DHCP Shield Pro

Enterprise DHCP Traffic Intelligence & Security Platform

Full DHCPv4 (RFC 2131) + DHCPv6 (RFC 8415) support. Works with any DHCP server, any vendor. Scales from branch offices to 10M+ managed devices.

Kernel-level enforcement | Self-hosted · air-gap ready | 10,000+ msg/s | MCP-native

Document version 2.1 · 2026-06-04

01 Overview

DHCP Shield Pro is a high-performance, kernel-integrated platform for DHCP traffic intelligence and security across IPv4 and IPv6 networks. It delivers complete visibility into DHCP traffic, automated threat detection and response, kernel-level enforcement at wire speed, and full traffic retention for compliance and forensics. **It is built for the protocol, not adapted to it.**

Designed for network security teams and DHCP infrastructure owners who need to identify rogue devices, prevent DHCP-based attacks, and keep control over address allocation — all without impacting DHCP server performance. It works with any DHCP server, any vendor, and scales from branch offices to deployments serving over 10 million devices.

Yours to run, end to end. Once deployed, the platform operates autonomously — measuring all DHCP traffic, acting on threats through configurable automation, and reporting on network behavior. Self-hosted, offline-capable, with a complete audit trail and no cloud dependency. **Nothing leaves your network unless you open a support session.**

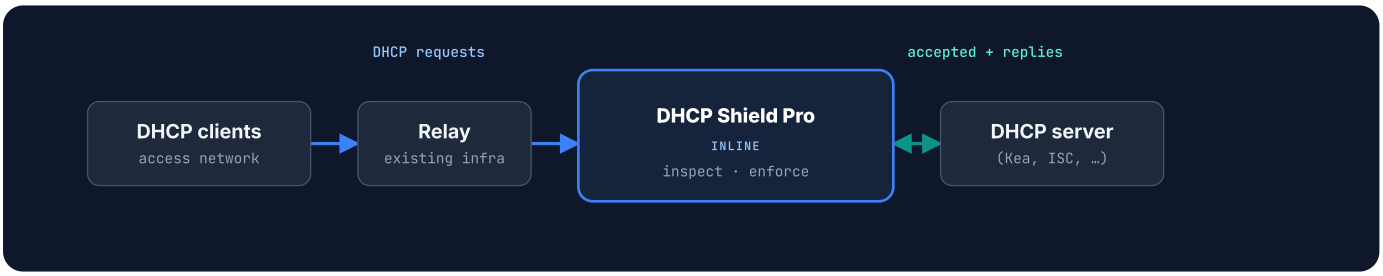
02 Deployment Architectures

Three ways to place the appliance in your network — from **full inline enforcement** to a completely **passive observer**. Pick per segment; mix and match across a single estate.

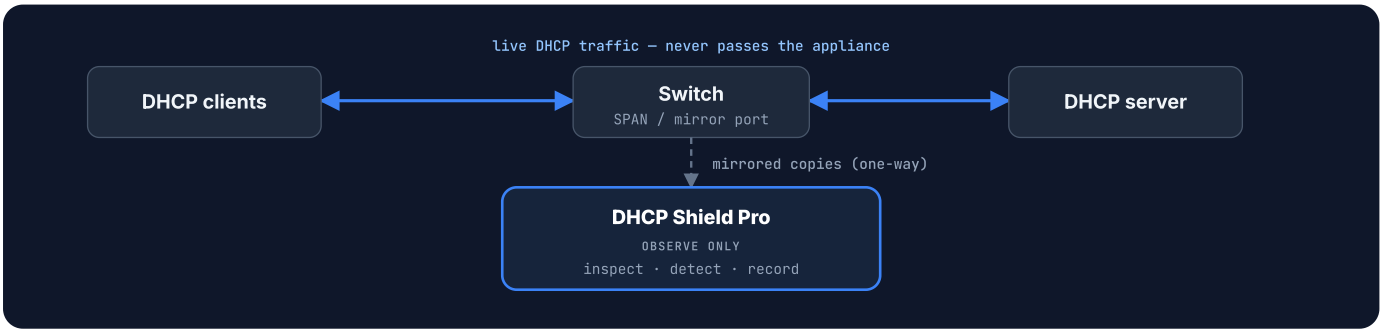
Mode	Network position	Live-traffic impact	What it does	Best for
Inline	In the DHCP path	Sub-ms added latency; fail-open	Full inspection **+ active enforcement**	Segments that must block, throttle or deny in real time
Mirrored `passive`	Off-path; receives a SPAN / mirror copy	**Zero** — live traffic untouched	Full inspection & detection; actions recorded, not applied	Evaluation, sensitive segments, monitor-only mandates
Remote sites	Central collector; sites forward copies	**Zero**; one-way over the WAN	Centralized visibility across many locations	Multi-site estates feeding a single console

