ClearPath MSP
ClearWatch

SOLUTION BRIEF

from ClearPath MSP

CLEARWATCH SOLUTION BRIEF · CHECK POINT QUANTUM SPARK

Quantum Spark monitoring, from the cluster to the circuit.

How ClearWatch reads Check Point Quantum Spark appliances, what it checks, and what that means for the people who run them.

PUBLISHED NOVEMBER 2026 LENGTH 6 PAGES APPLIES TO QUANTUM SPARK, R81.10 AND R82

EXECUTIVE SUMMARY

Firewall monitoring that sees what the firewall sees

A firewall is the one device every site depends on, and the one generic monitoring understands least. A ping says it is on. It does not say whether the standby member could take over, which internet circuit is carrying traffic, whether a VPN tunnel dropped overnight, or when a license runs out.

ClearWatch reads Check Point Quantum Spark appliances over SSH from inside the client's network, using a fixed list of read-only commands. Every cluster member is polled on its own address every 15 minutes, with its circuits, cluster state and VPN re-read every 3 minutes. Its readings become 23 built-in checks, the appliance's own backup is taken every night, and it appears on the same dashboards, maps and reports as every other device.

KEY TAKEAWAYS

- **Both cluster members are watched,** so a failed standby or a split brain is caught before a failover needs it.
- **Every circuit's real link state** is read, not only the one SD-WAN has chosen.
- **Read only, from inside the network:** nothing is installed on the firewall or opened to the internet.
- **One console for every client:** checks, nightly backups, a map and a report across all of them.

IN THIS BRIEF

01 **The challenge** — What generic monitoring misses on a firewall — 2

02 **How ClearWatch connects** — SSH from a ClearBridge, two clocks, adding a firewall — 2

03 **What ClearWatch reads** — Internet connections, VPN and hardware — 4

04 **Across every client** — Dashboard, network map and nightly backup — 5

05 **Checks and alerts** — 23 checks, their defaults and the report — 6

06 **Security and access** — The console, credentials and limits — 6

WHO THIS IS FOR

MSPs and IT teams responsible for Check Point Quantum Spark firewalls, alone or in clusters, at one site or across many clients.

AT A GLANCE

CHECKS
23 built in
Cluster, WAN, VPN, capacity, hardware, license and upkeep.

CLUSTERS
Both members
Each member polled on its own address.

POLLING
Every 15 minutes
Circuits, cluster and VPN every 3 minutes.

BACKUP
Every night
The appliance's own backup, 14 kept.

01 THE CHALLENGE

A firewall that answers a ping can still be failing

Most monitoring treats a firewall like any other box on the network: ping it, read a few SNMP values, alert when it stops answering. On a Check Point Quantum Spark appliance that leaves the questions that matter unanswered. Check Point's own Monitoring Blade is not available on Quantum Spark, and the values a generic tool can reach do not always mean what they appear to.

THE QUESTION	PING AND GENERIC SNMP	CLEARWATCH
Could the standby take over?	A cluster can report both members as active	Reads **both members** on their own addresses every 3 minutes and flags a split brain
Is the backup circuit healthy?	A healthy standby circuit reads as not active	Reads each circuit's **real link state**: Up, standby
Are the VPN tunnels up?	Not visible	Tunnels and peers re-read **every 3 minutes**
Is anything about to expire?	Not visible	License expiry warned at **30 days**, failed at 7
Is the configuration safe?	A manual export, if someone remembers	The appliance's own backup **every night**, 14 kept

Why "active" is not "up"

A Check Point's own **is-active** flag says which circuit SD-WAN has chosen to use, so a healthy backup circuit always reads false. ClearWatch reads each circuit's real link from the interfaces instead, which is why a standby line shows as **Up, standby** and not as down.

02 HOW CLEARWATCH CONNECTS

Read over SSH, from inside your network

A ClearBridge (the ClearWatch agent on a machine at the site) opens an SSH session to each cluster member and runs a fixed list of read-only commands. Nothing on the firewall is opened to the internet, and nothing is installed on it.

