colorfront

Remote Streaming

Security Overview

Introduction

Colorfront's Streaming Server solution offers a secure, reference-quality and low latency remote viewing experience that is suitable for critical QC or client approval. This document describes the security aspects of the technology, including encryption of transmitted data, networking configuration and protection against unauthorized access at playout.

The appliance streams HD, 2K & 4K, and stereo3D video, in Rec709 SDR or HDR with Dolby Vision, and uses SRT (Secure Reliable Transport Protocol) to deliver pristine quality, low-latency live video, plus multi-channel audio, over the public internet to multiple remote clients concurrently. Forensic NexGuard watermarking and 256-bit AES encryption are used to ensure content remains secure and protected.

Features

Colorfront Streaming Server is a 1RU dedicated server appliance offering multiple channels of live video streaming, via 12G-SDI input in UHD, with Dolby Vision support. Sub-second latency reference quality video streaming from live video gives users the quality of review you would expect in a grading suite or screening room, but remotely. Color- and frame-accurate footage in 4K HDR from various applications such as Blackmagic Resolve or Autodesk Flame – all in real-time.

- **Sub-second latency robust streaming**
  minimal delay realtime video delivery
- **8-800 mbit HEVC**
  much more efficient than intra-frame encoding for higher quality of service at any given bit-rate
- **SRT (Secure Reliable Transport Protocol)**
  pristine quality, low-latency live video over the public internet
- **10-bit 4:4:4 reference quality video**
  allows color accurate critical QC on a theater projector or 4K HDR reference broadcast monitor
- **Multi-channel audio**
  48kHz 16bit embedded AAC audio with 5.1, 7.1 sorround sound or immersive 5.1.4 channels
- **HD SDR to 4K HDR in stereo 3D**
  works with HD, 2K & 4K, and stereo3D content in Rec709 SDR or HDR
- **Dolby Vision tunneling**
  High Dynamic Range with with Dolby Vision on prosumer displays such as an LG OLED via HDMI
- **256-bit AES encryption**
  the same requirement the Hollywood studios trust for all their sensitive content
- **Watermarking**
  NexGuard forensic video watermarking, audio watermarking and visible per-user burn-ins
- **Multiple destinations**
  point-to-multi point solution allows collaboration with multiple remote clients simultaneously anywhere in the world
- **Streaming Player client on Windows & MacOS**
  low cost hardware supported on tower, 1RU and even on a laptop configuration
- **Professional AJA/BMD video out via SDI/HDMI**
  Supports AJA Kona 5/Corvid 44/io4K+/T-Tap Pro & BMD DeckLink Mini Monitor 4K/UltraStudio 4K Mini
- **Haivision Hub and Gateway compatibility**
  Interoperable with SRT solutions from other vendors such as AWS MediaConnect

System Architecture

The below schematics illustrate the two possible system architectures of the Colorfront Streaming solution using either the SRT Gateway for firewall traversal or streaming directly.

The standalone, 1RU Streaming Server located behind the facility firewall is directly connected to a third party post-production system via SDI video interface, and is encoding a live video stream. The carrier of the HEVC encoded video is SRT over UDP protocol. The stream is received and decoded by the Colorfront Streaming Player application running on commodity hardware, and displayed on a connected professional monitor or pro-sumer display.

