Vertical Cloud Connect Security

Last Modified on 11/12/2020 6:28 pm EST

VCC provides a highly secure cloud infrastructure for enterprise deployments. VCC cloud services (hosted on Google Cloud Platform) allows for on-premise Wave Servers and Vertical Cloud Connect Gateways (VCCG) to connect to VCC using industry-standard encryption over SSL/TLS connections. Browsers also connect to VCC servers using trusted SSL/TLS connections.

Below are the key security protocols and connectivity supported -

- VCC uses a TLS Certificates. Communications from VCCG, Wave, and browsers uses standard AES256 encryption.
- VCCG instances and Wave instances are paired, which issues a client certificate for them to use when connecting back to VCC to identify them.
- Browsers use HTTPS.
- Voice and video traffic between VCCG and browsers use SRTP.
- User passwords are not stored, but rather hashed using bcrypt and uniquely salted. Browsers are issued a one-week token, and are forced to provide their password again after expiration.

Below are specific ports that are utilized inbound, outbound and browser connectivity -

- VCCG Servers require Inbound UDP 20000-21000. This is for SRTP.

- VCCG Servers use outbound HTTPS (TCP 443) and encrypted TCP connections to port 50071 on vappcenter.com

- Wave Servers use outbound HTTPS (TCP 443) and encrypted TCP connections to port 50070 on vappcenter.com

- Wave Servers do not require any inbound connections for VPW or other vAppCenter applications (Note: ViewPoint Mobile on iOS or Android does require inbound Wave connections)

- Browsers use standard HTTPS (TCP 443) and HTTP (TCP 80), which is redirected to HTTPS