YOUR NETWORK
Check Point appliance
Each cluster member is read on its own address, never the cluster's virtual address.

→

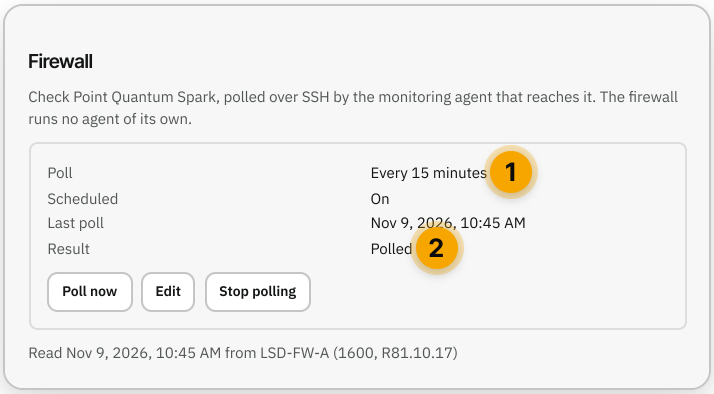
YOUR NETWORK
ClearBridge
Checks the appliance's SSH host key and refuses any command that is not on the list.

→

CLEARWATCH
Readings, checks, alerts
Turns about 17 commands per poll into the Firewall tab, checks and alerts.

Two clocks

A whole poll runs every 15 minutes by default (1), or at any interval from 5 minutes to a day. Between them, a fast poll re-reads the internet connections, cluster state and VPN every 3 minutes on both members, so a dead circuit, a failover or a dropped tunnel is seen within minutes. The Firewall tab says when each member was last read and what it answered (2).



02 HOW CLEARWATCH CONNECTS, CONTINUED

An address and an SSH login. ClearWatch does the rest.

Give ClearWatch the address of one member and an SSH login, and choose the ClearBridge that can reach it. There is no vendor to pick: the appliance is asked what it is, and nothing is created until it answers as a Check Point.

A live panel ticks off each step as the appliance answers 1. Every command in the session is a read 2. SNMP is set up along the way, with the community moved into ClearWatch's credential vault, and the other member is looked for and added only when the two name each other 3.

What you provide

- ✓ The address of one cluster member.
- ✓ An SSH login for the appliance, stored sealed in the vault.
- ✓ The ClearBridge allowed as an administrator on the appliance.

What it never does

- ✗ Push policy, change trust or restart a service.
- ✗ Run a command outside its fixed list.
- ✗ Create anything from an address that did not identify.

