Ion Protocol

Protocol

Summary

The Ion Protocol is a custom, in-house TCP protocol developed by Aqua Connect. It operates like RDP or RFB, but it has several improvements with things such as picture quality, speed, size, etc.

These features are currently being implemented with their position in the list being their priority. The protocol is transmitted on port 310, this value can be adjusted in the Ignision SE application. Please note that there is a known issue when adjusting this value related to RDP and it is actively being worked on. The protocol, however, doesn't show as a standard TLS 1.2 protocol. The reason for this is that an additional header is added to the packet that potentially contains additional information. This makes it harder for "man-in-the-middle" attacks and packet sniffers to pickup on the Ion packets and cause mayhem.

Security

Ion use OpenSSL to encrypt network traffic using the TLS v1.2 protocol (https://www.ietf.org/rfc/rfc5246.txt). The key is a 4,096-bit RSA key that uses a SHA-512 hash, stored in a base64 format. The certificate that is used by Ion and Ignision is an x509 v3 OpenSSL certificate that is stored in a base64 format. As of right now, there aren't any known vulnerabilities that directly affect Ion and Ignision when using TLS 1.2. Ion and Ignision will also pick a cipher from a list of all ciphers supported by the library (latest stable OpenSSL). For more information on how TLS and OpenSSL works, see these resources:

- http://realm.wiki.snowrealm.info/index.php?title=SSL
- https://en.wikipedia.org/wiki/Transport_Layer_Security
- https://www.ietf.org/rfc/rfc5246.txt
- https://en.wikipedia.org/wiki/Category:Web_security_exploits

It is also important to note that all the certificates and keys used by Ion and Ignision are owned and managed by the root user on the server. This helps prevent users on the system from toying with the integrity of the connection and it's security.