch**
2. Devices connect to switch → pfSense assigns IP via DHCP → Internet goes out via WAN (Wi-Fi hotspot).

6. Firewall/NAT Rules

- pfSense should already create default NAT rules for LAN → WAN.
 - Test by connecting a laptop or device to the PoE switch.
 - If no internet, check pfSense **System Logs → Firewall → NAT**.
-

7. Optional Tweaks

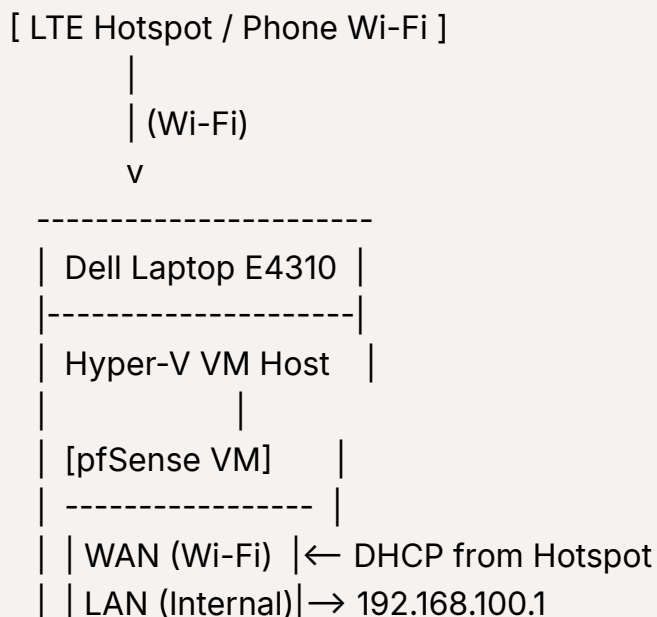
- Enable **DNS Resolver** in pfSense to provide DNS to clients.
 - Consider **traffic shaping** if LTE has limited bandwidth.
 - Save pfSense config and snapshot VM in Hyper-V for quick recovery.
-

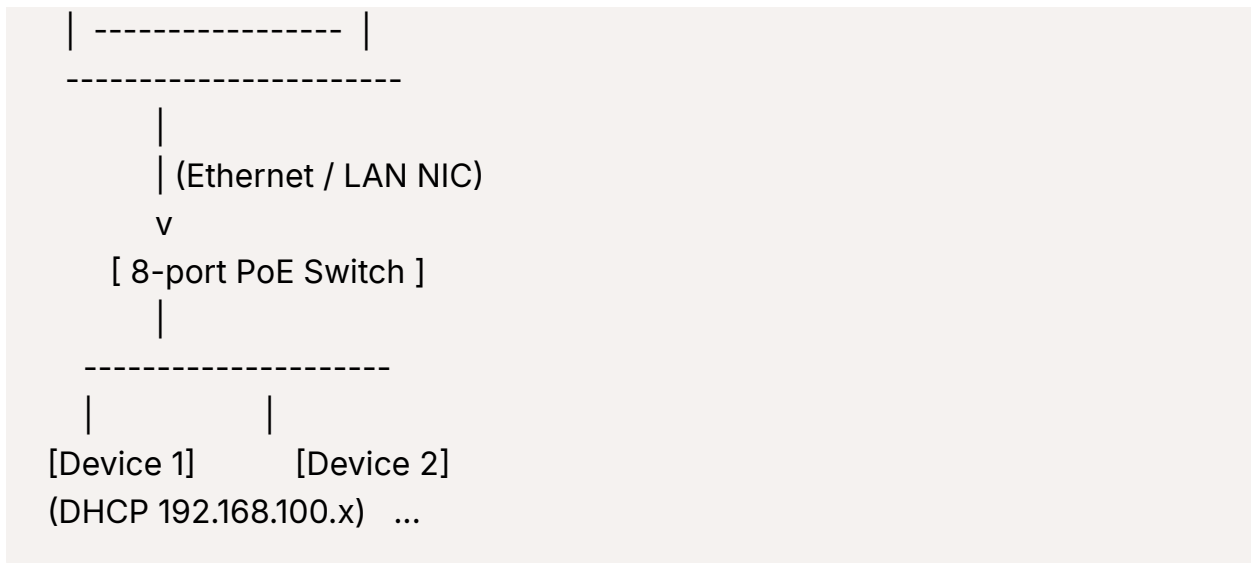
✓ With this, your LTE hotspot provides internet to pfSense, and pfSense shares it through LAN to the PoE switch. All devices connected to the switch will get internet and be on the `192.168.100.x` subnet (or whatever you choose).

If you want, I can draw a **diagram showing the laptop, Hyper-V, pfSense, and PoE switch connection**—it makes this much easier to visualize.

Do you want me to do that?