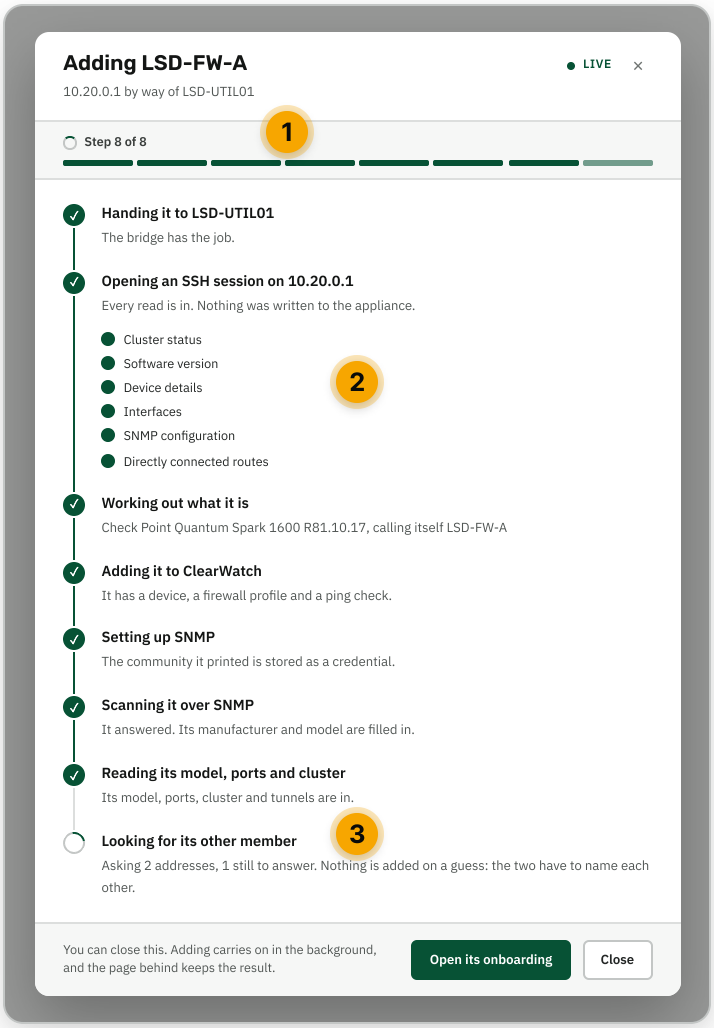


FIGURE 1 The live onboarding panel for LSD-FW-A, rebuilt from the ClearWatch console with demo data.



FIGURE 2 A 1600's front on the Ports tab. The artwork is simplified.

Its own front panel

The appliance fills in its make, model, serial and firmware, and the model and firmware stay current after an upgrade. On the Ports tab a 1600 or 1800 is drawn as its front: LAN with even numbers on top, LAN2 printed 2/Sync, DMZ over WAN. Internal links and tunnels sit as chips under the box, so no port is hidden.

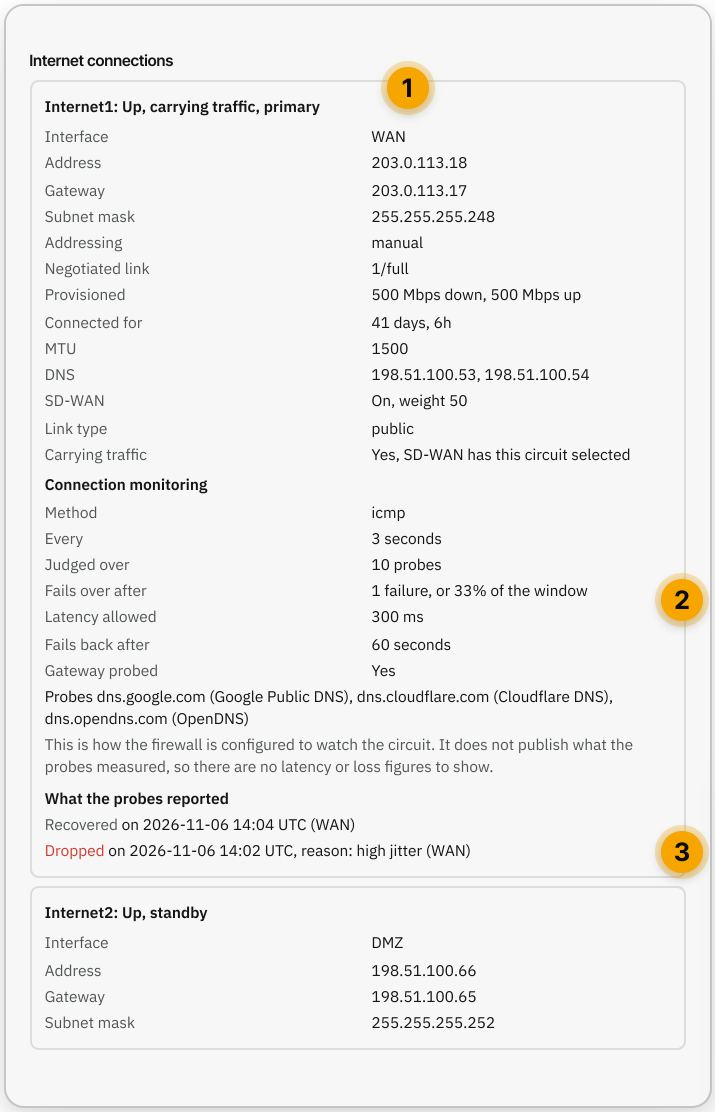
Requirements

- A Check Point Quantum Spark appliance on R81.10 or R82, standalone or in a cluster.
- A ClearBridge at the site that can reach each member over SSH.
- An SSH login on the appliance, and the ClearBridge on its list of allowed administrators.
- Each member's own address. The cluster's virtual address is never used.

