

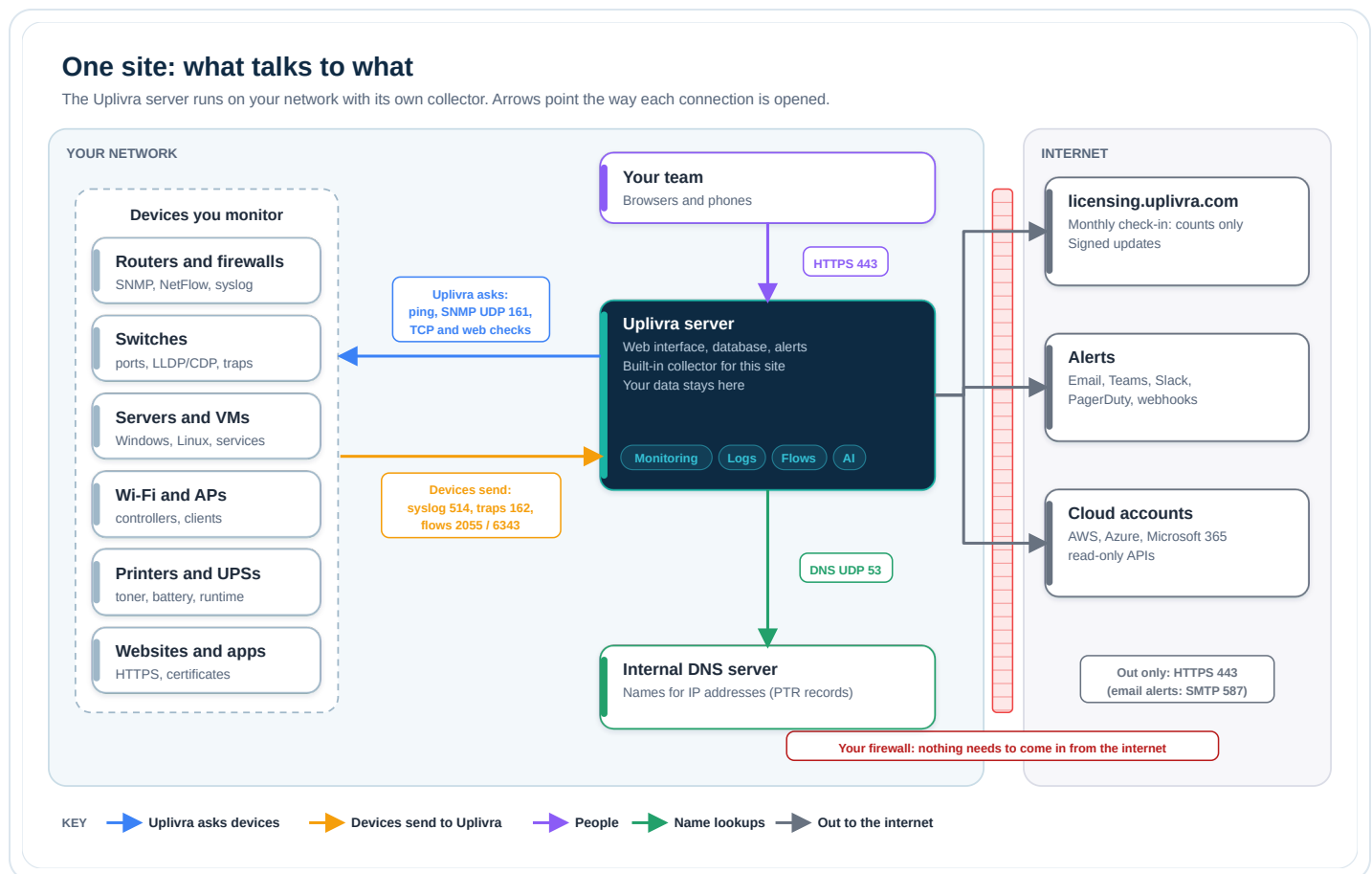
Uplivra architecture

Every traffic path, port and direction. Arrows point the way each connection is opened. The SVG files are in the diagrams folder for slides and proposals.