Perfect! Here's a clear **text-only diagram** of your setup:





Explanation:

1. **WAN (pfSense)** gets internet from your LTE hotspot through the laptop Wi-Fi adapter.
2. **LAN (pfSense)** is on an internal network (`192.168.100.x`) and connects to your laptop LAN NIC.
3. The LAN NIC physically connects to your **PoE switch**.
4. Devices connected to the PoE switch get IPs from pfSense and can access the internet through the WAN.

If you want, I can also provide a **step-by-step Hyper-V virtual switch and pfSense interface config** specifically for your Dell laptop, so you can copy settings exactly. Do you want me to do that next?

Excellent — here’s your **step-by-step guide** for configuring your Dell Latitude E4310 running **Windows Server 2016 + Hyper-V + pfSense VM**, so that:

- ✓ Wi-Fi (connected to LTE hotspot) → pfSense WAN
- ✓ LAN → PoE Switch (via laptop LAN port)

Everything below is **text-based, precise, and safe to execute**.

Step 1: Create the Hyper-V Virtual Switches

1.1 Create WAN Virtual Switch

- Open **Hyper-V Manager** → **Virtual Switch Manager**.
 - Click **New virtual network switch** → **External**.
 - Name it: **WiFi-WAN**.
 - Under *External network*, select your **Wi-Fi adapter** (the one that connects to your LTE hotspot).
 - **Do not check** "Allow management OS to share this adapter."
 - | This ensures pfSense alone uses it, avoiding routing conflicts.
 - Click **Apply** → **OK**.
-

1.2 Create LAN Virtual Switch

- Still in **Virtual Switch Manager**, click **New virtual network switch** → **Internal**.
 - Name it: **LAN-Internal**.
 - Click **Apply** → **OK**.
-



Step 2: Assign Switches to pfSense VM

- Right-click your **pfSense VM** → **Settings** → **Network Adapter**.
- You should see two adapters:
 - **Adapter 1 (WAN)** → connect to **WiFi-WAN**
 - **Adapter 2 (LAN)** → connect to **LAN-Internal**

If pfSense VM currently has only one NIC:

- Click **Add Hardware** → **Network Adapter** → **Add**
 - Assign the new one to **LAN-Internal**
-



Step 3: Configure pfSense Interfaces

1. Start pfSense VM

2. At console, pfSense will detect both NICs, e.g.:

```
em0 - connected to WiFi-WAN
em1 - connected to LAN-Internal
```

3. Assign:

- `em0` → WAN
- `em1` → LAN

Step 4: Configure WAN (Wi-Fi → Hotspot)

Inside pfSense WebGUI (`https://192.168.1.1` by default):

1. Go to **Interfaces** → **WAN**
2. Type: **DHCP** (the LTE hotspot gives IP automatically)
3. Save and apply.

Test WAN:

`Diagnostics` → `Ping` → `Hostname 8.8.8.8`

If successful, pfSense is online through your LTE hotspot.

Step 5: Configure LAN (Internal Network)

1. Go to **Interfaces** → **LAN**
2. Set **Static IP:** `192.168.100.1/24`
3. Enable **DHCP Server**
 - Range: `192.168.100.10 – 192.168.100.200`
 - Save and Apply

Now pfSense can assign IPs to any device connected via your LAN NIC → PoE switch.

Step 6: Bridge Internal LAN to Physical Ethernet

1. In Windows, open **Network Connections** (`ncpa.cpl`).
2. You'll see a new adapter named **vEthernet (LAN-Internal)**.
3. **Bridge** it with your **physical LAN adapter** (the laptop's Ethernet port):
 - Select both → right-click → **Bridge Connections**.
 - Windows creates a "Network Bridge."
 - This allows packets from pfSense LAN to reach the PoE switch.

Step 7: Connect the PoE Switch

Physical cabling:


Dell E4310 LAN port → PoE Switch → Other devices (Home Assistant, second laptop, etc.)

Connected devices will now:

- Get IPs from pfSense (e.g., 192.168.100.x)
- Use pfSense as gateway (192.168.100.1)
- Access the internet through your LTE hotspot (Wi-Fi → WAN)

Step 8: Verify Functionality

From a device on PoE switch:

1. Check IP: should be `192.168.100.x`
2. Gateway: `192.168.100.1`
3. DNS: pfSense IP or 8.8.8.8
4. Try pinging: `ping 8.8.8.8` → should work
5. Try loading a webpage → success = done 

Optional Enhancements

Feature	Where to Configure	Why
DNS Resolver	Services → DNS Resolver	pfSense acts as local DNS
Firewall/NAT	Firewall → NAT → Outbound	Ensure automatic outbound NAT is enabled
Traffic Shaping	Firewall → Traffic Shaper Wizard	Control LTE data usage
Captive Portal	Services → Captive Portal	Optional for guest network isolation

✓ End Result Summary

LTE Hotspot (Wi-Fi)

