Firewall Core + WFP Monitor
Unified Documentation

Overview

Firewall Core is a defensive Windows Firewall and WFP monitoring framework designed to detect, log, and optionally enforce outbound network behavior using a phased escalation model (A–C4).

Directory Layout

C:\Firewall\
- Install-Firewall.ps1
- Uninstall-Firewall.ps1
- firewall-install.cmd
- uninstall-firewall.cmd
- install-debug.log
- README.md
- Monitor\
- Modules\
- Maintenance\
- Scripts\
- State\
- Tests\
- Logs\

Installer

The installer copies payload files, enables WFP auditing, applies firewall rules, registers scheduled tasks, and initializes state files. A CMD wrapper is provided for elevation and logging.

CMD Wrappers

firewall-install.cmd launches Install-Firewall.ps1 as Administrator and captures output to install-debug.log. uninstall-firewall.cmd performs the inverse cleanup.

WFP Monitor Phases

Phase A: Audit only
Phase B: Baseline observation
Phase C2: Temporary blocking
Phase C3: Persistent blocking
Phase C4: Deny-hash enforcement

State Files

- baseline.json: firewall rule baseline
- wfp.bookmark.json: last processed event
- wfp.strikes.json: escalation counters
- wfp.blocked.json: enforced blocks
- wfp.denyhash.json: permanent deny list

Event IDs

3400 – Summary
3401 – Alert
3402 – Persistent block
3404 – Deny-hash block

Security Model

Least privilege, SYSTEM-only enforcement, signed scripts, tamper detection, and reversible deployment.

Uninstall (Planned)

The uninstall process removes scheduled tasks, firewall rules, certificates, and restores defaults while preserving logs if requested.