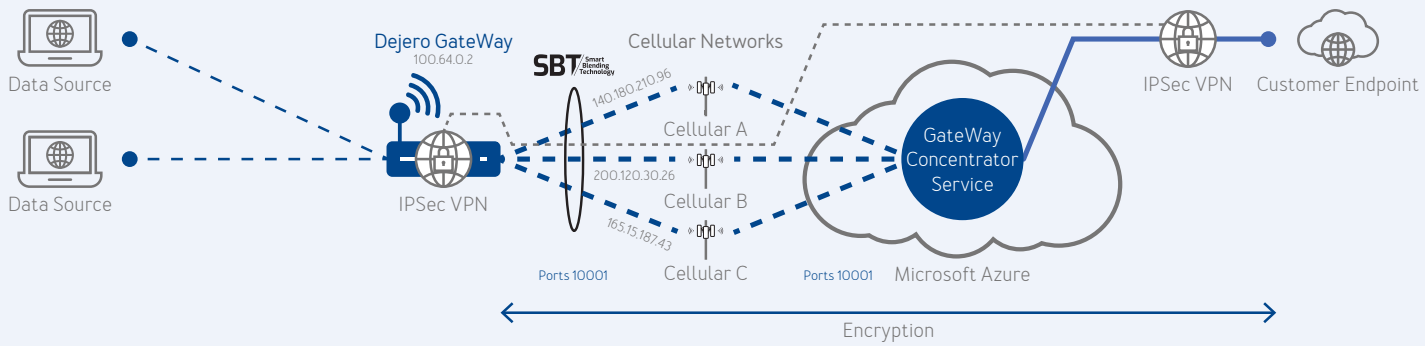
Dejero | GateWay VPN Client

Dejero is excited to introduce a new VPN client leveraging the robust open-source StrongSwan IPSec client, fortified with a FIPS-140-2 compliant encryption stack. This enhancement significantly bolsters the security posture of our GateWay platform, ensuring the confidentiality and integrity of data in transit.

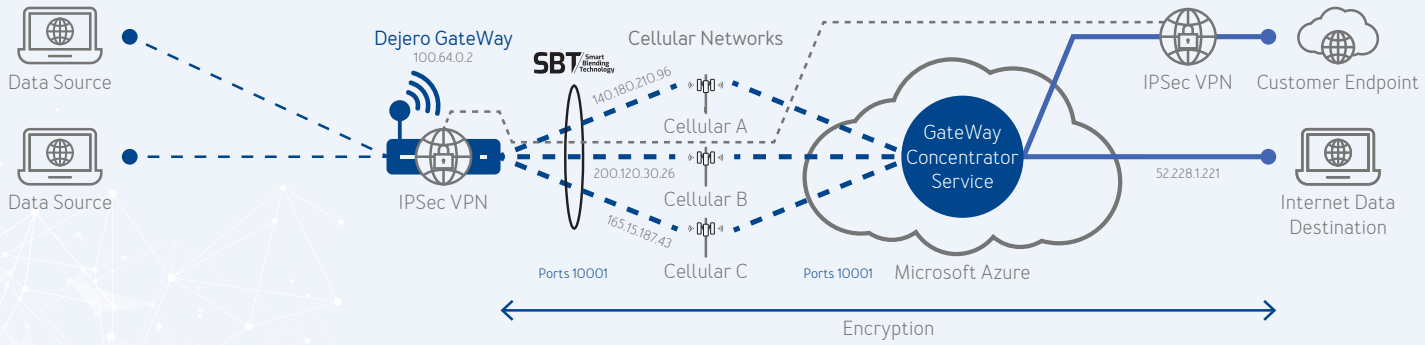
Overview

The GateWay IPSec client is intended to connect to a wide variety of customer controlled IPSec servers such as firewalls or routers. This will allow end-user data to be tunneled securely to one or more remote endpoints. In addition, the GateWay will support split domain tunnels which enables end-users to direct traffic to specific VPN connections or allow some data to be transmitted outside the tunnels directly to the Internet.

GateWay to Remote Endpoint VPN



GateWay to Remote Endpoint VPN With Split Domain Routing



Technical Implementation

The new Dejero VPN client utilizes the StrongSwan client as its foundation, known for its strong standards compliance and reliability. We have integrated a FIPS-140-2 compliant encryption stack, which adheres to stringent security requirements set by the U.S. government. This compliance ensures that all cryptographic modules used by our VPN client meet rigorous standards for design and implementation. Future improvements will include FIPS-140-3 compliant encryption.

Initial Release Features

The initial release of the Dejero VPN client will include:

- **IPSec/IKEv2 implementation using an AES-256 cipher suite**
- **Auto-reconnect:** IKEv2/IPsec offers an efficient reconnect function if your VPN connection is interrupted.
- **Multi-endpoint support:** Multiple VPN connections to different remote endpoints
- **Split Domain Tunneling:** Policy based routes can be implemented to direct specific traffic to secure VPN endpoints or directly to the Internet.
- **Supported across multiple devices:** IKEv2/IPsec is supported across a wide variety of devices, including firewalls, servers and a wide range of routers.
- **Pre-shared key authentication:** This allows for quick and straightforward VPN setup, especially in scenarios with a limited number of clients.
- **User-based credentials:** This provides individual authentication for each user, enabling granular access control and auditing.

Subsequent Release Features

A future release will further enhance the VPN client capabilities with:

- **Digital certificate generation:** This provides a more secure and scalable method for authentication compared to pre-shared keys.
- **Support for user-supplied certificates:** This allows users to bring their own digital certificates for authentication, promoting interoperability and flexibility.