03 WHAT CLEARWATCH READS

Every circuit, tunnel and sensor, in the appliance's own words

Each figure on a firewall's Firewall tab is what the appliance reported, beside the range it declares for itself. Where the appliance publishes nothing, the page says so instead of guessing.



Internet connections

Internet1: Up, carrying traffic, primary (1)

Interface	WAN
Address	203.0.113.18
Gateway	203.0.113.17
Subnet mask	255.255.255.248
Addressing	manual
Negotiated link	1/full
Provisioned	500 Mbps down, 500 Mbps up
Connected for	41 days, 6h
MTU	1500
DNS	198.51.100.53, 198.51.100.54
SD-WAN	On, weight 50
Link type	public
Carrying traffic	Yes, SD-WAN has this circuit selected

Connection monitoring (2)

Method	icmp
Every	3 seconds
Judged over	10 probes
Fails over after	1 failure, or 33% of the window
Latency allowed	300 ms
Fails back after	60 seconds
Gateway probed	Yes

Probes dns.google.com (Google Public DNS), dns.cloudflare.com (Cloudflare DNS), dns.opendns.com (OpenDNS)

This is how the firewall is configured to watch the circuit. It does not publish what the probes measured, so there are no latency or loss figures to show.

What the probes reported (3)

Recovered on 2026-11-06 14:04 UTC (WAN)
Dropped on 2026-11-06 14:02 UTC, reason: high jitter (WAN)

Internet2: Up, standby

Interface	DMZ
Address	198.51.100.66
Gateway	198.51.100.65
Subnet mask	255.255.255.252

FIGURE 3 Internet connections on the Firewall tab.

Cluster and capacity

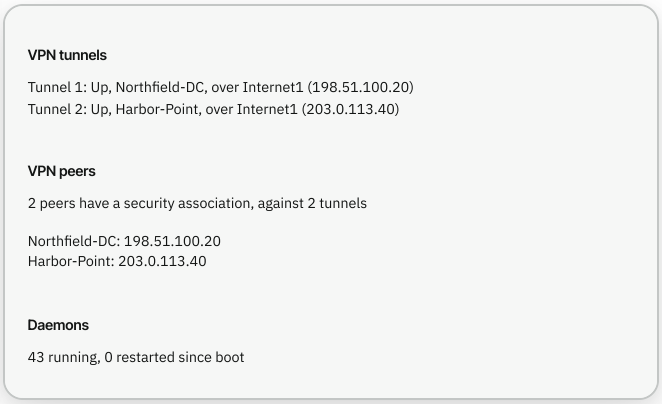
Each member's role and state, its peer, memory and connections against the appliance's own watermarks, and the installed policy with its install time.

Internet connections

Each circuit gets a card with its real link state and whether it is carrying traffic (1), with its addressing, provisioned speed, uptime and SD-WAN role. The card shows how the appliance itself watches the circuit (2), and every drop and recovery it logged, with its own reason (3). A spare circuit set aside on the Ports tab reads Not in use and is not counted as down.

VPN

Route-based tunnels show up or down with the peer and the circuit they ride. R82 prints no tunnel state, so there a tunnel is up while its peer holds a security association, and the tab says so. Domain-based VPNs are counted by the peers holding one.