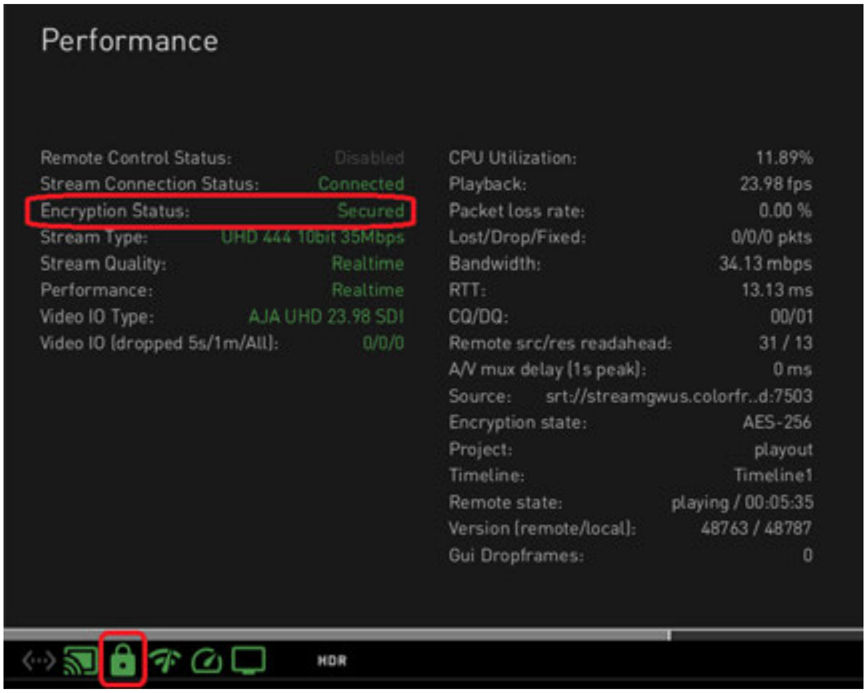
Video SRT Transport

SRT

SECURE
RELIABLE
TRANSPORT

SRT stands for Secure Reliable Transport. SRT is an open source payload agnostic transport protocol and technology stack that optimizes streaming performance across unpredictable networks. SRT operates at the network transport level with the UDP protocol as an underlying transport layer, acting as a wrapper around your content. It can transport any type of video format, codec, resolution, or frame rate.

With **end-to-end 128/256 bit AES encryption**, valuable content is protected all the way from the server to the Colorfront provided, secure Streaming Player client application. The handshaking process used by SRT supports outbound connections without the potential risks and dangers of permanent exterior ports being opened in a firewall, thereby maintaining corporate LAN security policies and minimizing the need for IT intervention.



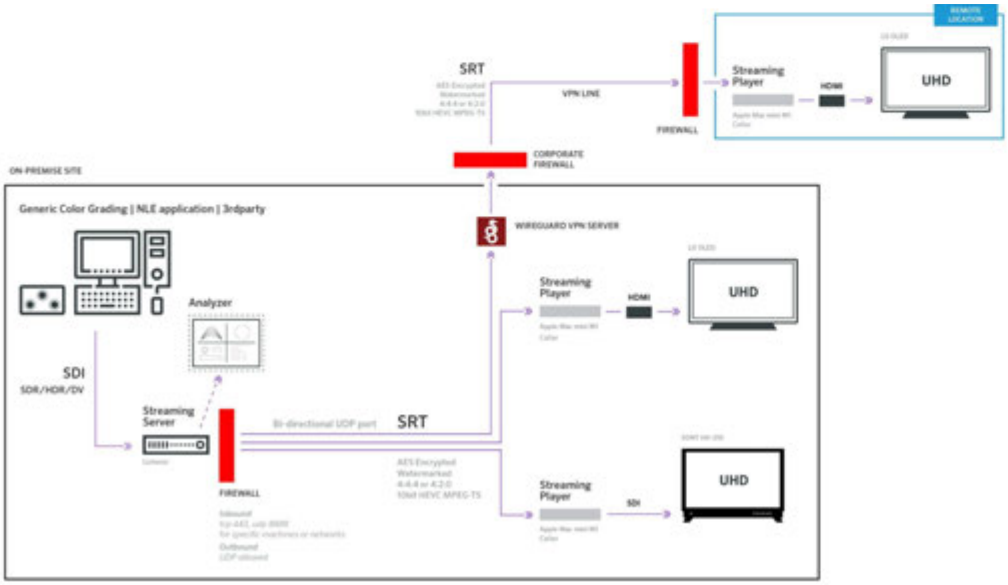
Performance

```
Remote Control Status:                    Disabled    CPU Utilization:                          11.89%
Stream Connection Status:                Connected    Playback:                              23.98 fps
Encryption Status:                         Secured    Packet loss rate:                         0.00 %
Stream Type:                UHD 444 10bit 35Mbps    Lost/Drop/Fixed:                     0/0/0 pkts
Stream Quality:                           Realtime    Bandwidth:                          34.13 mbps
Performance:                              Realtime    RTT:                                  13.13 ms
Video IO Type:                   AJA UHD 23.98 SDI    CQ/DQ:                                   00/01
Video IO (dropped 5s/1m/All):                0/0/0    Remote src/res readahead:              31 / 13
                                                      A/V mux delay (1s peak):                  0 ms
                                                      Source:    srt://streamgwus.colorfr..d:7503
                                                      Encryption state:                      AES-256
                                                      Project:                               playout
                                                      Timeline:                            Timeline1
                                                      Remote state:               playing / 00:05:35
                                                      Version (remote/local):          48763 / 48787
                                                      Gui Dropframes:                              0
```