Solid blue — live DHCP traffic Solid teal — accepted traffic Dashed — mirrored copies, one-way

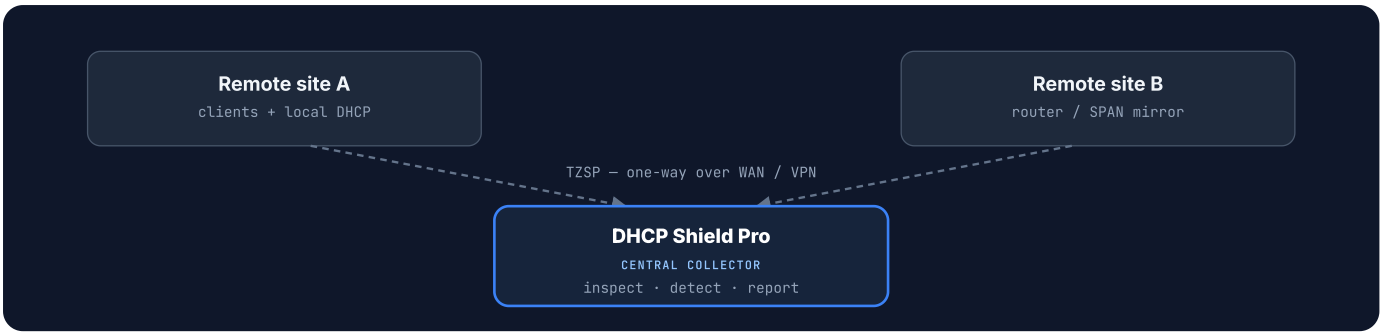
MODE 1 Inline (full control) — the appliance sits in the DHCP path and enforces in real time.



MODE 2 Mirrored (passive) — off-path on a SPAN copy. Zero traffic impact; observe only.



MODE 3 **From remote sites** — many sites forward one-way copies to one central appliance.



03 Key Capabilities

Everything below ships in one self-hosted appliance — no add-on modules, no per-feature SKUs.

Deep Packet Inspection

Full DHCPv4 + DHCPv6 parsing — all message types, all options, relay agent suboptions, DUID resolution.

Kernel-Level Enforcement

Block, deny, throttle, allow, monitor — sub-ms latency via Linux nftables, zero DHCP server impact.

Automated Detection & Response

Rule-based scheduler: configurable thresholds, 30+ filter fields, priority-ranked actions, full audit trail.

AI-Powered Analysis `optional`

LLM anomaly detection with risk scoring (0–10), triggered as an automation action.

Traffic Retention

90-day default, full transaction logs, MAC history search, CSV/PCAP export for compliance and law enforcement.

Real-Time Streaming

DHCP Stream console with 30+ server-side filters, regex, compound AND/OR logic.

Packet Capture

tshark-powered, BPF filters, WebSocket streaming, PCAP download, full protocol dissection in-browser.

Dashboards & Reporting

8 dashboards, 67+ widgets, weekly automated reports, custom report builder, Sankey flow visualization.

REST API & CLI

230+ endpoints and 230+ `dpictl` commands — every GUI action scriptable, with an in-product OpenAPI reference.

AI Assistant Integration MCP

Native MCP server: query traffic, triage alarms, enforce from Claude Code or any MCP client — read by default, writes gated.

Operational Metrics

Prometheus scrape endpoint with dedicated token auth — health and operational metrics only, no per-device data on the wire.

Built for the Protocol

DHCPv4 (RFC 2131) and DHCPv6 (RFC 8415) native — not bolted onto a generic packet broker.

04 Network Visibility & Compliance

Every DHCP packet is parsed, classified, and stored — every field below is extracted and searchable across the full retention window.