VPN tunnels

Tunnel 1: Up, Northfield-DC, over Internet1 (198.51.100.20)
Tunnel 2: Up, Harbor-Point, over Internet1 (203.0.113.40)

VPN peers

2 peers have a security association, against 2 tunnels

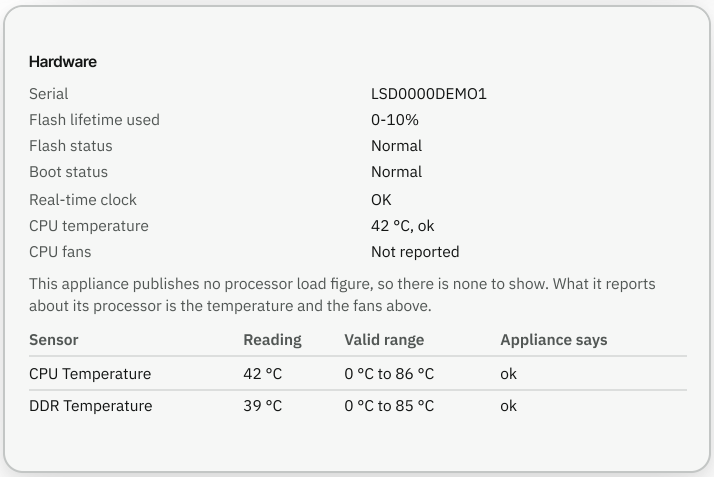
Northfield-DC: 198.51.100.20
Harbor-Point: 203.0.113.40

Daemons

43 running, 0 restarted since boot

Hardware

Flash wear, boot status, the real-time clock and every sensor the appliance reports, each checked against the valid range the appliance declares for itself. The appliance publishes no processor load figure, and the tab says so rather than inventing one.



Hardware

Serial	LSD0000DEMO1
Flash lifetime used	0-10%
Flash status	Normal
Boot status	Normal
Real-time clock	OK
CPU temperature	42 °C, ok
CPU fans	Not reported

This appliance publishes no processor load figure, so there is none to show. What it reports about its processor is the temperature and the fans above.

Sensor	Reading	Valid range	Appliance says
CPU Temperature	42 °C	0 °C to 86 °C	ok
DDR Temperature	39 °C	0 °C to 85 °C	ok

04 ACROSS EVERY CLIENT

Every firewall on one globe, every cluster on the map

The same poll feeds the Firewalls dashboard, the topology map and the nightly backup, so a firewall added once shows up everywhere it matters.