In short: collectors only connect **out** on HTTPS 443. Devices send logs, traps and flows to a collector on your network. The server's only internet connections are out: monthly license check-in (counts only), alerts you turn on, and cloud APIs you connect.

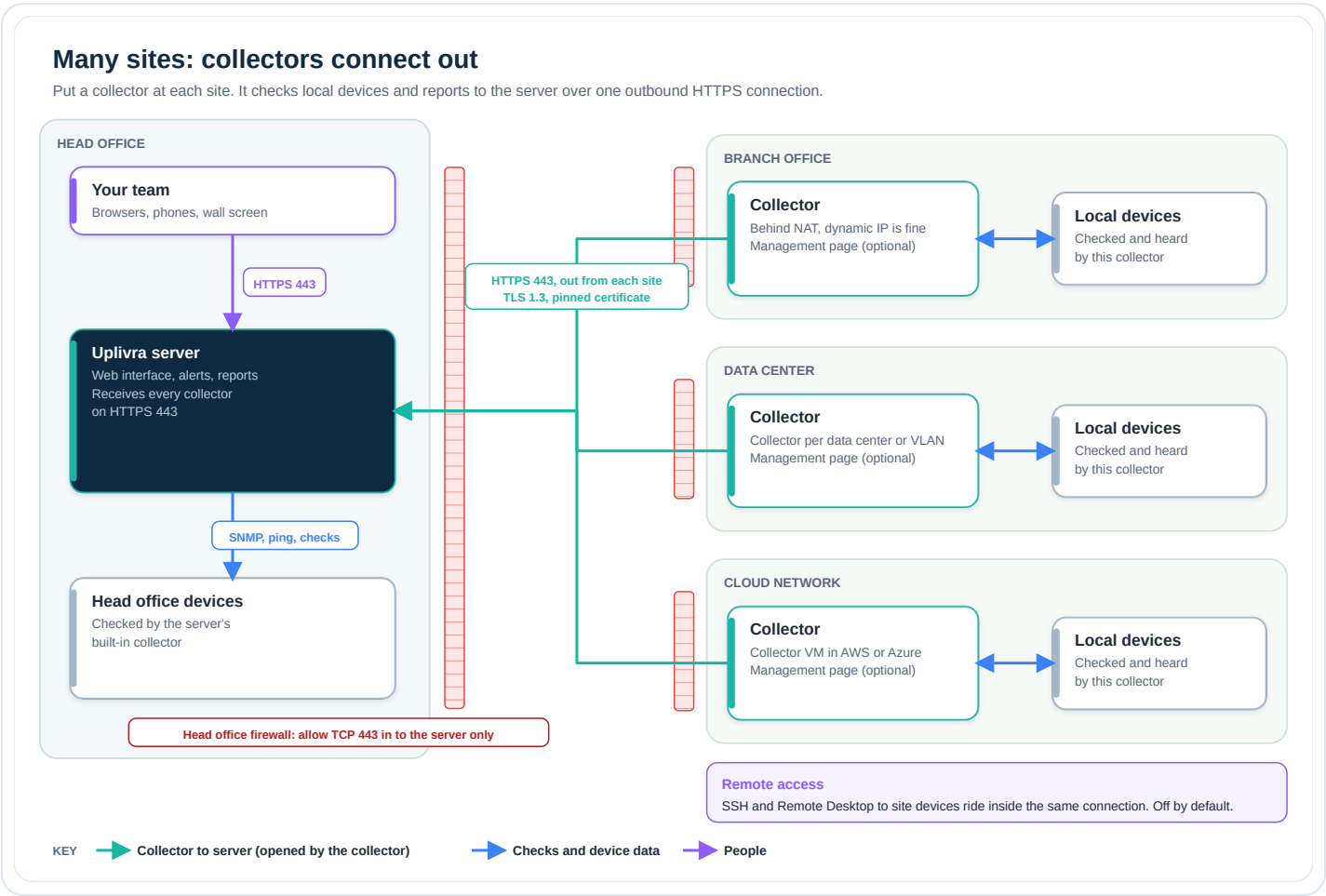
One site: what talks to what

The Uplivra server (with its built-in collector) on your network: what it asks devices, what devices send it, and the few connections it makes out to the internet.



