Interface implementation

Connection tunnels

In adherence to PCI DSS standards, DECTA positions its servers within the Cardholder Data Environment, prohibiting direct communication with external hosts.

The initial step involves establishing an SSH or TLS tunnel between DECTA's servers and the Client's jump hosts.

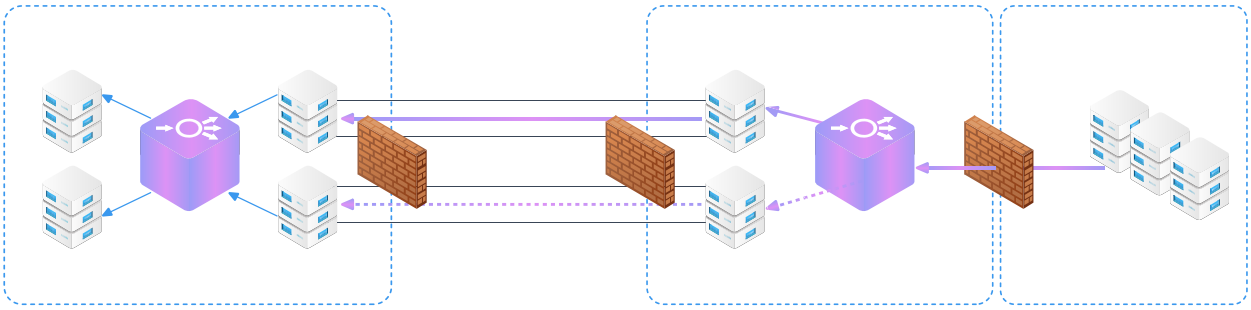
For production, DECTA employs two SSH jump servers to ensure high availability, fault tolerance, and uninterrupted maintenance of tunnel servers without downtime.

From the Customer's side, DECTA requires one or two endpoints (IP addresses) for tunnel termination.

Upon successful establishment of the tunnels, DECTA's servers can initiate connections using the ISO8583 Native interface over the established tunnel.

Customers are responsible for implementing SSH or TLS endpoints capable of accepting SSH (SSH tunneling with port forwarding) or TLS (tunnel) connections for both primary and secondary tunnels. These endpoints will forward traffic to the Native host-to-host interface endpoint servers.

The following diagram illustrates the implementation of the Native host-to-host interface using two jump servers on the Customer side:



Host-to-host connection schema

Deployment

1. Prepare SSH or TLS jump servers or serverless endpoints and allow connections from DECTA IP addresses;
2. Report back to DECTA IP addresses of created servers or endpoints;

3. For SSH implementation:
    - DECTA will create an SSH tunnel user, generate an SSH key pair, and share the username with the public key.
    - Customer creates SSH user named “username”;
    - Customer puts the public key file, received from DECTA, to “~/.ssh/authorized_keys” of the corresponding user;
    - Customer enables local port forwarding for SSH server.
4. For TLS implementation:
    - Both parties generate and exchange TLS certificates and use them for authentication and encryption.