The “green lock” indicator in the client application shows successful connection to an encrypted stream.

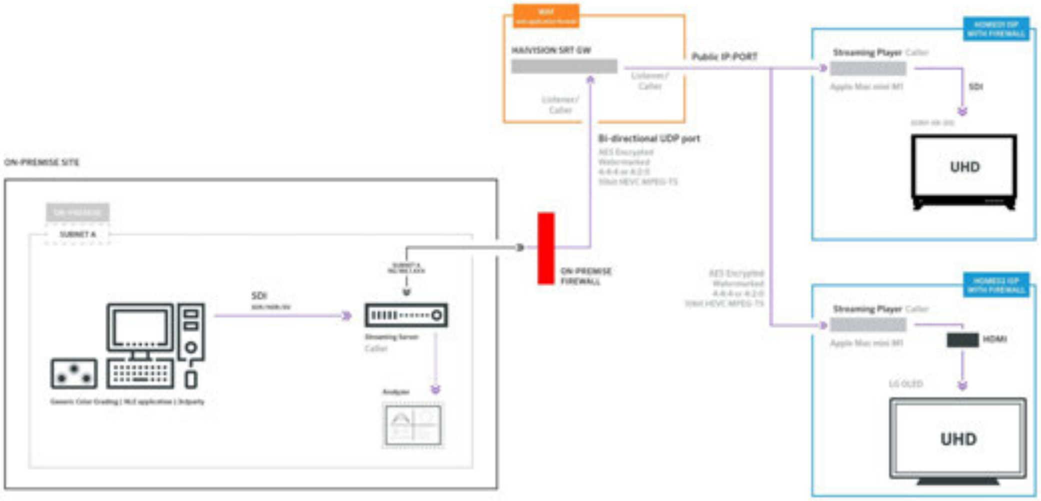
Direct Streaming

Establishing the communication for direct streaming from the Streaming Server to one or multiple clients requires either the parties to be on the same network, or port forwarding (NAT) rules to be in place. This is necessary for the UDP communication requests to traverse the network gateways, such as routers and firewalls. Often a Virtual Private Network (VPN) connection is used to provide a secure, encrypted tunnel through which a remote (authorized) user can access a facility network. In this scenario the stream is transferred “tunnel-in-tunnel” providing an extra layer of security, at the expense of network traffic overhead.



Streaming via the Gateway

The encrypted SRT stream may be sent directly to a **Haivision SRT Gateway**, a Haivision product for secure routing of live video streams across different types of IP networks. In this configuration the Gateway offers secure firewall traversal resulting in a simpler network configuration.
https://www.haivision.com/products/srt-gateway/