DHCPV4 FIELDS · RFC 2131

Field	Reference	Detail
Client MAC	chaddr	Hardware address of requesting client
Source MAC	Ethernet header	Layer-2 source; may differ from chaddr behind relays
Client Identifier	Option 61	Unique client identity (RFC 4361)
Hostname	Option 12	Client-supplied hostname
Vendor Class	Option 60	Device type / manufacturer string
FQDN	Option 81	Fully qualified domain name (RFC 4702)

Field	Reference	Detail
Requested IP	Option 50	Address the client prefers
Server ID	Option 54	Responding server identity
Message Type	Option 53	DISCOVER, OFFER, REQUEST, ACK, NAK, DECLINE, RELEASE, INFORM
Lease Time	Option 51	Granted lease duration
XID	Header	Transaction ID for DORA correlation

OPTION 82 SUBOPTIONS · RELAY AGENT INFO

Suboption	RFC	Purpose
Circuit ID	3046	Port / VLAN identification
Remote ID	3046	Relay device identity
Link Selection	3527	Subnet selection for forwarding
Subscriber ID	3993	ISP subscriber identification
RADIUS Attributes	4014	RADIUS-sourced relay metadata
Access Network ID	7839	Access network type and identity
Vendor-Specific	4243	Relay vendor extensions

DHCPV6 FIELDS · RFC 8415

Field	Detail
Client / Server DUID	LLT, EN, LL, UUID variants
Message Type	All 13 types (Solicit ... Relay-Reply)
Link Address	Relay link address for subnet
Peer Address	Client-facing address at relay
Interface / Remote ID	Relay interface and identity
Subscriber ID	Subscriber identification
IA Address / IA Prefix	Assigned address; delegated prefix (PD)
T1 / T2 Timers	Renewal and rebind timers

COMPLIANCE FEATURES

- **MAC history search** — look up any MAC across the full retention window; export for audit or law enforcement.
- **Transaction reconstruction** — rebuild complete DHCP conversations by XID, including all options exchanged.
- **90-day default retention** — configurable; all transactions stored with full field fidelity.
- **CSV export** — any filtered view exportable for offline analysis or regulatory submission.

05 Device Management & Monitoring

Every device that sends a DHCP message is catalogued automatically — **no agents, no enrollment.** Presence on the network is enough.

PER-DEVICE RECORD

Data point	Retention
Complete message history	90 days (configurable)
Message type distribution	5min / 1h / 24h / 7d
Enforcement actions executed	Full history
LLM analysis & risk scores	Full history
IP address history	90 days
Vendor / hostname changes	90 days
Relay paths	90 days
Protocol indicator	v4 / v6 / dual-stack
Hourly & daily patterns	90 days

REAL-TIME MONITORING

DHCP Stream console

Live view, 30+ server-side filters with regex and compound AND/OR. Clients receive only matching traffic — no bandwidth waste.

Packet capture

Embedded tshark + BPF, streamed to the browser over WebSocket. Wireshark-depth dissection; PCAP download. No external tools.

Interactive terminal

Browser-based `dpictl` (230+ commands) — every GUI function, scriptable.

Historical search

90-day retention, regex across all fields, pre-aggregated at 5min/1h/24h/7d, CSV export.

On-demand device probe: embedded nmap-based diagnostics from the GUI or API. **Protocol badges** distinguish v4-only, v6-only, and dual-stack devices at a glance.

06 Threat Detection & Response

The application inspects and classifies; the **Linux kernel enforces**. That separation is what delivers wire-speed control with zero load on your DHCP server.

> **Fail-open by design.** Enforcement runs in kernel space via nftables, **before packets reach the server** — sub-millisecond latency, automatic TTL expiration so no stale rules accumulate, and per-message-type policies. If the application stops, traffic passes through unimpeded.

ACTION REFERENCE

Block — `2 hours`
Drop all DHCP traffic from device. Events still recorded for audit.

Deny — `indefinite`
Drop all traffic and suppress events. Device goes silent.

Throttle — `24 hours`
Rate-limit requests to a configurable ceiling.

Allow — `30 days`
Bypass inspection. For trusted infrastructure devices.

Monitor — `7 days`
Enhanced logging. No enforcement.

Cleanup — `instant`
Remove device from all enforcement sets immediately.