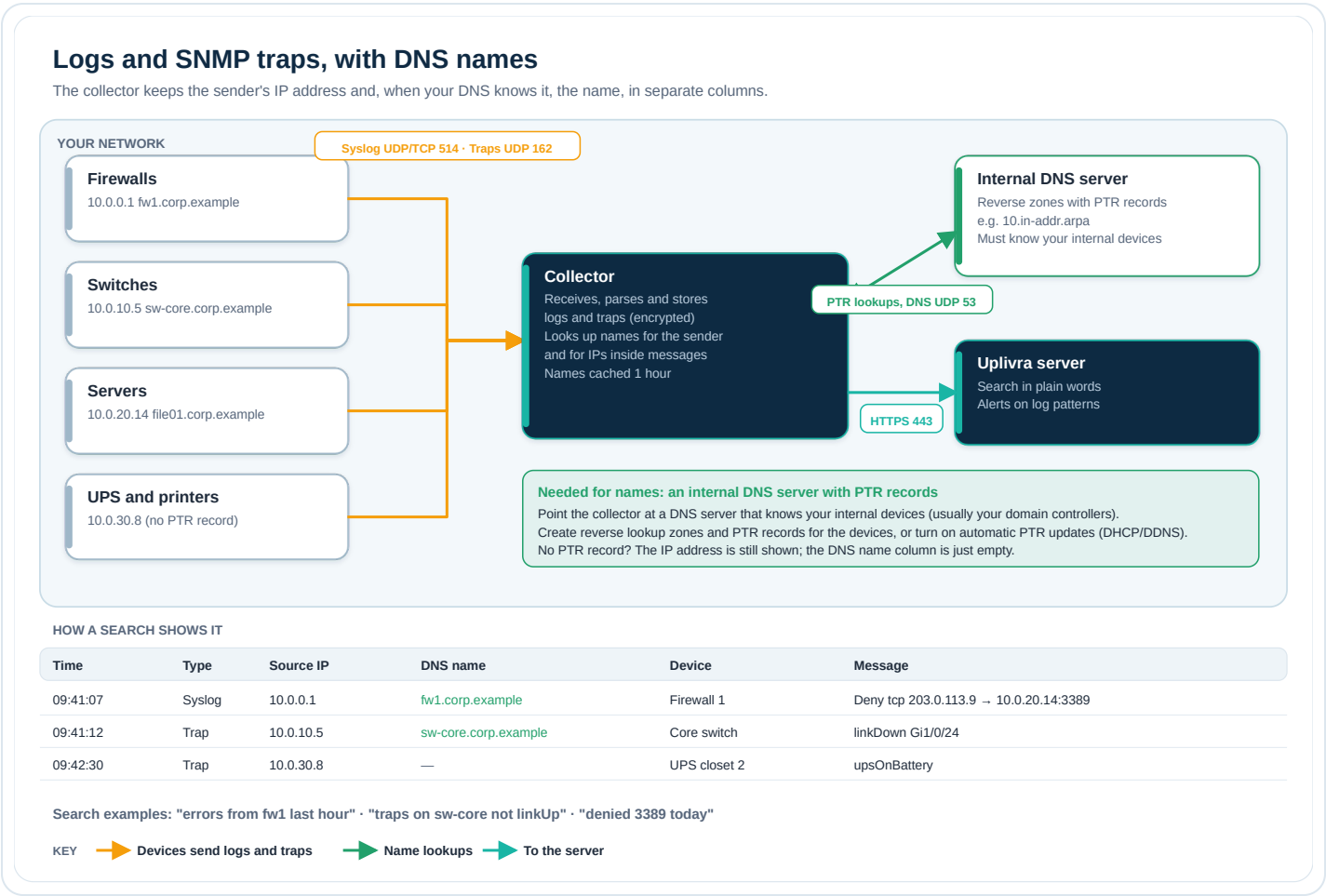
Many sites: collectors connect out

Collectors at branches, data centers and cloud networks connect out to the server on HTTPS 443. Nothing connects in to a branch.