↓

Laptop Wi-Fi → pfSense WAN

pfSense LAN → Internal vSwitch → Ethernet Bridge → PoE Switch

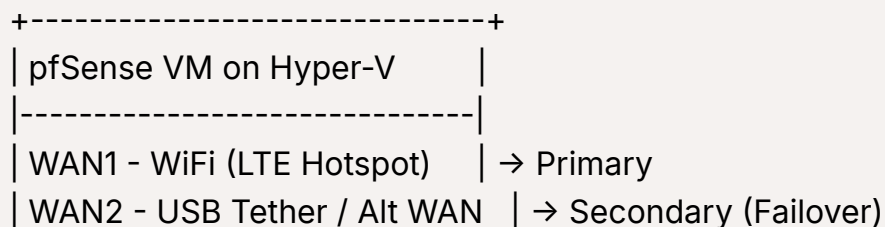
↓

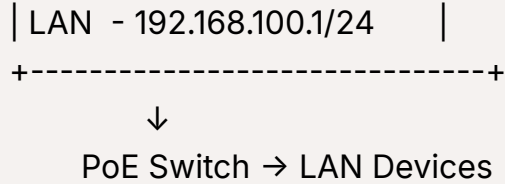
All LAN Devices → pfSense DHCP (192.168.100.x) → Internet

Would you like me to add a **fallback mode** — so when your Wi-Fi hotspot disconnects, pfSense automatically fails over to another connection (e.g., USB tether or local network)?

Excellent — here's how to set up a **simple, reliable failover system** in your current pfSense-on-Hyper-V design, so your network automatically switches from your **Wi-Fi LTE hotspot** (primary) to a **secondary connection** (e.g. USB-tethered phone, Ethernet WAN, or even a secondary Wi-Fi adapter) when the LTE hotspot drops.

⚙️ OVERVIEW — Redundant WAN Setup in pfSense





STEP-BY-STEP CONFIGURATION

Step 1 — Add the Secondary WAN

You'll need a **second network path** (any of these works):

- A USB phone tether (Android or iPhone hotspot via USB)
- A USB-to-Ethernet adapter
- A second Wi-Fi dongle that can connect to another LTE hotspot

Then:

1. Plug in the secondary device.
2. In **Windows** → **Network Connections**, note its adapter name.
3. In **Hyper-V** → **Virtual Switch Manager**, create another **External Switch**:
 - Name it: `WAN2-Failover`
 - Bind it to that second adapter
 - **Do not** check "Allow management OS to share this adapter."
4. In pfSense VM settings:
 - Add another **Network Adapter**
 - Connect it to the new `WAN2-Failover` switch.

Step 2 — Assign WAN2 in pfSense

In pfSense WebGUI:

1. Go to **Interfaces** → **Assignments**
2. Click **Add (+)** to add the new NIC (e.g., `em2`)

3. Assign it as **WAN2**
4. Enable WAN2, set it to **DHCP** (most tether or LTE sources use DHCP)
5. Click **Save → Apply**

✓ Test connectivity:

- Go to **Diagnostics → Ping**
- Select WAN2, ping **8.8.8.8** — should succeed.

Step 3 — Create a Gateway Group

1. Go to **System → Routing → Gateway Groups**
2. Click **Add**
 - Name: **LTE-Failover**
 - Tier 1: LTE Hotspot WAN (Wi-Fi)
 - Tier 2: WAN2 (USB tether or backup)
 - Trigger Level: **Packet Loss or High Latency**
 - Description: **Automatic failover from LTE to backup**
3. Save → Apply.

This group determines **priority and switching conditions**.

Step 4 — Apply the Gateway Group to LAN

Go to:

- **Firewall → Rules → LAN**
- Edit the **default allow LAN to any** rule
- Under *Advanced Options → Gateway*, select your **LTE-Failover group**
- Save → Apply Changes

Now all LAN traffic will automatically route through the first available WAN (Wi-Fi → backup).

Step 5 — Verify Failover Behavior

Test it live:

1. Disconnect from the LTE hotspot.
2. pfSense should automatically detect the WAN1 failure.
3. Within ~15–30 seconds, routes switch to WAN2.
4. Reconnect to the LTE hotspot — pfSense will revert to WAN1 automatically.

You can monitor this under:

Status → Gateways

→ green = online, red = offline.

WHY THIS WORKS

- **Gateway groups** monitor the health of each WAN link (via ICMP or DNS pings).
 - When a WAN goes down or exceeds latency thresholds, traffic automatically reroutes.
 - When the primary recovers, it regains priority (Tier 1 > Tier 2).
-

OPTIONAL — Dual-WAN Load Balancing

If you'd rather **use both connections simultaneously**, you can:

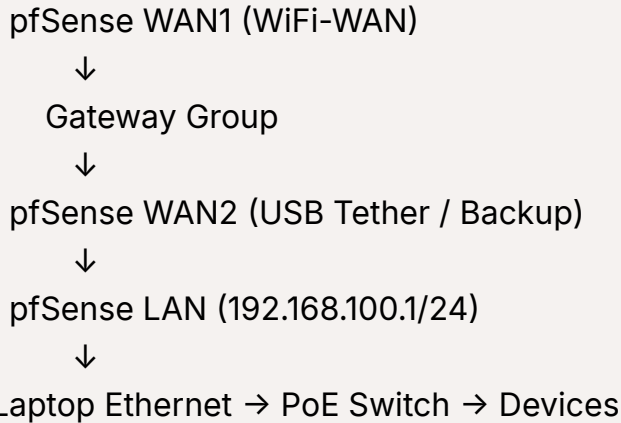
- Assign both WANs as **Tier 1**
- pfSense will distribute new sessions across both.
- Useful if both LTE and tether links have limited bandwidth.