Every action is reversible with a dedicated undo. Bulk actions support filter-based selection, preview with sampling, job management, progress tracking, and MAC export.

FIREWALL MANAGER

Full web-based management of the nftables configuration — no SSH or command line required.

Ruleset management	Detail
Configuration library	Save, name, version, restore — full audit trail
JSON editor	Syntax highlighting, bracket matching, search, undo/redo
Import / Export	Standard nftables JSON (`nft -j`) — portable
Validation	Checked against the kernel before applying
Pre-built profiles	Low / Medium / Strict throttling, v4 & dual-stack
Soft delete & restore	Recoverable; full version history preserved

Application modes

Mode	Scope / use case
Add	Append rules — incremental, minimal risk
Table	Replace the DHCP inspection table only — standard updates
All	Flush entire ruleset and replace — full reset, confirmed

Firewall visualizer

- Chain-by-chain rendering, color-coded actions
- Hook selection: prerouting → postrouting
- Live per-rule packet / byte counters with deltas
- Set & map inspector; saved-vs-running side by side

AUTOMATION ENGINE

Runs on a configurable schedule, querying pre-aggregated traffic data to detect anomalies without manual intervention.

Rule parameter	Options
Source table	5min / 1h / 24h / 7d aggregation
Lookback interval	Configurable (e.g. 1h, 24h)
Filter criteria	30+ DHCP fields, DHCP-Stream syntax
Thresholds	Request count, unique IPs — AND/OR
Action on match	Block, deny, throttle, allow, monitor, **analyze**
Priority	1–100; highest wins on conflict
Check interval	How frequently the rule executes

AI analysis `optional`

The **analyze** action sends matched traffic to the LLM engine — one of six automation actions, not a separate subsystem. It returns:

- Risk score (0.0–10.0) with classification rationale
- Recommended action with confidence level
- Behavioral observations — spoofing, starvation, coordination signals

Supports local LLM backends and any OpenAI-compatible endpoint. Runs entirely on-premises with local models.

Alarms

Firing → Acknowledged → Resolved. SLA tracking on time-to-ack and time-to-resolve; escalation when alarms linger. Every automation run is logged: rule, MACs affected, action, result.

07 Reporting & Executive Visibility

Generated automatically — a weekly executive report every Monday at 03:00 UTC, plus 8 live dashboards. **No configuration required.**

WEEKLY TRAFFIC REPORT

Section	Detail
Total traffic	Incoming, accepted, blocked counts
DHCPv4 / v6 breakdown	Per-message-type, with blocked totals
Unique MACs	Daily average across the window
Top blocked devices	Most enforcement actions
Protocol split	v4 vs v6 ratio
Sankey diagram	Ingress → classification → disposition

Retained 365 days; week-over-week trend comparison from historical snapshots.

DASHBOARDS · 67+ WIDGETS

Dashboard	Widgets
Network Overview	12
DHCP Health	10
Security & Enforcement	9
Device Intelligence	8
Automation & Alarms	7
AI Analysis	6
Performance	8
Traffic Flow	7

Visualizations: Sankey, treemaps, bar / time-series / pie charts, gauges, KPI cards, sparklines, sortable tables. **Network Map:** built-in tile server with OpenStreetMap data — no external map service; device clustering, status filtering, density heatmaps, historical replay. **Per-user layouts** persist across sessions. **Custom report builder:** any metrics, filters and time ranges, IPv6 relay columns, CSV export.

08 Performance & Capacity

Reference figures measured on an **AMD Ryzen 7 8700G** (8 cores / 16 threads) with simulated DHCP traffic.

REFERENCE PLATFORM

Metric	Measured
Sustained throughput	10,000+ msg/s
Kernel enforcement latency	< 1 ms
DPI processing overhead	~0.06 ms / packet
CPU at 5,000 msg/s	50% of one core
Kernel set capacity	2.5 million entries

SIZING GUIDE

Tier	Devices	Rate	Cores	Storage (90d)
Standard	≤ 100K	~1K/s	2	50 GB
Large	≤ 1M	~5K/s	4	250 GB
Enterprise	≤ 10M	10K+/s	8	1 TB+

> Storage assumes ClickHouse columnar compression (10–15× typical). Kernel set entries = burst rate × expiration window — at 5,000 msg/s with 1-min expiry, ~300,000 entries.