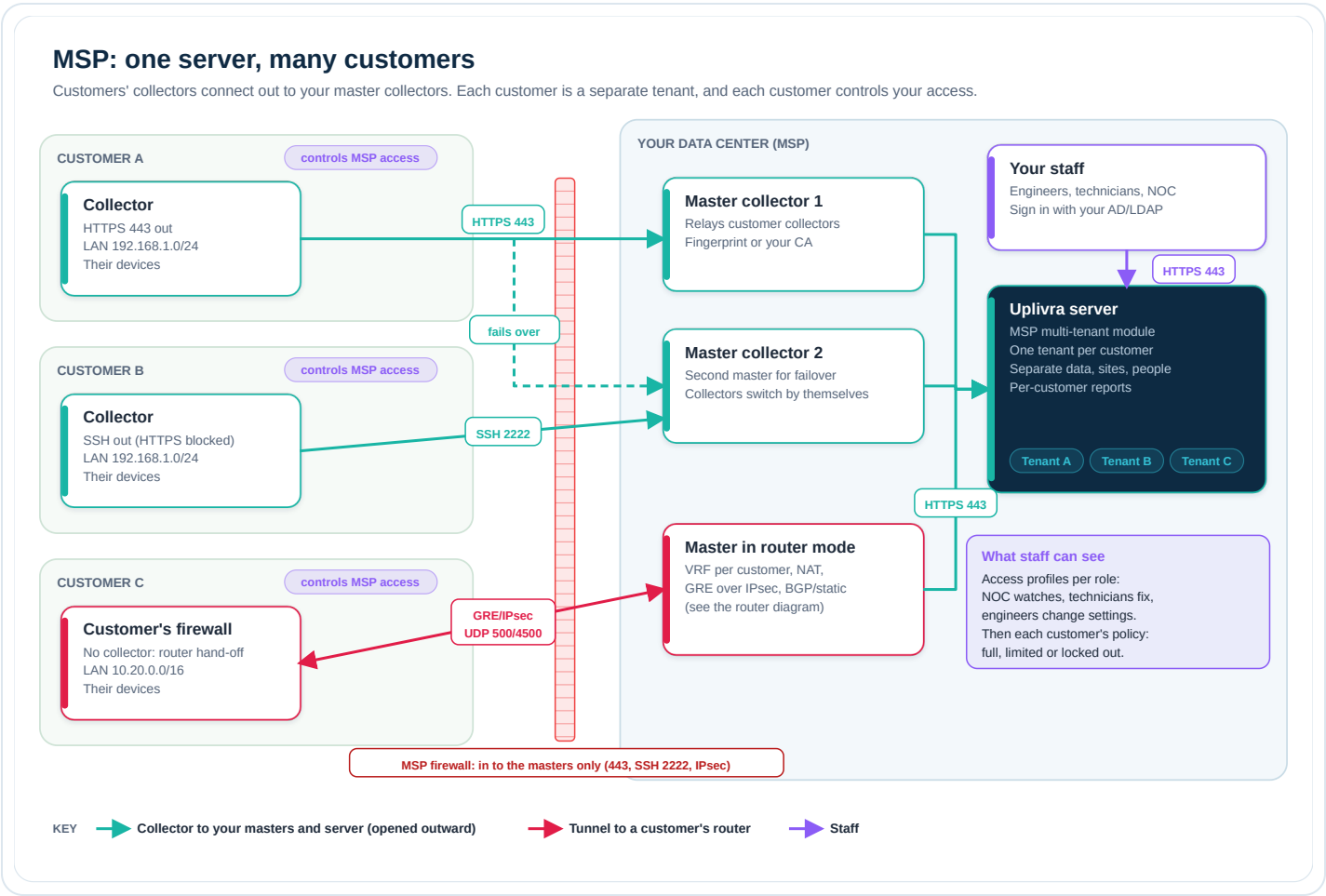
Logs and SNMP traps, with DNS names

Devices send syslog and traps to a collector, which looks up names in your internal DNS and keeps both the IP and the name.



MSP: one server, many customers

A multi-tenant server and master collectors in the MSP's data center. Customers connect out; staff see only what their role and each customer allow.