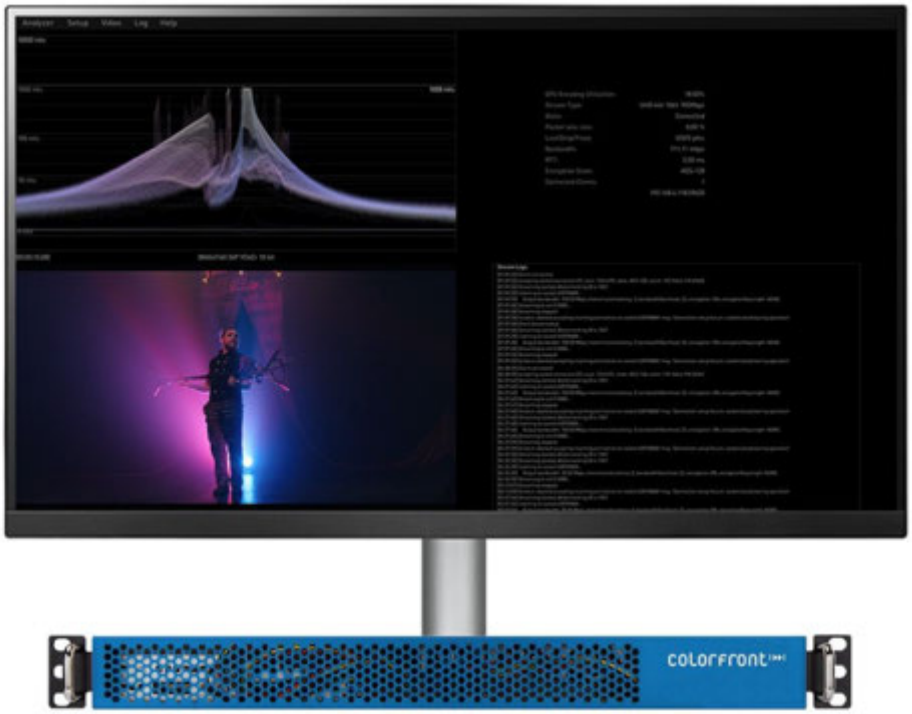
Haivision SRT Gateway can run on premises, in a private data center, or in the public cloud, such as AWS EC2. The Streaming Server is the caller, there is no need to open up the firewall for incoming connections.

Only a single outbound UDP port connection needs to be allowed from the on-premise Streaming Server to the Haivision SRT Gateway, which is set up in listener mode. A single Haivision SRT Gateway can serve multiple streams on separate ports, and multiple Streaming Player clients can connect to a given port on the Haivision SRT Gateway.

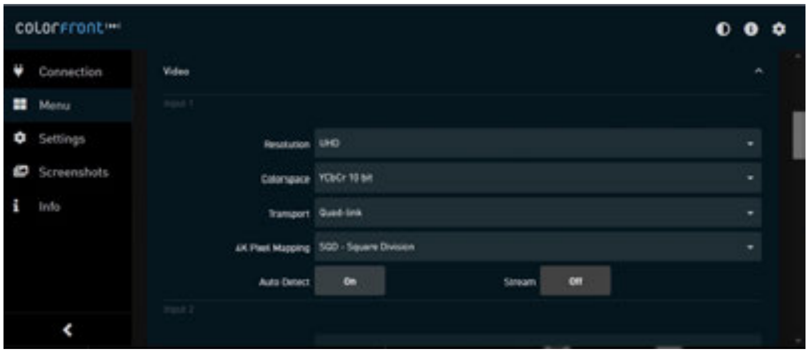
Components

Streaming Server

Colorfront Streaming Server is a Windows application running on a 1RU Supermicro computer. AJA Kona5 video card captures the live video feed from up to four (4) SDI input connections. The system is located on premise, part of the facility infrastructure. Editing, mastering and other post-productions systems to be accessed remotely are connected via SDI video signal. This server is behind the facility firewall with a single UDP connection to the Haivision SRT Gateway. As the Streaming Server is the caller, there is no need to open up the firewall for incoming connections.



The incoming video feed is never written to any storage device, it is encoded from memory using NVidia GPU accelerated HEVC encoding.



