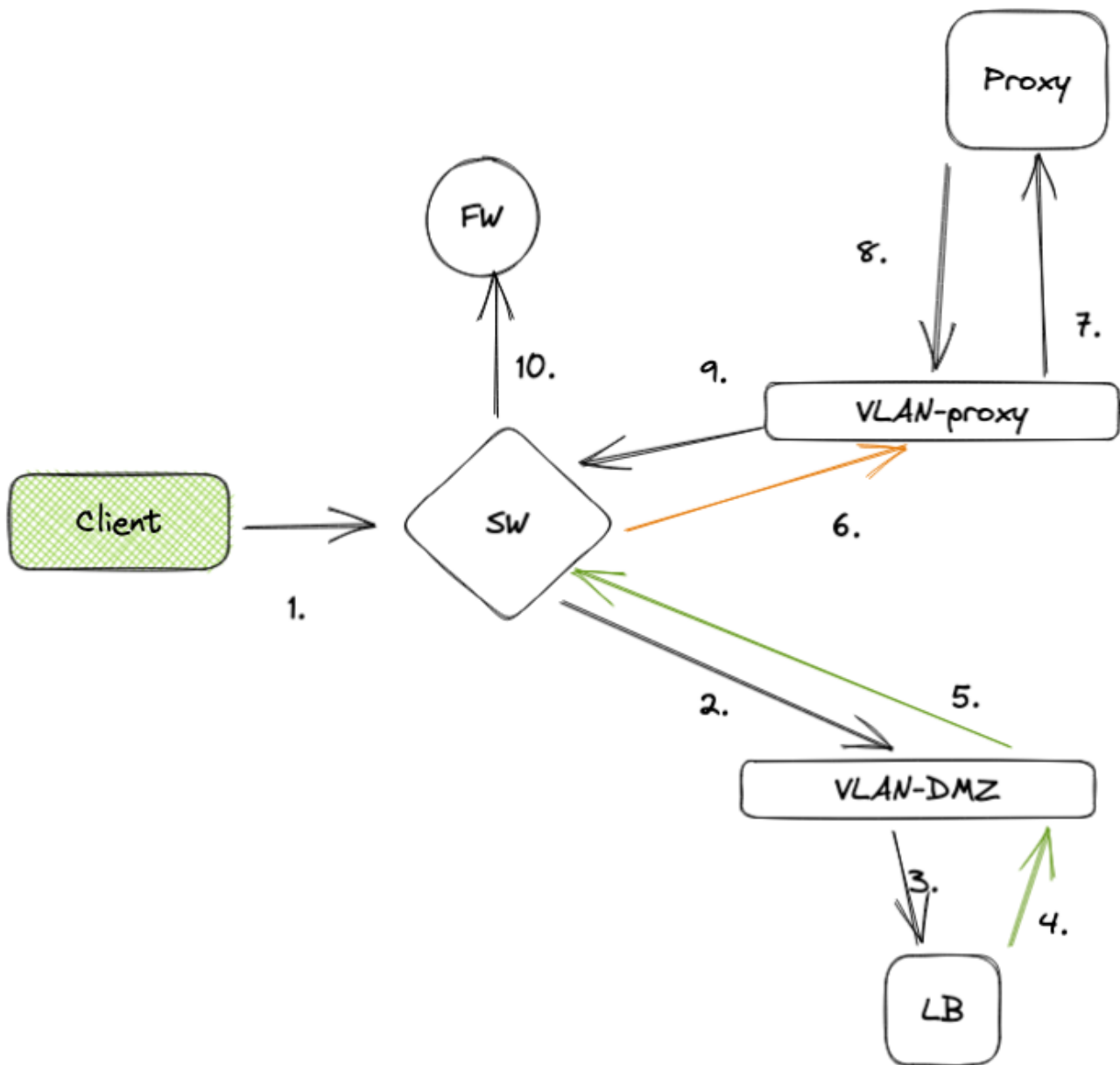


A10 outbound decryption using I3 path

Why an alternative L3 path

Client had this set of "explicit" proxies server behind a load balancer [purple one], and a pac file to point this LB whenever an access is needed to internet