HTTPS 443

fails over

SSH 2222

GRE/IPsec

UDP 500/4500

HTTPS 443

MSP firewall: in to the masters only (443, SSH 2222, IPsec)

KEY

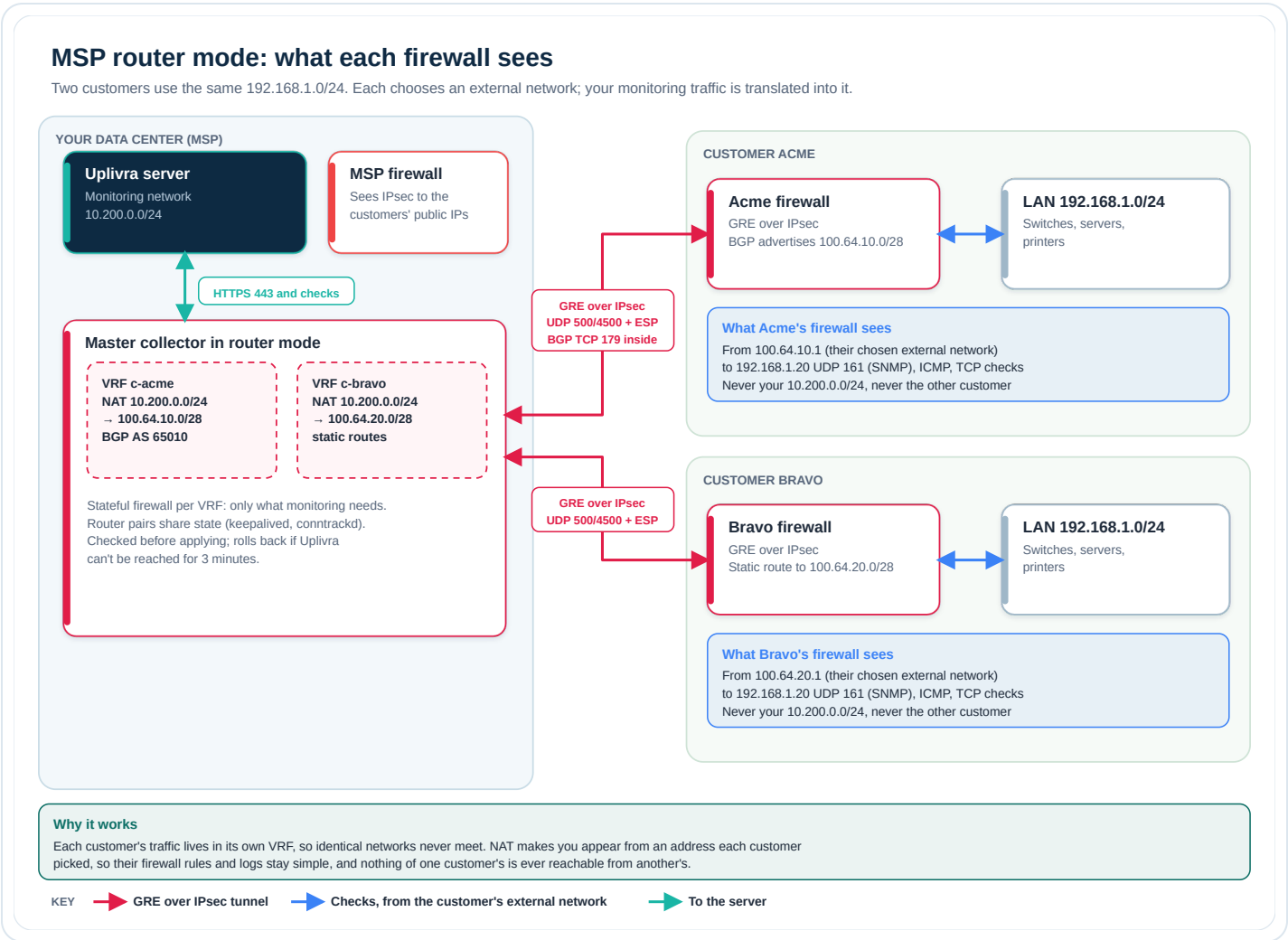
Collector to your masters and server (opened outward)