Resolution: UHD

Colorspace: YCbCr 10 bit

Transport: Quad-link

4K Pixel Mapping: SQD - Square Division

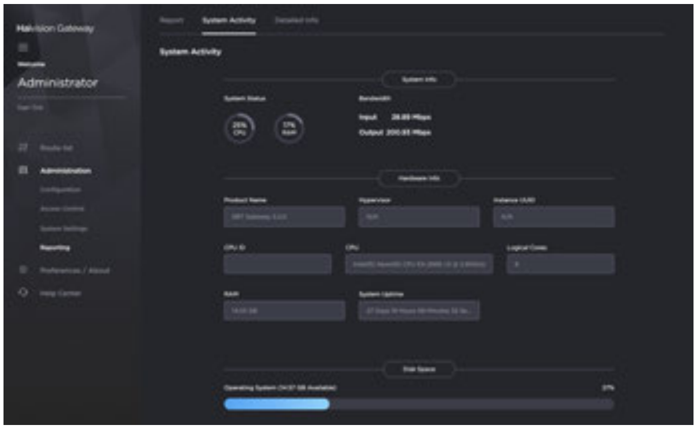
Auto Detect: On

Stream: Off

A Web Control Interface page is hosted on the Streaming Server machine, which is accessible from other computers via HTTPS if the server's firewall is configured to allow that.

SRT Gateway

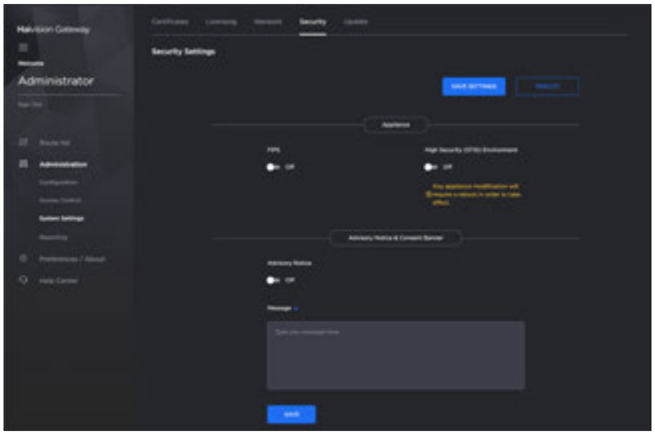
The Haivision SRT Gateway is a robust, scalable network bridge between the source stream and the clients. It has useful protocol conversion, stream replication and routing options, both on premise and in the cloud. Furthermore, by utilizing the gateway product as the bridge between the stream source and destination, it is possible to implement a set of security policies that allow communication between different networks, without compromising security by opening up ports on the firewall.

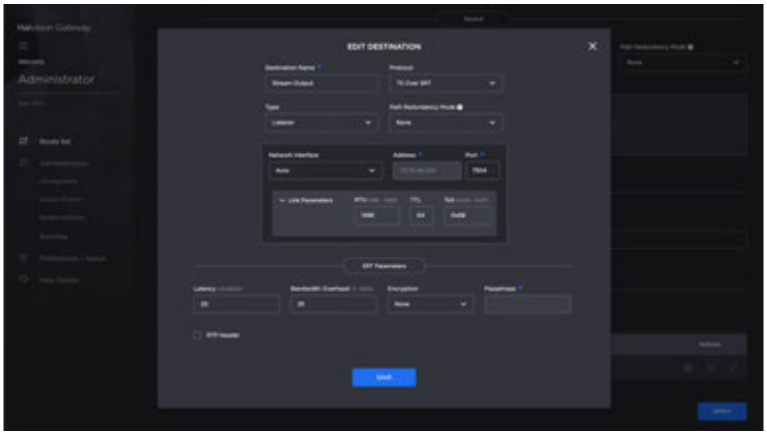


Input 28.88 Mbps

Output 200.85 Mbps

IP firewalls normally block external access to a network and thus prevent video streams from being delivered from one location to another. The SRT Gateway can be configured to be the listener, so that the Streaming Server behind the firewall can send streams as a caller, without breaching network security policies and minimizing the need for IT intervention.



