INTEGRATING OVRC WITH YOUR CORPORATE NETWORK

CONTACTING TECH SUPPORT

Phone:	866.838.5052 | 704.909.5229
Email:	TechSupport@SnapAV.com

WHY?

- This document details the security protocols used by OvrC, and instructs system administrators how to enable the capabilities of OvrC to be used through a corporate firewall.

Foundation:

1. **All OvrC communication is initiated by the device and sent outbound to OvrC.** There is no need to alter your firewall to allow for inbound traffic.
2. **Communication is executed with WebSocket protocol.** All communication to and from OvrC is done over HTTPS using TLS 1.2.
3. **OvrC Pro tunnels have a 30-minute timeout.** Subsequent communication requires that the device open a new tunnel, which gets sent to a new random port. This applies to networks using the OvrC Pro Device.

SnapAV Device Requirements:

Direction: **Outbound**

Protocol: **HTTPS**

Destination: **cloud.ovrc.com**

Ports: **443** and **22**

DNS Lookup: **Enabled, port 53**

TCP: **Enabled**

Tunneling with OvrC Pro Devices:

Direction: **Outbound**

Protocol: **TCP**

Destination: **tunnel.ovrc.com**

Port Range: **32255–65535**