SMARTTILE · DEVICEAUTOMATE™ · PFSENSE / NETGATE

pfSense, watched from the inside

One REST API key on the firewall gives SmartTile the pfSense view a NOC needs — system health, WAN gateway latency and loss with failover history, interface bandwidth, VPN tunnels and on-demand config.xml backups — and an up/down check that still works when the firewall sits behind someone else's router.

SMARTTILE INTEGRATES WITH

pfSense CE 2.8.x and pfSense Plus (Netgate) through the free pfSense REST API package v2 (pfrest), authenticated with a static API key sent as `X-API-Key` over HTTPS.

HOW SMARTTILE AUTOMATES IT

Polls every enabled firewall on its own interval (120 s default), stores health, gateway and interface history, writes identity to the device record, and — for firewalls monitored through the API — marks the device DOWN after 3 failed polls, records the outage and opens the Rev.io ticket.

CATEGORY

Device
DeviceAutomate™

A pfSense firewall behind a customer's own router often will not answer ping, so a ping-only monitor either shows it **down for ever** or shows nothing but up/down. The pfSense REST API answers the questions a NOC actually asks — is the WAN gateway dropping packets, did it fail over, which tunnels are up, what changed in the config. SmartTile connects per company with that company's own key, polls it on a schedule, and puts the firewall on the same /devices pane as the rest of the network.

What the API turns on

Up/down that survives double NAT

Connect My Network pings the firewall once: if it answers, ping is the check; if not, the **API poll is the heartbeat**. Three failed polls in a row mark it DOWN; a good poll brings it back UP.

Outage → ticket, honestly counted

An API-monitored firewall going DOWN is written to state history (so Uptime and availability include it) and opens a Rev.io ticket when auto-ticketing is on for the device. Snoozes and per-device ticket delays are honoured.

WAN gateway SLA + failover

Every poll stores each gateway's latency, jitter (stddev) and loss, kept 35 days. A gateway changing status is recorded as a failover event, shown in the Analytics modal.

Interface bandwidth

Per-interface in/out byte and error counters are accrued each poll and turned into throughput graphs in the Bandwidth modal — WAN flagged — with 35 days of history.

Health at a glance

CPU, memory, swap, disk, temperature, mbuf and uptime; services that are enabled but stopped; DNS resolver state; DHCP leases; CARP / HA and maintenance mode.

VPN tunnels, live

The VPN button reads IPsec SAs (phase 2, subnets, bytes, IKE version), OpenVPN servers with connected sessions, and the WireGuard tunnel count, live from the firewall.

config.xml backups

Backup Now pulls the full config.xml, masks passwords, keys, PSKs and SNMP communities, and stores a version in the device's Config Backups list — only when it has changed.

Identity that fills itself

Vendor (Netgate), model, serial and pfSense version are written to the device record through the shared identity writer — blanks filled, a manual edit never overwritten.

What it takes on the firewall

1. **Install the REST API package** (one SSH command as root). pfSense CE 2.8.x: `pkg-static add …/pfSense-2.8.1-pkg-RESTAPI.pkg` ; pfSense Plus: the asset for your version from `github.com/pfrest/pfSense-pkg-RESTAPI/releases` .
2. **Create the key.** Web GUI → **System** → **REST API** → **Keys** → **+ Add**, as an admin user. Copy it — it is shown once.
3. **Let SmartTile in.** A WAN rule allowing SmartTile's address `157.245.117.9` to the web GUI port over HTTPS. Behind another router, port-forward that HTTPS port to the firewall. Ping is not required.
4. **Connect.** SmartTile → **Connect My Network** → pfSense card: address (e.g. `https://203.0.113.10:10443`), key, location, then **Connect firewall**. It tests the key, polls once and imports the device.

Admins can also add and edit firewalls under DeviceAutomate → pfSense Manager, with **Test** and **Poll now** per firewall.

CHOICE	WHAT HAPPENS
Automatic (recommended)	One ping probe: answers → ping monitoring; no answer → pfSense API monitoring. No false DOWN behind NAT.
Ping	Standard ICMP monitoring of the firewall address; the API still feeds graphs and health.
pfSense API	The API poll is the heartbeat: DOWN after 3 consecutive failed polls, UP on the next good one.
Self-signed certificate	Untick "trusted TLS certificate"; SmartTile then accepts the firewall's own cert. HTTPS is always required.

Exactly what SmartTile calls on the pfSense REST API v2

GET	`/api/v2/status/system`	CPU, memory, disk, temp, uptime, serial, platform
GET	`/api/v2/status/gateways`	gateway latency, stddev, loss, status
GET	`/api/v2/status/carp`	CARP / HA and maintenance mode
GET	`/api/v2/status/ipsec/sas`	IPsec tunnels and phase 2
GET	`/api/v2/vpn/wireguard/tunnels`	WireGuard tunnels (if the package is installed)
GET	`/api/v2/diagnostics/config_history/revisions`	last 10 config changes (Analytics)
POST	`/api/v2/diagnostics/command_prompt`	only `cat /cf/conf/config.xml`, only on Backup Now
GET	`/api/v2/system/version`	pfSense version (also the Test call)
GET	`/api/v2/status/interfaces`	interface state + byte/error counters
GET	`/api/v2/status/services`	services enabled but stopped, DNS resolver
GET	`/api/v2/status/openvpn/servers`	OpenVPN servers and sessions
GET	`/api/v2/status/dhcp_server/leases`	DHCP lease counts
GET	`/api/v2/system/restapi/version`	REST package version / update available

Security and control

Reads, with one exception

Every monitoring call is a GET. The only POST runs one fixed command — `cat /cf/conf/config.xml` — and only when someone presses Backup Now. SmartTile never changes a rule or setting.

The key stays in the vault

Encrypted at rest (AES-256-GCM) on save. The API returns only whether a key is set; the edit form shows dots, never the key. It travels only in the `X-API-Key` header over HTTPS.

Your company, your firewalls

Each company connects its own firewalls. Admins see and change only firewalls in their own company; the device's Uptime, Bandwidth, VPN and Backup routes check tenant ownership.

Secrets masked in backups

Passwords, hashes, pre-shared keys, private keys, API keys and SNMP communities are replaced with MASKED before the backup is hashed or stored.

Change summary and rollback

CHANGE	RISK	ROLLBACK
Install the pfSense REST API package	Low — adds an API to the web GUI; no traffic or policy change.	Remove the package.
Create one REST API key as an admin user	The key can call the API; SmartTile uses it for reads and the one backup command.	Delete the key under System → REST API → Keys; access ends at once.
WAN rule for 157.245.117.9 to the GUI port (and a port-forward if behind NAT)	Low — one source address to the existing GUI port.	Remove the rule / forward.

Common objections

OBJECTION	ANSWER
"Our firewall does not answer ping."	It does not need to. Automatic mode detects that and monitors through the API — the reason this flow exists.
"Will you change our configuration?"	No. Monitoring is reads only; the backup command only reads config.xml, and only when a person presses Backup Now.
"Does a blip page us?"	No. The firewall turns DOWN only after 3 consecutive failed polls, and a restart of SmartTile never fires a false DOWN on its first poll.
"We use a self-signed certificate."	Fine — untick the trusted-certificate box. The connection is still HTTPS.

One key on the firewall — and your pfSense tells the NOC what ping never could.