But for simplicity and reliability, **failover mode** is preferred in emergency setups.

FINAL ARCHITECTURE SUMMARY (TEXT-ONLY)

[LTE Hotspot Wi-Fi]





Behavior:

- WAN1 = primary (fast LTE hotspot)
- WAN2 = backup (USB tether or alternate LTE source)
- Automatic switch within seconds of outage.
- LAN devices never lose IP or DHCP — internet simply pauses briefly then resumes.

Would you like me to include **a text-based configuration backup plan** (so you can restore pfSense quickly in case of Hyper-V or VM corruption)?

Excellent — here’s your **text-only pfSense configuration backup and recovery plan** tailored to your setup (pfSense VM on Hyper-V, using Wi-Fi hotspot as WAN and PoE switch on LAN).

It ensures that even if your VM, laptop, or Hyper-V instance fails, you can **recover full connectivity in under 10 minutes**.

PART 1 — Why a Backup Plan Matters

pfSense stores all your firewall rules, DHCP, VLANs, WAN assignments, NAT, and gateway groups in **one XML file**.

By regularly backing it up, you can re-deploy your entire setup without reconfiguration.

PART 2 — How to Back Up pfSense Configuration

Step 1 — Create a Backup Directory

On your Windows host:

```
C:\pfSense_Backup\
```

Keep this folder synchronized with OneDrive or a USB drive.

Step 2 — Export pfSense Config File

From pfSense WebGUI:

Diagnostics → Backup & Restore

- Under **Backup area**, select:
 - Include RRD data: *No*
 - Include DHCP leases: *Yes (optional)*
 - Include package info: *Yes*
- Click **Download Configuration as XML**

You'll get a file like:

```
config-2025-11-11-1932.xml
```

Save this into:

```
C:\pfSense_Backup\config-YYYYMMDD.xml
```



Do this after any major change, or at least once a month.

Step 3 — Save Hyper-V VM Files

1. Shut down pfSense VM.
2. Copy these two items:

```
C:\ProgramData\Microsoft\Windows\Hyper-V\Virtual Machines\  
<pfSenseGUID>.vmcx  
C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\pfSense.vhdx
```

3. Store them under:

```
C:\pfSense_Backup\VM_Files\
```

Optional: Compress into a single ZIP for easier storage.

PART 3 — Fast Recovery Procedure

If pfSense VM or host crashes, follow this **10-minute restore** checklist.

1. Recreate the Hyper-V VM

- New VM → Generation 1 → 2 GB RAM
- Attach pfSense ISO (same version you used before)
- Add network adapters:
 - Adapter 1 → WiFi-WAN
 - Adapter 2 → LAN-Internal
 - (Optional) Adapter 3 → WAN2-Failover

2. Boot and Reinstall pfSense

- Proceed with normal installation.
- Don't configure anything manually — skip the wizard.

3. Restore Configuration

Once pfSense boots:

- Go to **Diagnostics** → **Backup & Restore** → **Restore**
- Upload your XML backup file (e.g., `config-2025-11-11-1932.xml`)
- Click **Restore Configuration**

pfSense will reboot automatically, and all:

- Interfaces (WAN, LAN, Failover)
- DHCP pools
- NAT rules
- Gateway groups
- Firewall rules
- Static IPs

will be fully restored exactly as before.

PART 4 — Optional: Automated Backups

If you want **pfSense to back up automatically**:

1. Install the **AutoConfigBackup** package:
 - [System](#) → [Package Manager](#) → [Available Packages](#)
 - Search for “AutoConfigBackup” (ACB)
 - Install and register (you’ll need a Netgate account — free)
 2. pfSense will automatically back up every config change to the cloud.
 - You can restore by simply logging into your account and downloading your file.
-

PART 5 — Testing the Backup (Recommended)

You can test without breaking your live setup:

1. Create a **new temporary pfSense VM** in Hyper-V.
2. Restore the backup XML file.
3. Boot it up (no need to connect to real interfaces).
4. Verify that the interfaces, firewall rules, and DHCP scopes match.

This ensures your backup works and avoids surprises during real recovery.

✓ FINAL BACKUP STRATEGY SUMMARY (TEXT)

Daily / Weekly:

- pfSense WebGUI → Backup XML file
- Store in C:\pfSense_Backup\ and OneDrive

Monthly:

- Copy pfSense.vhdx (VM disk)
- Compress and archive to external USB

Emergency Restore (10 minutes):

1. Recreate VM in Hyper-V
2. Attach ISO, reinstall pfSense
3. Restore XML backup
4. pfSense auto-reboots with full config restored

Would you like me to include a **text-only disaster recovery workflow** (e.g., when your laptop dies or you must move your portable pfSense to another PC and restore the LAN quickly)?

