Interconnection Gateway architecture

Architecture Overview

Connectivity between the Service Provider's network and Zequenze's cloud-based platforms is established through a fully redundant VPN connection architecture.

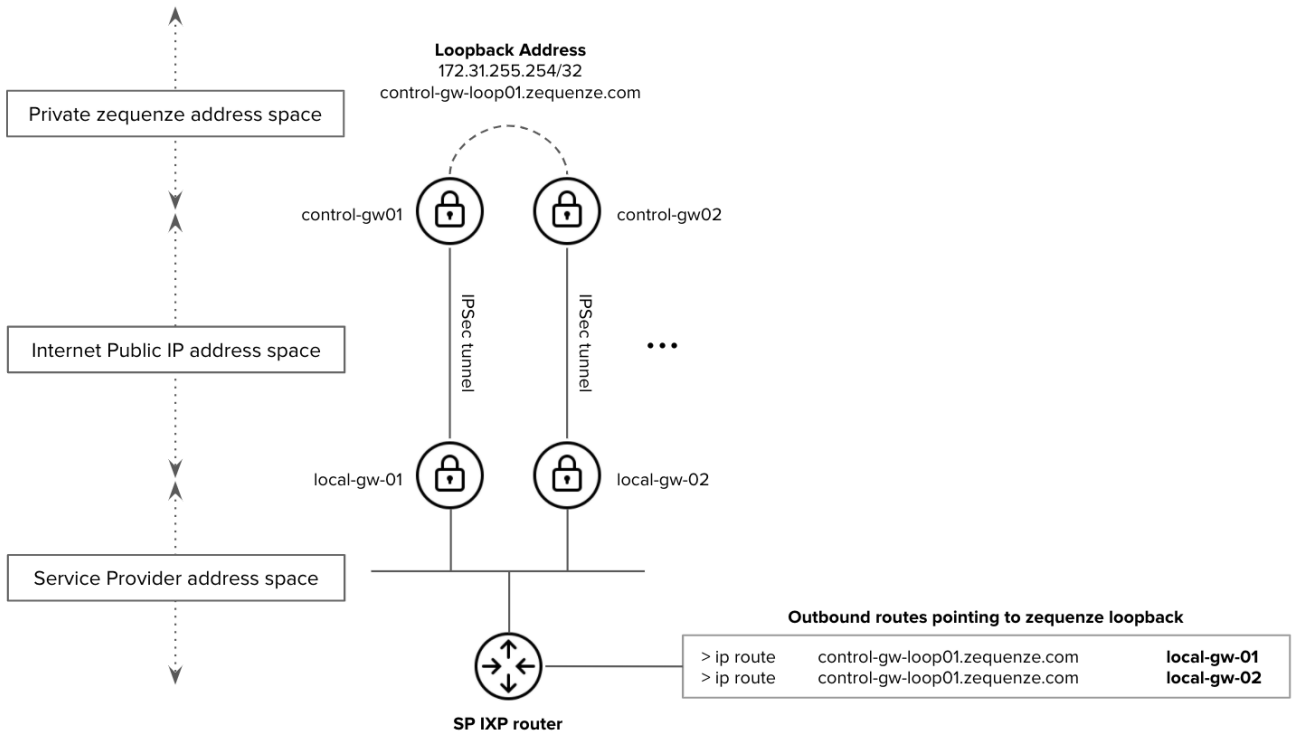

Figure 1. Zequenze Application-VPN architecture - interconnection with the Service Provider network

Distributed Gateway Architecture

Zequenze's cloud architecture implements a distributed application model that integrates both VPN and edge-application functionalities within the same gateway infrastructure. This design eliminates the need to propagate Service Provider IP prefixes throughout Zequenze's cloud infrastructure.

Device Configuration

Service Providers need to configure their customer premises equipment (CPE) to communicate with the edge-application gateways. Supported device types include:

- WiFi Access Points
- DSL modems
- FTTH ONT (Optical Network Terminals)
- eMTA (embedded Multimedia Terminal Adapters)
- LTE/5G routers

Once devices are pointed to the edge-application gateways, all internal communications within Zequenze's cloud architecture are handled automatically.

Simplified Routing Configuration

To maximize simplicity and resiliency, Service Provider devices only need to be configured with a single loopback FQDN/IP address. This loopback address remains active across all edge-application gateways in the array.

Example: `control-gw-loop01.zequenze.com` (as shown in Figure 1)

Service Provider Requirements

From a routing perspective, the Service Provider must ensure:

- IP reachability to the loopback FQDN/IP address from their border/IXP peering router
- Proper route advertisement as detailed in Figure 1

Resiliency and High Availability

Active-Active Gateway Operation

All edge-application gateways operate in always-active mode (1:1 or 1:N configurations). This allows traffic to be routed to any edge-application gateway in the array at any time without service interruption.

