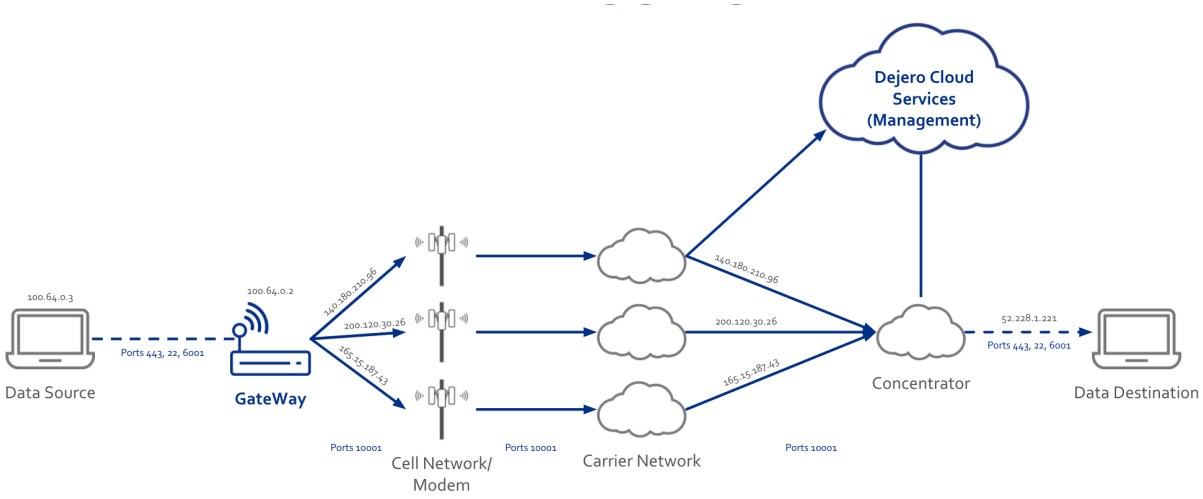
Dejero Smart Blending Technology – Security Overview

Smart Blending uses a packet-based approach to distributing data across links, enabled by real-time measurements of connection characteristics. This design avoids the drawbacks of solutions that maintain flow stickiness to connections and delivers superior performance with asymmetric connections like 4G LTE, 5G, and satellite—making it especially valuable in mobile and nomadic situations.

Additionally, novel adaptive input and output buffering combined with application acceleration techniques enable connections with significantly different characteristics to be effectively and efficiently used for applications that are very jitter sensitive.



The Dejero GateWay device supports multiple links and creates a tunnel through each link between the GateWay device and the GateWay Cloud Service. There is a control plane connection over TCP to enable the exchange of link performance metrics and coordination of the intelligent packet management. That connection is a TLS 1.3 connection with AES 256 encryption. Then, each WAN interface creates a tunnel from the gateway to the concentrator that is HMACSHA-1 encoded. The gateway will transparently forward any IP encrypted payload across the connection such as your encrypted video stream.

-The Dejero GateWay uses TLS 1.3 AES 256 encryption for its control plane and management traffic connections. Furthermore, each WAN interface creates a tunnel from the gateway to the concentrator that is protected with HMACSHA-1 encoding.

- Traffic is forward per-packet across these individual tunnels obfuscating data flows across multiple carrier paths. The Dejero GateWay uses up to 6 modems and up to 5 Ethernet connections across different carriers. Packets move simultaneously across the different carriers and routes to arrive to the cloud concentrators.

-The Dejero GateWay transparently forwards any IP encrypted payload or VPN service across the connection to the concentrator while still maintaining the ability to aggregate bandwidth across multiple carriers. There is no elephant flow restriction in bandwidth availability.

- The Dejero Internet service is protected by a Stateful Firewall with default rules to only permit traffic for established connections. Port forwarding and 1:1 SNAT rules can be configured as needed.

- Dejero incorporates security best practices throughout the Dejero Gateway platform. Dejero monitors, tests internally and in 3rd party labs and integrates regular security updates for Dejero software.