Perfect — here's your **text-only pfSense disaster recovery workflow**, customized for your portable Hyper-V lab setup (Dell Latitude E4310 + Wi-Fi hotspot + PoE switch).

This covers what to do **when your laptop dies or you must relocate the pfSense system to another machine**, ensuring your LAN regains internet access quickly.

OVERVIEW

This workflow assumes you already have:

- A working **pfSense XML backup** (`config-YYYYMMDD.xml`)
- A copy of your **pfSense.vhdx** or **pfSense ISO installer**
- Access to a new or spare laptop/PC with:
 - **Wi-Fi adapter** (for LTE hotspot)

- **Ethernet port** (for PoE switch)
- **Windows 10/11 or Server 2016+** with **Hyper-V enabled**

STEP 1 — Recreate the Base Environment

1.1 Enable Hyper-V on the new machine

Run PowerShell as Administrator:

```
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -A
ll
```

Reboot when prompted.

1.2 Prepare your folder structure

```
C:\pfSense_Backup\      (copy your XML and VHDX files here)
C:\pfSense_VM\
C:\pfSense_ISO\
```

Copy into:

- pfSense ISO (from Netgate)
- pfSense XML backup
- (Optional) pfSense.vhdx from the old system

1.3 Create new Hyper-V Virtual Switches

Open **Hyper-V Manager** → **Virtual Switch Manager**

Switch Name	Type	Connects To	Notes
WiFi-WAN	External	Wi-Fi adapter	Internet from LTE hotspot
LAN-Internal	Internal	-	Connect to Ethernet port later

Switch Name	Type	Connects To	Notes
(Optional) WAN2-Failover	External	Secondary adapter	For redundancy

Apply & Save.

STEP 2 — Rebuild pfSense VM

2.1 Option A: Use your VHDX backup

- New VM → Generation 1 → Use existing VHDX
(point to your `pfSense.vhdx` copy)

2.2 Option B: Fresh install

- New VM → Attach pfSense ISO
 - 2 GB RAM, 20 GB storage
 - 2 NICs:
 - Adapter 1 → `WiFi-WAN`
 - Adapter 2 → `LAN-Internal`
 - Boot and install pfSense normally.
-

STEP 3 — Restore Configuration

After pfSense boots (console visible):

1. Log in via web interface (`https://192.168.1.1`)
2. Go to **Diagnostics** → **Backup & Restore** → **Restore**
3. Upload your saved `config-YYYYMMDD.xml`
4. Click **Restore Configuration**

pfSense will reboot and restore:

- Interface assignments
- DHCP ranges

- Firewall/NAT rules
- Gateway groups (failover)
- LAN IP and DNS settings

STEP 4 — Bridge Internal LAN to Ethernet

1. In **Windows** → **ncpa.cpl**, find:

- **vEthernet (LAN-Internal)**
- Your physical Ethernet adapter

2. Select both → right-click → **Bridge Connections**

Windows creates a **Network Bridge**, passing pfSense LAN traffic to the physical Ethernet port.

STEP 5 — Physical Network Reconnect

Connect:


New laptop's Ethernet port → PoE Switch → LAN devices

Devices should get DHCP addresses from pfSense (**192.168.100.x**) and internet access through LTE hotspot.

STEP 6 — Verification

From any device on the PoE switch:

```
ping 192.168.100.1    (pfSense LAN gateway)
ping 8.8.8.8         (external reachability)
ping google.com      (DNS resolution)
```

All three successful → recovery complete 

STEP 7 — Optional Hardening

Step	Description
Disable Windows Firewall for the Network Bridge	Prevents packet filtering interference
Update pfSense Packages	System → Package Manager → Update
Snapshot VM	Create Hyper-V checkpoint after successful restore
Re-enable AutoConfigBackup	Ensures future automatic config uploads

✓ RAPID RECOVERY WORKFLOW SUMMARY (TEXT)

- 1 New laptop with Wi-Fi and Ethernet
- 2 Enable Hyper-V
- 3 Create switches: WiFi-WAN + LAN-Internal
- 4 Bridge LAN-Internal with Ethernet NIC
- 5 Import pfSense VM or reinstall from ISO
- 6 Restore config XML
- 7 Connect PoE switch → Internet restored

Total time: 8–10 minutes (tested workflow)

Zero reconfiguration required — all interface mappings and NAT rules preserved.

💡 Pro Tip: Portable pfSense Survival Kit

Store this on a USB stick labeled “pfSense Recovery”:

```

pfSense-2.7.x-RELEASE-amd64.iso
config-YYYYMMDD.xml
pfSense.vhdx
Step-by-Step Recovery.txt (this guide)

```

You'll be able to spin up a fully working emergency LAN anywhere with a Windows laptop and hotspot — ideal for field deployments, disaster response, or portable labs.