09 AI Assistant Integration · MCP

Drive the platform from your AI tooling. A native Model Context Protocol server lets Claude Code — or any MCP client — query intelligence, triage alarms, and apply enforcement directly.

★ **A capability no other DHCP-security product in this category offers.** 40+ MCP tools, on-premises, with the same audit guarantees as the GUI and CLI.

READ BY DEFAULT, WRITES GATED

Read tools — traffic summaries, device lookups, alarm state, one-shot situation snapshots — need only **viewer** access. Write tools (block, throttle, allow, acknowledge) are gated behind an **operator** credential, and a **read-only launch mode** hides them entirely.

Every write requires an audit reason and a client-supplied idempotency key — retries are safe, and every action is attributable and audit-logged.

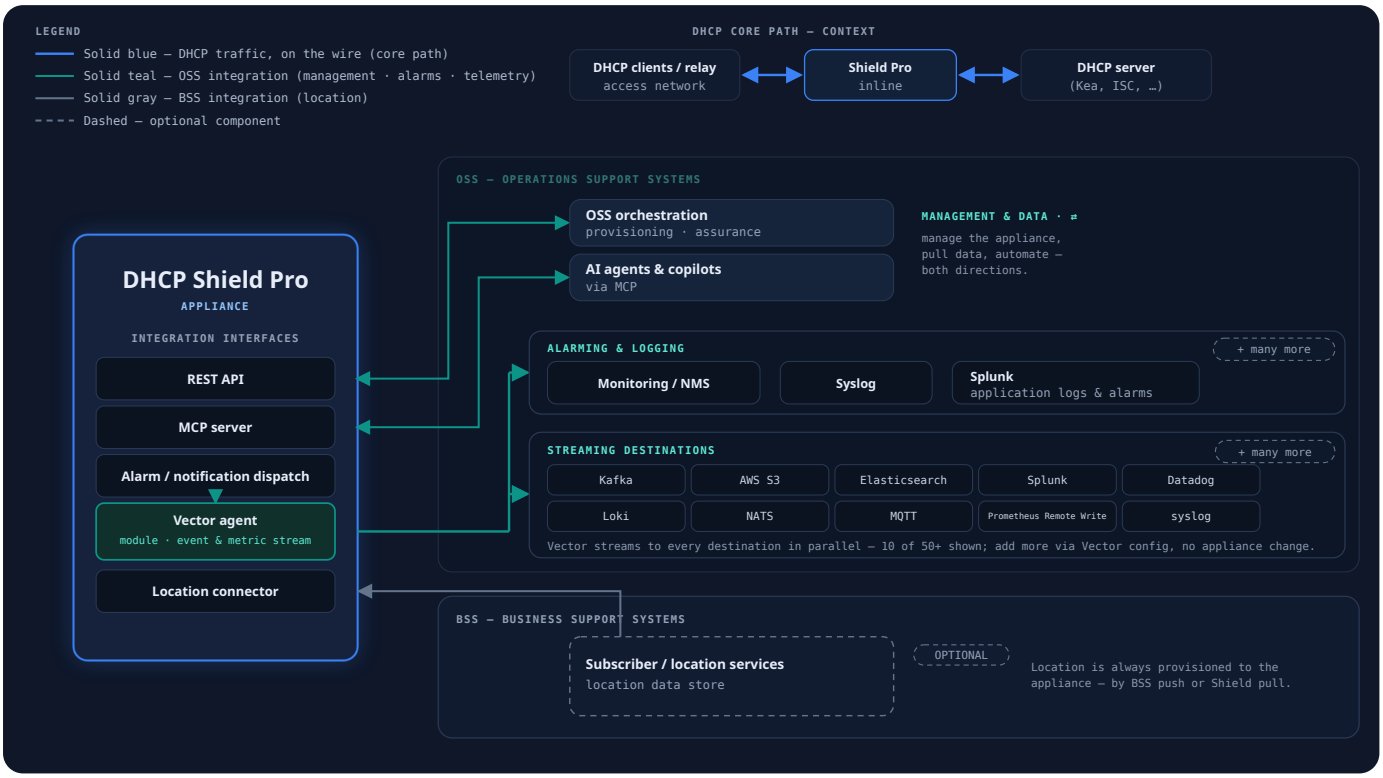
WHAT YOU CAN DO THROUGH IT

Category	Examples	Access
Traffic intelligence	Window summary, 24h snapshot, device lookup	`viewer`
Alarm triage	List firing, LLM summaries, recent actions	`viewer`
Enforcement	Block, throttle, allow; acknowledge alarm	`operator`

Runs inside your network — no cloud, no data leaving the perimeter. Reachable through the optional support session with your consent and a full audit trail, no standing access.