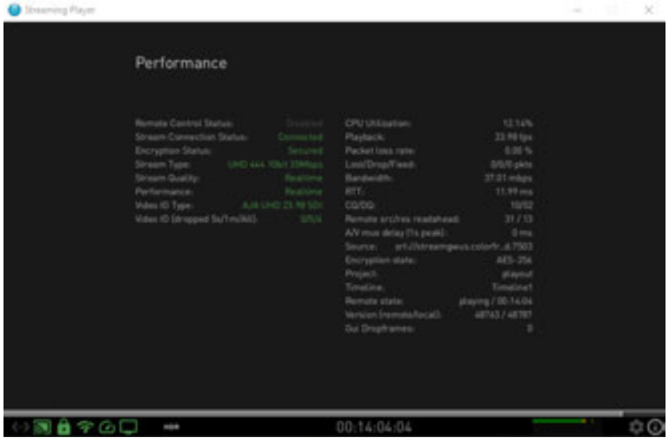


Streaming Player Client

The Colorfront Streaming Player is the receiver software running on Microsoft Windows or Mac OS X. By setting up the IP address and port number of the streaming source - typically an SRT Gateway output, and the necessary encryption passphrase, this software de-encrypts and decodes the video stream. The user looks at the content either on the directly connected computer monitor, or using consumer or professional HDMI or SDI displays.

The

For more information about the security aspects of the Streaming Player application please see *Content Watermarking* below.



```
Performance

Remote Control Status:            Disabled    CPU Utilization:                   12.14%
Stream Connection Status:        Connected    Playback:                       23.98 fps
Encryption Status:                 Secured    Packet loss rate:                  0.00 %
Stream Type:        UHD 444 10bit 35Mbps    Lost/Drop/Fixed:               0/0/0 pkts
Stream Quality:                   Realtime    Bandwidth:                     37.01 mbps
Performance:                      Realtime    RTT:                             11.99 ms
Video IO Type:          AJA UHD 23.98 SDI    CQ/DQ:                              10/02
Video IO (dropped 5s/1m/All):       0/0/4    Remote src/res readahead:         31 / 13
                                              A/V mux delay (1s peak):            0 ms
                                              Source:     srt://streamgeus.colorfr...d:7503
                                              Encryption state:                 AES-256
                                              Project:                          playout
                                              Timeline:                       Timeline1
                                              Remote state:           playing / 00:14:04
                                              Version (remote/local):     48743 / 48787
                                              Our Dropframes:                         0

00:14:04:04
```

Streaming Player client software has **screengrab protection** to prevent recording the video content or capturing the screen on the client computer. This operating system level limitation, both on the Windows and the Mac platform also block screen sharing applications from transferring the visual content.

The video frames are decoded in memory, there are no temporary files saved to storage. Downloading or saving video or audio content from the player application is not possible.

Streaming Session Lifecycle

Creating a Session (direct)