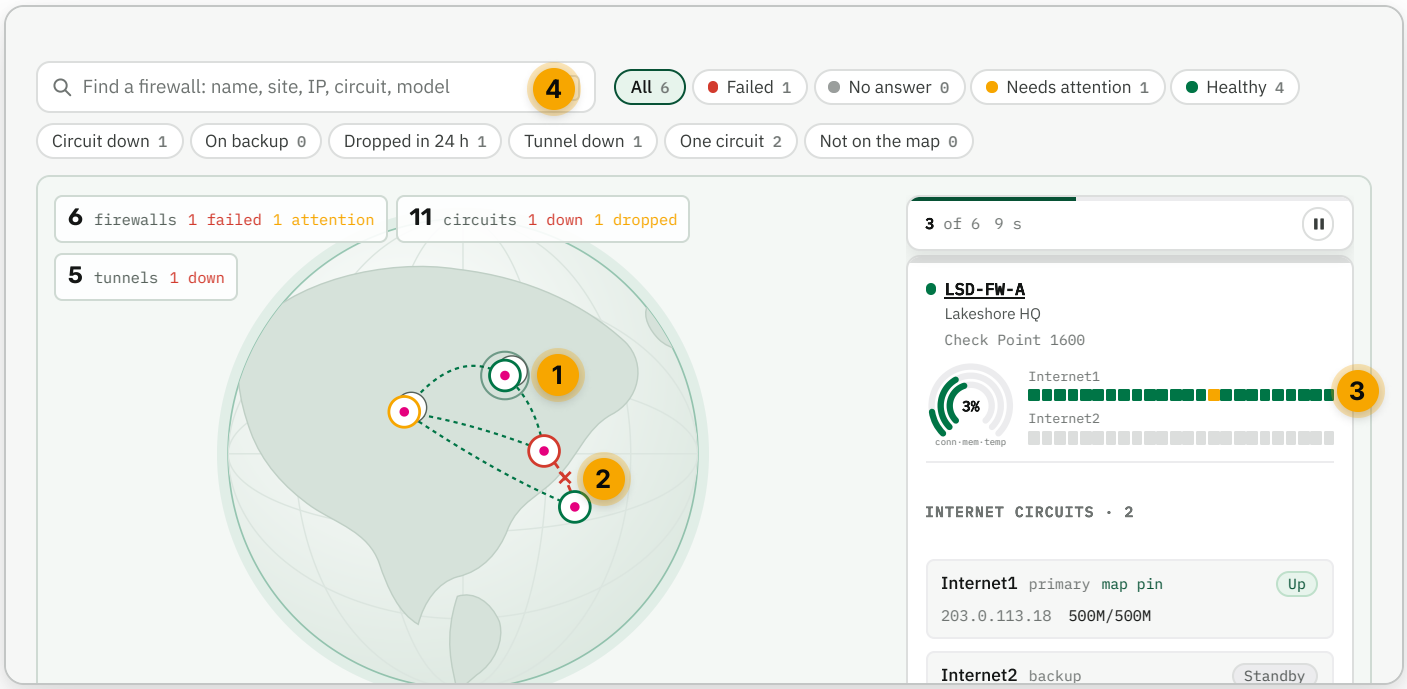
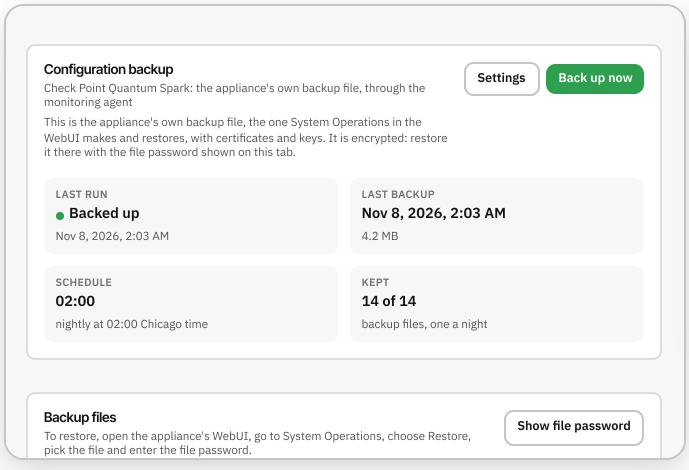


FIGURE 4 The Firewalls dashboard across three clients. The globe is simplified.

Each firewall is placed by where the public address of its active circuit registers, or by the circuit you choose for the map (1), with site-to-site tunnels drawn between monitored firewalls, red and dashed when down (2). A card tours every firewall worst first, with a strip per circuit for the last 24 hours (3). Search by name, site, address, circuit or model, or filter by status and by what is wrong (4); a tile per firewall below the globe lists every check with its reading.

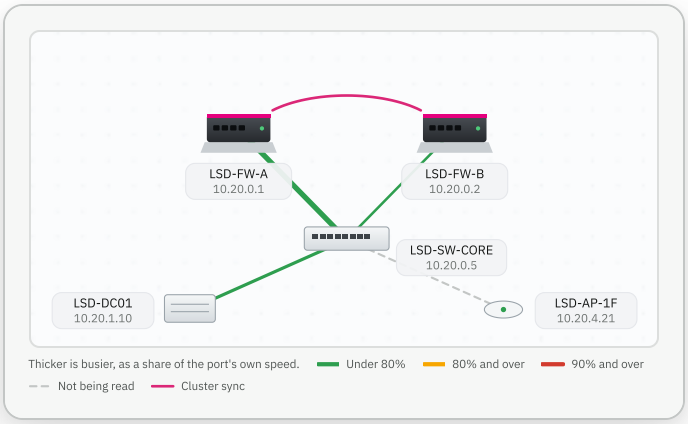
Nightly configuration backup

Set up for both members after their first poll. Each night at 2:00 the appliance writes its own encrypted backup and ClearWatch keeps the last 14, with **Back up now** on demand. Each file's password is shown only on request, and that is logged.



On the network map

Both members appear on the topology map as their own devices, joined by their cluster sync link, with the switches and devices cabled to them.