10 Integration & API

Built to slot into the stack you already run — scrape it, stream it, query it, script it.



How DHCP Shield Pro plugs into the operator's OSS / BSS ecosystem — management & data via REST and MCP, telemetry fanned out by the bundled Vector module, and location provisioned from BSS.

REST API `230+ endpoints`

Events, devices, actions, metrics, automation, config, users, sessions. Interactive OpenAPI reference served locally.

CLI · dpictl `230+ commands`

Every GUI function has a CLI equivalent — scripted ops, cron jobs, headless deployments.

Prometheus metrics

Token-authenticated scrape endpoint scoped to the metrics route. Liveness, alarm counts, storage/query health, queue depth — **no per-device data on the wire.**

Authentication & authorization

Authentication	JWT, API keys, OAuth2, MFA (TOTP)
Authorization	RBAC — Admin, Operator, Viewer
Network controls	IP-based access restrictions
Audit	All auth + admin actions logged

Data pipeline

Vector.dev	Stream to Kafka, Elasticsearch, Splunk, Datadog…
External LLM	OpenAI-compatible API for cloud analysis
ClickHouse	Direct SQL for custom analytics & BI

11 Deployment & Licensing

Linux-native, root-privileged, inline or mirrored (see **§02 Deployment Architectures**). Settings split between a YAML core and a runtime database layer.

REQUIREMENTS

Operating system	Linux, kernel 6.1+
Firewall subsystem	nftables (kernel enforcement)
Privileges	Root (nftables + NFQueue)
Network position	Inline, or mirrored via TZSP

LICENSE TIERS

Capability	Basic	Pro	Ent.
DHCPv4 inspection & enforcement	✓	✓	✓
Dashboards & reporting	✓	✓	✓

CONFIGURATION MODEL

Layer	Managed via	Change
Core settings	YAML file	Restart
Operational settings	Database (GUI/API)	Runtime

Database settings override YAML defaults — admins adjust thresholds, toggles and automation rules without touching files.

Capability	Basic	Pro	Ent.
REST API & CLI	✓	✓	✓
Traffic retention & export	✓	✓	✓
LLM-powered analysis	—	✓	✓
Automation engine	—	✓	✓
DHCPv6 support	—	—	✓
Managed device limit	100K	1M	∞

Offline-capable licensing. The appliance verifies a cryptographically signed license file locally with an embedded public key — **no call-home, no cloud check.** Runs fully disconnected, suitable for air-gapped and isolated networks.

Remote support (optional). An on-demand session opens a single outbound SSH backchannel to the vendor. Over that one channel an operator can share a chat thread, a read-only terminal screencast, the `dpictl` CLI, the MCP tool surface, and — only when you grant it — a root shell. Every action is audit-logged; the session is entirely operator-initiated, and closing it ends all access.

12 Specifications Summary

Protocols	DHCPv4 (RFC 2131), DHCPv6 (RFC 8415)
DHCP server compatibility	Any vendor, any implementation
Throughput	10,000+ msg/s sustained (lab-tested)
Enforcement latency	< 1 ms (kernel space)
DPI overhead	~0.06 ms / packet (application space)
Retention	90 days default, configurable
Dashboards	8 dashboards, 67+ widgets
API / CLI	230+ endpoints (interactive OpenAPI) · 230+ commands
AI assistant integration	MCP server, 40+ tools — read by default, writes gated
Metrics	Prometheus scrape endpoint, token-authenticated
Automation actions	Block, deny, throttle, allow, monitor, analyze
Max tracked devices	2.5M in kernel enforcement sets
Authentication	JWT, API keys, OAuth2, MFA (TOTP), RBAC
Licensing	Offline-capable, signed file verified locally — air-gap ready
Deployment	Linux 6.1+, nftables, root privileges