Traffic Flow Management

All responses from Zequenze to the Service Provider are sent through the same edge-application gateway that received the initial request. This approach ensures:

- Compatibility with active-standby scenarios within the Service Provider's network
- Prevention of asymmetric traffic routing issues

Failure Handling

Service Providers must implement proper failure detection mechanisms to prevent traffic black-holes in their VPN gateways when connectivity issues occur with Zequenze edge-application gateways.

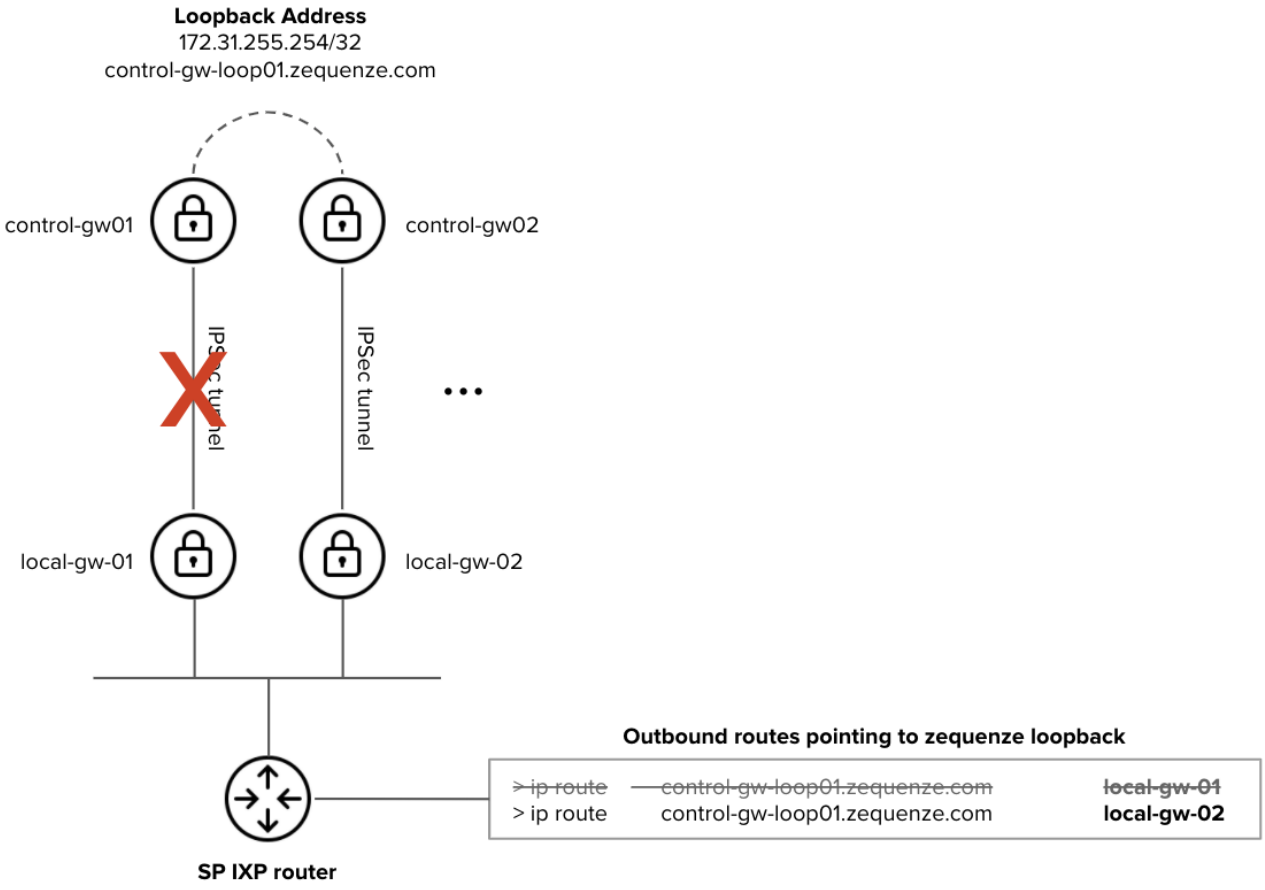

Figure 2. Zequenze Application-VPN architecture - High Availability considerations

Failure Scenario Example

In the failure scenario illustrated in Figure 2:

- The SP IXP router must be notified that the Zequenze edge-application gateway (`control-gw-loop01.zequenze.com`) is no longer reachable via `local-gw-01`
- Traffic must be automatically redirected to `local-gw-02` to maintain service continuity

This requires proper routing protocol configuration or health-check mechanisms on the Service Provider's infrastructure to detect and respond to gateway failures.

Revision #2
Created 2026-02-13 22:26:31 UTC by ipena@zequenze.com
Updated 2026-02-14 01:08:16 UTC by ipena@zequenze.com