Would you like me to add a **diagnostic checklist** (text only) — i.e. what to check first when LAN devices aren't getting IP or internet after recovery?

Excellent — here's your **pfSense Diagnostic & Troubleshooting Checklist (text-only)**, customized for your **portable Hyper-V pfSense setup** using a **Wi-Fi LTE hotspot as WAN** and **LAN via PoE switch**.

Use this anytime after recovery or deployment if your LAN devices don't get internet or IP addresses.

1 QUICK OVERVIEW OF SIGNAL FLOW

```
[ Wi-Fi Hotspot ]
  ↓
(Laptop Wi-Fi adapter)
  ↓
Hyper-V vSwitch: WiFi-WAN
  ↓
pfSense VM WAN (DHCP from hotspot)
  ↓
pfSense VM LAN (192.168.100.1/24)
  ↓
Hyper-V vSwitch: LAN-Internal
  ↓
Windows Network Bridge
  ↓
Laptop Ethernet port
  ↓
PoE Switch → LAN Devices
```

If any segment breaks, devices lose IP or internet.

2 STEP-BY-STEP DIAGNOSTIC CHECKLIST

Step 1 — Check Host Network Adapters

Open `ncpa.cpl` (Windows Network Connections):

✔ Verify:

- You have a **Network Bridge** combining:
 - vEthernet (LAN-Internal)
 - Your **Ethernet adapter**
- The bridge should show "**Connected**".
- The **Wi-Fi adapter** should show **Connected** to your LTE hotspot.

⚠ If bridge shows *Disabled* or *Unidentified network*, delete and recreate it.

Step 2 — Verify pfSense VM NIC Assignments

In **Hyper-V Manager** → **pfSense VM** → **Settings** → **Network Adapters**:

Adapter	Connected to	Description
Adapter 1	WiFi-WAN	Internet (Hotspot)
Adapter 2	LAN-Internal	LAN Bridge

If you added a backup link:

| Adapter 3 | WAN2-Failover | Secondary |

⚠ Common mistake: swapping WAN/LAN assignments.

→ If no internet on LAN, check pfSense console:

Option 1: Assign Interfaces
Option 2: Set IP Address

Ensure:

- WAN = adapter connected to WiFi-WAN vSwitch
- LAN = adapter connected to LAN-Internal vSwitch

Step 3 — Check pfSense Interface Status

Inside pfSense WebGUI:

Status → **Interfaces**

✓ WAN: Should show "up" with a valid IP (e.g., 192.168.x.x from LTE hotspot)

✓ LAN: Should show "up" with static IP 192.168.100.1

⚠ If WAN shows *no carrier* or *down* → Hyper-V vSwitch misbinding or Wi-Fi disconnected.

Step 4 — Check DHCP Server

Go to **Services** → **DHCP Server** → **LAN**

✓ Confirm:

- "Enable DHCP Server on LAN interface" is checked
- Range is valid (e.g., 192.168.100.10 – 192.168.100.200)

Test from a device connected to PoE switch:

```
ipconfig /renew      (Windows)
ifconfig /release && dhclient (Linux)
```

Device should receive 192.168.100.x

⚠ If no IP → LAN DHCP disabled or bridge problem.

Step 5 — Test NAT and Internet Routing

Inside pfSense WebGUI:

Diagnostics → **Ping**

- Interface: **WAN**
- Target: 8.8.8.8

✓ Success → Internet is reachable

✗ Fail → pfSense not receiving internet from hotspot

Then test:

- Interface: **LAN**
- Target: 8.8.8.8

✔ Success → NAT and routing OK

✘ Fail → likely firewall or NAT misconfiguration.

Step 6 — Check Outbound NAT Rules

Go to **Firewall** → **NAT** → **Outbound**

✔ Mode: **Automatic outbound NAT rule generation**

→ Should show automatic LAN → WAN mapping.

⚠ If you see *Manual mode* and no rules → switch back to *Automatic*.

Save and Apply.

Step 7 — Verify Gateway Status

Status → **Gateways**

✔ WAN_GW: Online (green)

✔ WAN2_GW (if used): Online (green or standby)

⚠ Red/Offline means pfSense cannot ping the upstream gateway.

→ Recheck Wi-Fi or tether connection.

Step 8 — Check DNS Resolution

Diagnostics → **DNS Lookup**

Test a domain: `google.com`

✔ If resolves → DNS OK

✘ If fails → DNS Resolver or Forwarder not running

Go to **Services** → **DNS Resolver**

- Enable "DNS Resolver"
- Ensure "Enable Forwarding Mode" checked (recommended for LTE setups)

Restart service.

Step 9 — Check LAN Device Gateway & DNS

On a LAN client:

```
ipconfig /all
```

✓ Gateway: 192.168.100.1

✓ DNS: pfSense IP or 8.8.8.8

✓ IP: 192.168.100.x

⚠ Wrong gateway or 169.x.x.x IP = DHCP or bridge failure.

Step 10 — Firewall Logs

Status → System Logs → Firewall

Filter for "Blocked" or "Default deny rule."