Tunnel to a customer's router

Staff

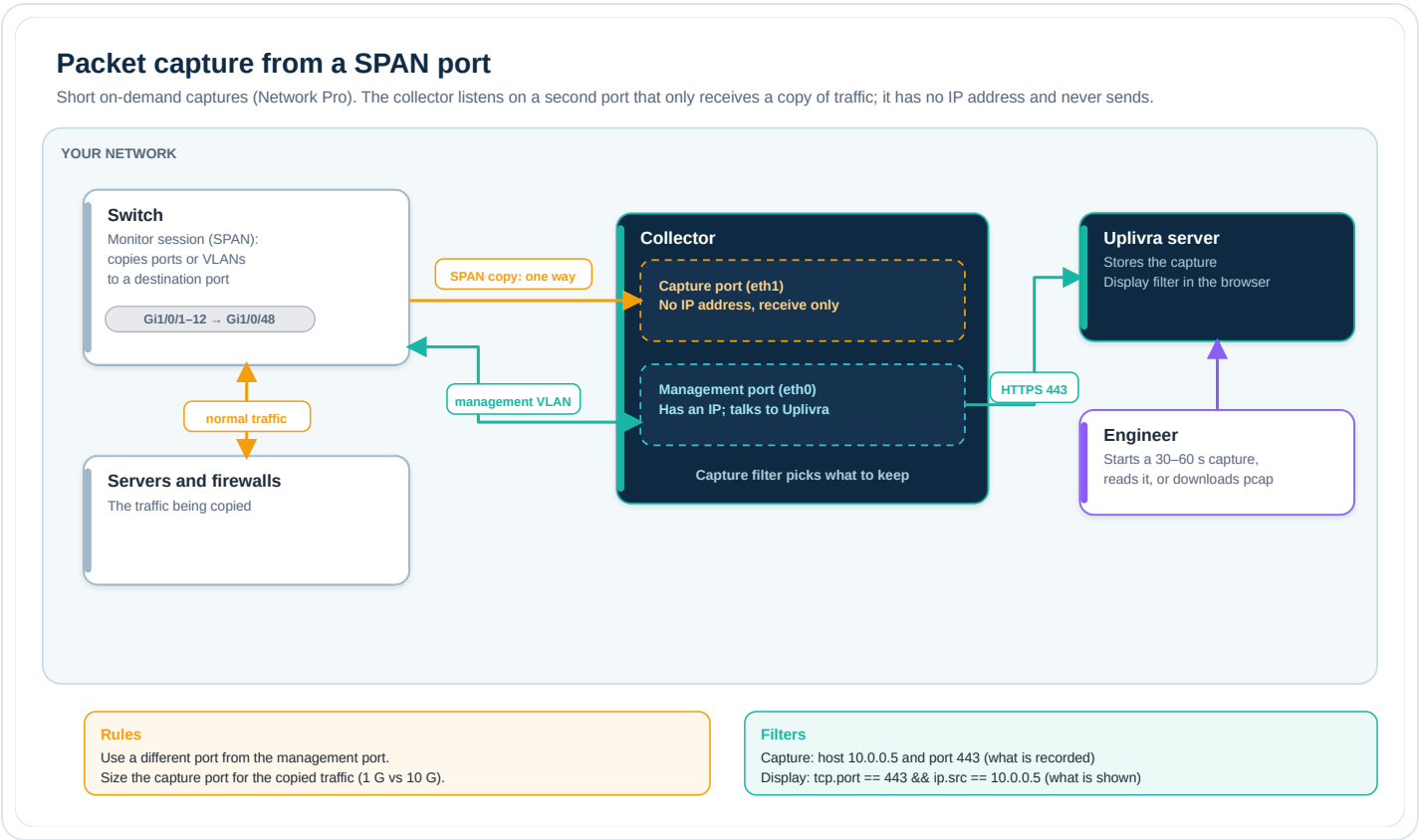
MSP router mode: what each firewall sees

Per-customer VRFs, GRE over IPsec, BGP or static routes, and NAT into an external network each customer chooses, so overlapping networks just work.