05 CHECKS AND ALERTS

23 checks for every Check Point

Levels read **warning / failed**, each a default you can change for everyone or one firewall. Each alert lands in its own lane, so an outage is never filed beside a license reminder.

AREA	CHECKS	DEFAULT LEVELS
Cluster and availability	Cluster member state, cluster split brain, firewall polling	Member down or split: failed · no poll for 1 / 4 hours
Internet and VPN	WAN connections down, no internet connection carrying, internet connection dropped, VPN tunnels down, VPN peers established	WAN down 1 / 2 · drops 1 / 3 a day · tunnels 1 / 3 · peers set per site
Capacity	Firewall memory, connection capacity, peak connection capacity, memory allocation failures, firewall disk	Memory 80 / 92% · connections 70 / 85% · disk 80 / 90%
Hardware	Hardware sensors, flash wear, boot status, real-time clock	Sensors out of range 1 / 2 · flash, boot, clock: failed
Security and upkeep	Security policy installed, license expiry, daemons not running, daemons restarted, commands refused, WANs not monitored	License 30 / 7 days · daemons 1 / 2, restarts 1 / 3

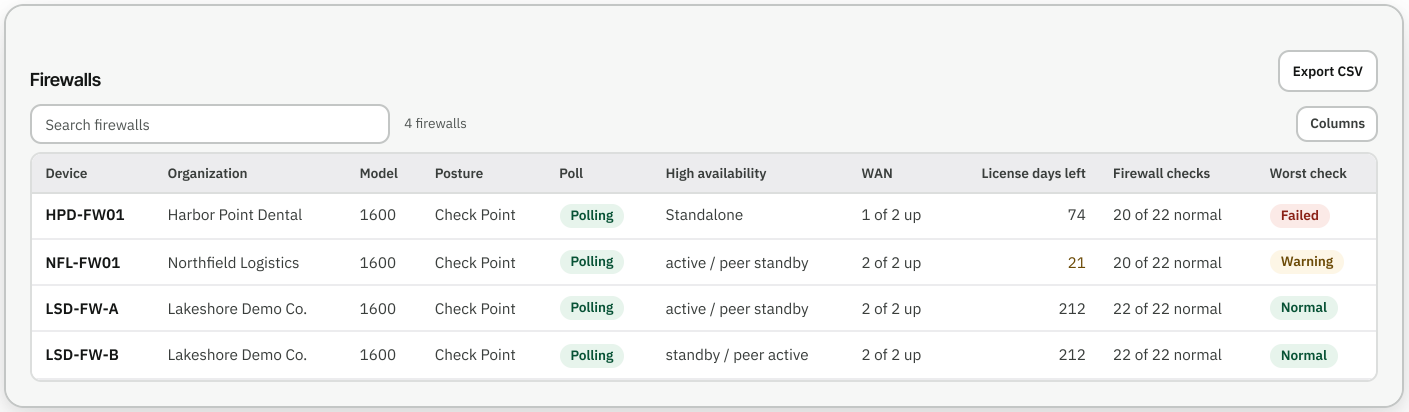


FIGURE 5 The Firewall status report: posture, high availability, license days left and the worst check, across every client.

06 SECURITY AND ACCESS

A console, no password typed

When an engineer needs the command line, they open SSH to the appliance from its device page, relayed by the ClearBridge. The login is supplied from the vault, so nobody types or sees it.

Every session is audited, capped at three per firewall and closed after 15 idle minutes, and can be recorded. Opening one needs its own permission, which nobody holds by default.

Good to know

- ClearWatch reads only; the backup asks the appliance to write its own file.
- Logins and SNMP communities are sealed in the vault and handed only to the ClearBridge that needs them.
- The appliance publishes no processor load figure, so there is no CPU check, and no per-interface throughput, latency or loss.
- The backup is an encrypted archive, so one night is not compared with the next.

Bring your Quantum Spark firewalls into view.

Start a free trial, or ask us to onboard your first cluster with you.

clearwatch.com

ClearWatch™ is a trademark of ClearPath MSP. Check Point and Quantum Spark are trademarks of Check Point Software Technologies. Screens show demo data.