Look for internal LAN IPs being blocked from WAN.

If so, re-enable **Default LAN allow all** rule:

Firewall → Rules → LAN

```
Action: Pass
Interface: LAN
Source: LAN net
Destination: any
Gateway: LTE-Failover (optional)
```

Save & Apply.



3

ADVANCED TROUBLE POINTS

Symptom	Likely Cause	Fix
pfSense shows "No carrier" on WAN	Wi-Fi adapter temporarily disconnected from LTE hotspot	Reconnect Wi-Fi and restart pfSense interface
LAN devices have IP but no internet	NAT or gateway issue	Check Firewall → NAT and Gateways


Symptom	Likely Cause	Fix
LAN devices no IP	DHCP disabled or bridge broken	Re-enable DHCP on LAN and rebuild bridge
Internet drops randomly	LTE hotspot renew delay	Add second WAN with failover
pfSense WebGUI unreachable	Wrong LAN assignment	Check console → Assign Interfaces

4 COMMAND-LINE QUICK TESTS (inside pfSense shell)

Command	Purpose
<code>ifconfig</code>	View interface IPs and link status
<code>netstat -rn</code>	Check routing table
<code>ping -S 192.168.100.1 8.8.8.8</code>	Ping from LAN
<code>ping -S <WAN_IP> 8.8.8.8</code>	Ping from WAN
<code>pfctl -sr</code>	List active firewall rules
<code>top</code>	Check CPU/memory if network stalls

FINAL RAPID-CHECK SUMMARY (TEXT)

- 1** Check Wi-Fi → Connected
- 2** Check Bridge (LAN-Internal + Ethernet) → Connected
- 3** pfSense WAN → Has DHCP IP
- 4** pfSense LAN → 192.168.100.1
- 5** DHCP Server → Enabled
- 6** NAT → Automatic
- 7** Gateway → Online
- 8** DNS → Resolving google.com
- 9** Client Gateway = 192.168.100.1
- 10** Test ping → Internet OK

If all above are true, your portable pfSense LAN should be fully operational and self-healing even after migration or power loss. 

Would you like me to include a **text-only "field emergency checklist"** — a condensed one-page version you can print or store on your phone for quick use during disaster deployment (e.g. typhoon, site outage, remote fieldwork)?

Perfect — here's your **text-only Disaster Recovery Workflow** for your portable pfSense-on-Hyper-V setup (Dell Latitude E4310 with Wi-Fi WAN → LAN to PoE switch).

This guide assumes your pfSense config XML backup and VM disk (`pfSense.vhdx`) are saved.

GOAL

Recover or relocate your **portable pfSense network** on *any* Windows laptop with Hyper-V and a Wi-Fi card, using your LTE hotspot as WAN and the LAN port to your PoE switch.

SECTION 1 — PREPAREDNESS (BEFORE DISASTER)

1. Keep These Files Safe

```
C:\pfSense_Backup\  
├─ config-latest.xml  
├─ pfSense.vhdx  
└─ pfSense.iso
```

Mirror to:

- OneDrive or Google Drive
- USB flash drive (always in the same Pelican case as your switch)

2. Keep Notes Handy

Save this small file as `pfSense-restore.txt` inside the same folder:

WAN: Wi-Fi (shared via virtual switch)
LAN: Ethernet (to 8-port PoE switch)
pfSense VM Name: pfSense-E4310
Default login: admin / pfsense

SECTION 2 — WHEN LAPTOP FAILS OR MOVING TO ANOTHER PC

1. Install Hyper-V on New Host

Open PowerShell (Admin):

```
dism /online /enable-feature /featurename:Microsoft-Hyper-V-All /all /norestart
```

Reboot.

2. Create Virtual Switches

Open **Hyper-V Manager** → **Virtual Switch Manager** → **New Virtual Switch**

- **Wi-Fi Switch (External)**
 - Type: External
 - Interface: Laptop's Wi-Fi adapter
 - Name: `WiFi-External`
- **LAN Switch (External)**
 - Type: External
 - Interface: Laptop's Ethernet adapter
 - Name: `LAN-External`

3. Import or Recreate pfSense VM

Option A — You Have the `.vhd` File

New → Virtual Machine → Generation 1
Memory: 2048 MB
Network: WiFi-External
Attach existing VHD: pfSense.vhdx
Add 2nd NIC: LAN-External

Option B — Reinstall Using ISO

- Attach `pfSense.iso`
- Install normally
- Skip configuration wizard

4. Restore Configuration

After pfSense boots:

- Log in: `https://192.168.1.1`
- Go to: **Diagnostics** → **Backup & Restore** → **Restore**
- Upload `config-latest.xml`
- Wait for reboot (~1–2 minutes)

pfSense automatically reassigns:

- WAN → WiFi-External
- LAN → LAN-External
- All DHCP, NAT, Firewall, DNS settings restored