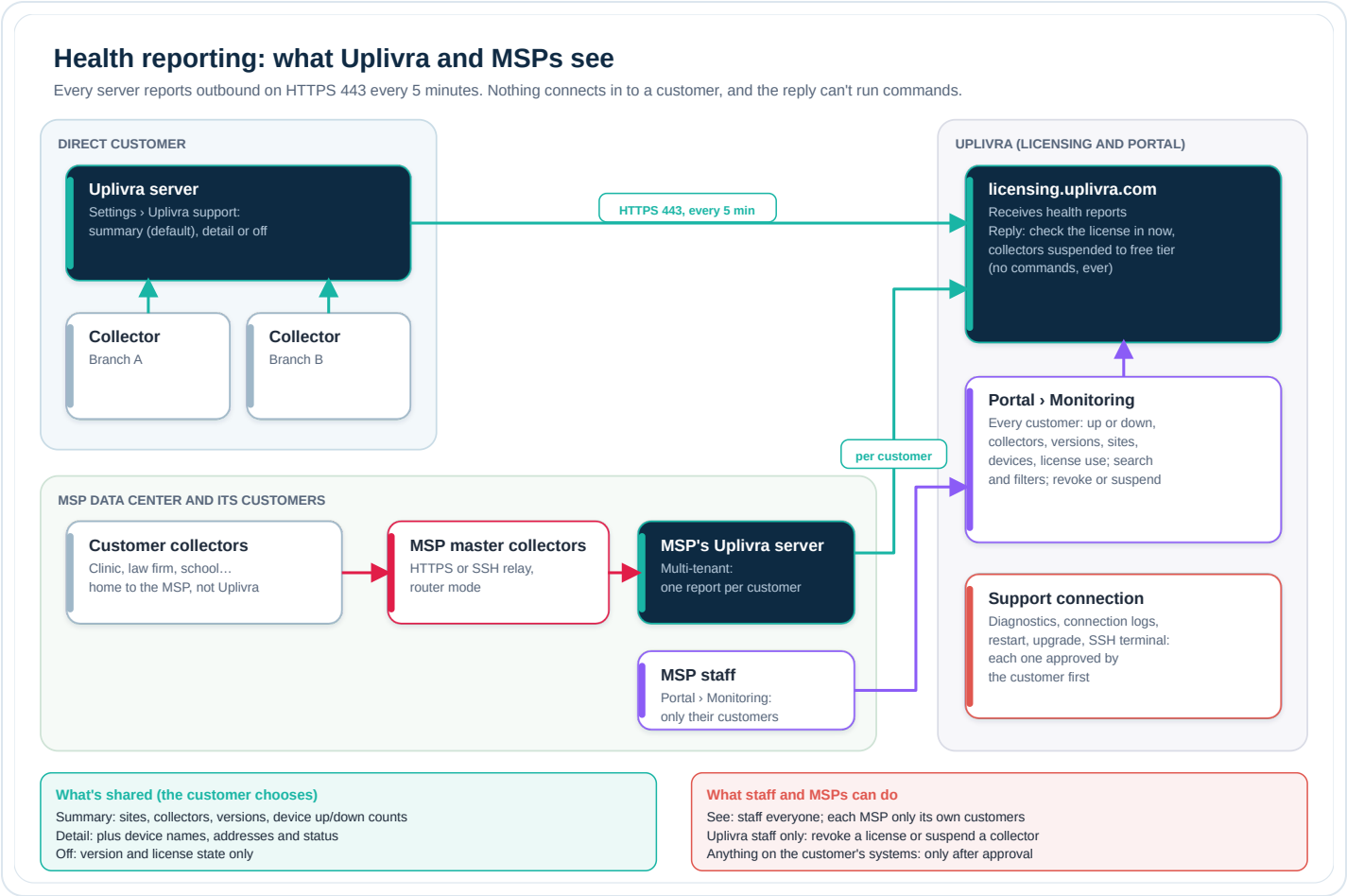
Packet capture from a SPAN port

A collector records mirrored traffic on a second network port with no address, separate from its management port, and uploads the capture over HTTPS.



Health reporting: what Uplivra and MSPs see

Every customer's server reports its health to the Uplivra portal every 5 minutes, outbound on HTTPS. MSP customers home to the MSP's data center, and the MSP's server reports each customer. Staff see everyone; each MSP sees only its own customers. Actions still need the customer's approval.



Packet capture collector: record all the time, pull any moment

A dedicated collector records one or more SPAN ports around the clock into encrypted storage. Your Uplivra server licenses it, and pulls the minutes you ask for, or the minutes before an alert.