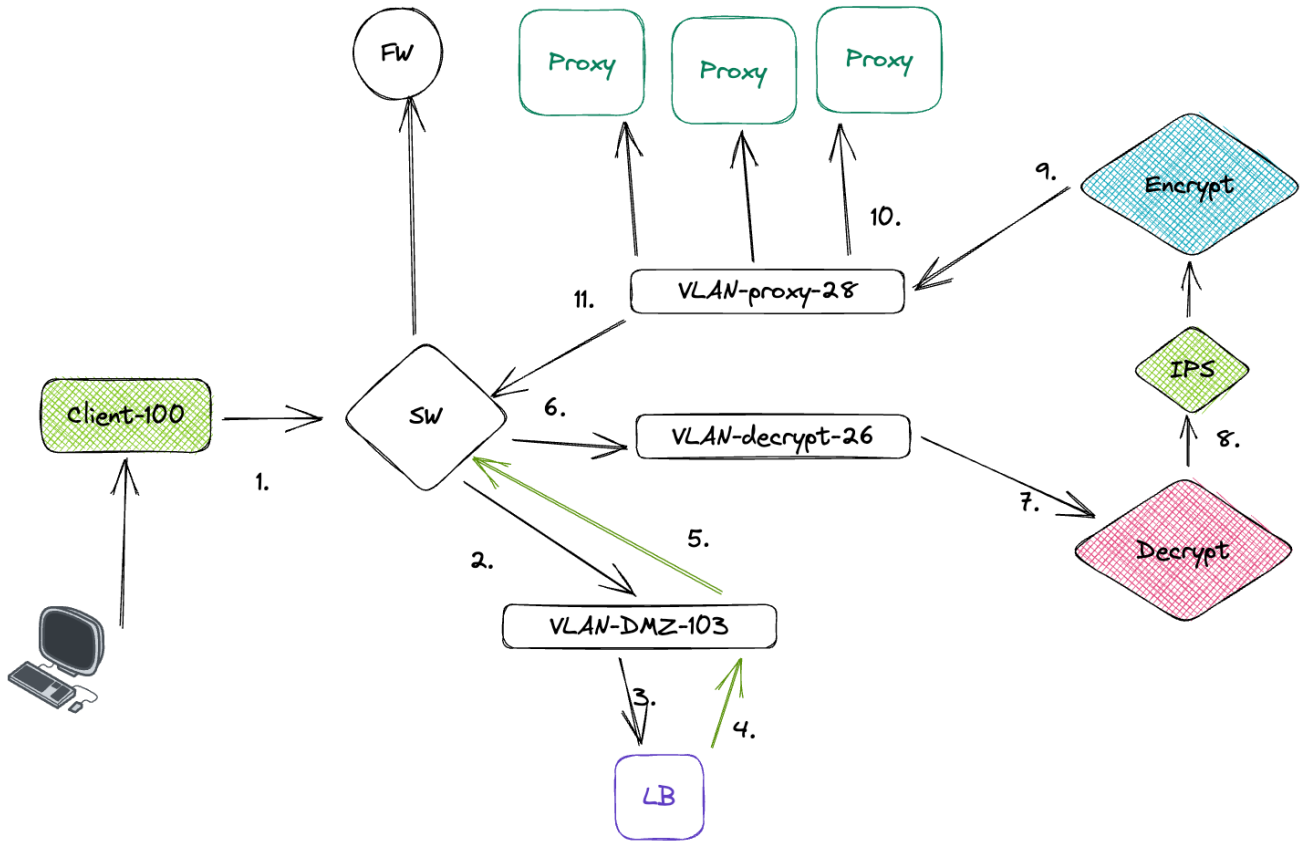
Current Topology



Security policy mandates deep packet inspection for outgoing traffic.

The proxies and the load balancer was not a physical node as well as the clients which are vdi nodes.

With this type of topology, we created an alternative I3 path which is health checked by load balancer and auto-bypassed in case of a failure within decryption solution.



How

Using an alternative entrypoint and added as a 4th proxy to lb's server farm, our explicit and decrypted path acted as another proxy. And an active healthcheck on load balancer continuously did checks in case any security solution between decrypt and encrypt path creates a problem.

Timeline

Project took 6 months to poc and implemet

Current status

more than 1500 users are actively decrypted and deep packet inspection is online