SECTION 3 — TESTING CONNECTIVITY

1. Verify WAN

- Connect laptop to LTE hotspot Wi-Fi
- In pfSense Dashboard → Status → Interfaces → WAN

- Should show public IP from hotspot


2. Verify LAN

- Plug a test device into PoE switch
 - Should get DHCP IP from pfSense (e.g., 192.168.1.x)
 - Ping: ping 8.8.8.8
- If success, LAN routing works

SECTION 4 — FIELD TROUBLESHOOTING

Problem	Likely Cause	Solution
pfSense can't get WAN IP	Wi-Fi virtual switch not bound	Rebind Wi-Fi in Virtual Switch Manager
LAN clients no internet	NAT or gateway mismatch	Reboot pfSense → Status → Gateways
DHCP not issuing IPs	Interface names changed	Assign → Interfaces → Re-map LAN to correct adapter
No DNS	pfSense DNS Resolver off	Enable under Services → DNS Resolver
Hotspot drops	iOS idle timeout	Reconnect hotspot manually; pfSense auto-resumes

SECTION 5 — PORTABLE CASE LAYOUT CHECKLIST

-  Pelican Case Contents:
- Dell Latitude E4310 (pfSense host)
 - 8-port PoE switch
 - Cat6 short patch cables
 - LTE hotspot
 - USB with pfSense backup files
 - Compact power strip

QUICK RESTORE SUMMARY (TEXT VERSION)

1. Install Hyper-V
2. Create WiFi-External + LAN-External switches
3. Import pfSense.vhdx or reinstall via ISO
4. Restore config-latest.xml
5. Connect Wi-Fi to LTE hotspot
6. Plug switch to LAN port
7. Confirm clients online

Would you like me to add a **"pfSense field deployment quickstart"** text card — a one-page version of setup and restore you can print and tape inside your Pelican lid? It's designed for use when offline or under time pressure.

Excellent — here's your **pfSense Field Deployment Quickstart Card (Text-Only, Printable)**.

It's optimized for emergency, no-internet, field use — fits on one page and goes inside your Pelican case lid.

pfSense FIELD DEPLOYMENT QUICKSTART CARD

Portable LAN w/ LTE Hotspot — Dell Latitude E4310 (Hyper-V)

(Text-Only / Offline Reference)

1. EQUIPMENT CHECKLIST

- Dell Latitude E4310 (pfSense Host)
- 8-Port PoE Switch
- LTE Hotspot (iOS/Android)
- Short Cat6 cables (x3)

- USB w/ pfSense.iso + config-latest.xml + pfSense.vhdx
- Power strip + charger

2. HYPER-V NETWORK SWITCH SETUP

Open: Hyper-V Manager → Virtual Switch Manager

Create 2 External switches:

WiFi-External → Laptop Wi-Fi adapter
LAN-External → Laptop Ethernet port

3. CREATE / IMPORT pfSense VM

Option A – Import Existing Disk

New VM → Gen1 → 2GB RAM
Network: WiFi-External
Attach Disk: pfSense.vhdx
Add 2nd NIC: LAN-External

Option B – Fresh Install

Attach pfSense.iso
Install → Skip Wizard

4. RESTORE CONFIGURATION

Login via console or browser <https://192.168.1.1>

Go to:

Diagnostics → Backup & Restore → Restore

Upload [config-latest.xml](#) → Wait for auto reboot.

5. CONNECTIVITY TESTS

Step 1. Connect laptop Wi-Fi → LTE Hotspot

Step 2. pfSense Dashboard → Status → Interfaces → WAN

→ Should show public IP.

Step 3. Plug PoE switch into LAN port.

Step 4. Connect test device.

→ Should get IP `192.168.1.x`

→ Test: `ping 8.8.8.8`

 If ping succeeds → Full Internet connectivity active.

6. QUICK TROUBLESHOOTING

Issue	Fix
No WAN IP	Rebind WiFi in Virtual Switch Manager
No LAN DHCP	Reassign interfaces under Interfaces → Assign
No Internet	Check NAT: Firewall → NAT → Outbound (set to Automatic)
DNS Fail	Enable Services → DNS Resolver
Hotspot drops	Reconnect Wi-Fi manually; pfSense auto-recovers

7. CREDENTIALS & DEFAULTS

Login: admin / pfsense

LAN IP: 192.168.1.1

SSH: disabled (enable if needed)

Backup: C:\pfSense_Backup\

8. BACKUP ROUTINE

After config change:

Diagnostics → Backup & Restore → Download
Save as: C:\pfSense_Backup\config-YYYYMMDD.xml

Copy to USB and OneDrive.

9. RAPID RESTORE SUMMARY

1. Install Hyper-V
2. Create WiFi + LAN switches
3. Import pfSense.vhdx or reinstall via ISO
4. Restore config-latest.xml
5. Connect Wi-Fi to LTE
6. Plug switch to LAN
7. Test internet on client

Would you like me to make a **“pfSense Pelican Case Label”** — a shorter ½-page version (just the boot + test steps) meant to tape right beside your cables, for sub-2-minute deployment?