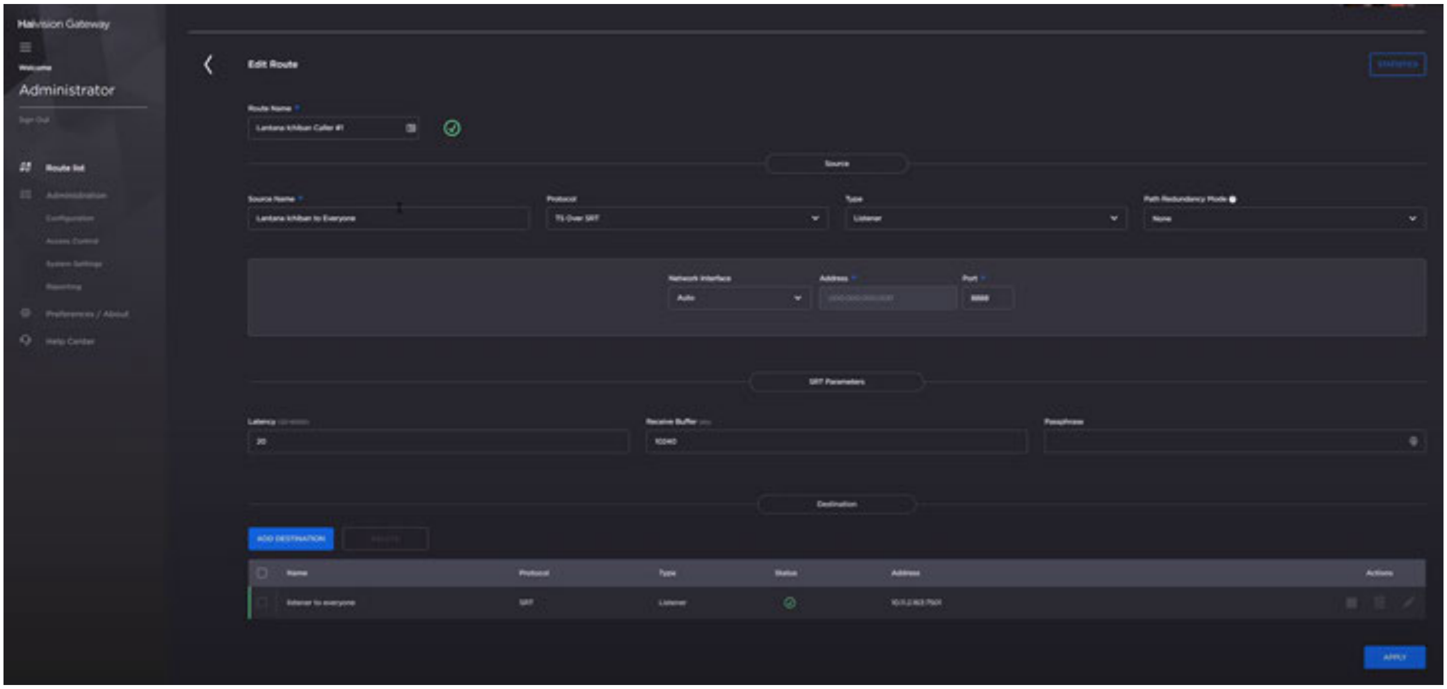
A streaming session is initiated from the Streaming Server unit itself. By starting a session the operator performs the following actions:

- Sets up new, random 64 character passphrase for the required streaming channels (up to 4) to take maximum advantage of the 256-bit AES encryption
- Configures for each both the visible, burn-in watermark and the forensic watermark payload ID.
- Shares the secret passphrase and the address (IP, port) with the client via some secure communication channel

Creating a Session (via SRT Gateway)

The secure communication between the Streaming Server and the SRT Gateway is established. To initiate new streaming sessions the operator performs the following actions:

- If needed re-configures for each both the visible, burn-in watermark and the forensic watermark payload ID in the Streaming Server unit.
- Logs in to the Gateway with 2-factor authentication
- Creates the required number of routes with 256 AES encryption, each with a random passphrase
- Shares the secret passphrase and the address (IP, port) with the clients via some separate and secure communication channel



Route Name *: Lantana Ichiban Caller #1

Source Name *: Lantana Ichiban to Everyone
Protocol: TS Over SRT
Type: Listener
Path Redundancy Mode: None

Network Interface: Auto
Address *:
Port *: 8888

Latency: 20
Receive Buffer: 10240
Passphrase:

Name	Protocol	Type	Status	Address	Actions
listener to everyone	SRT	Listener	✓	[illegible]	

Setting up a new route in the SRT Gateway

Client Connection

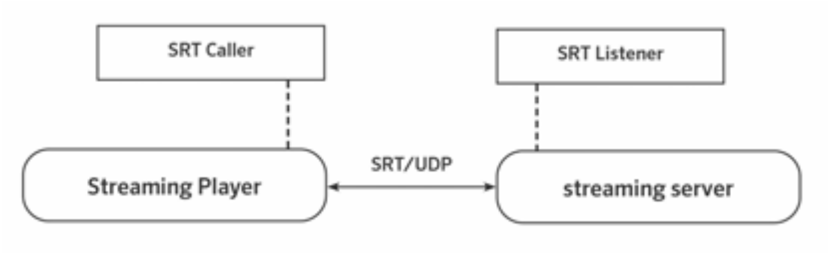
Client application connects to the stream by the operator manually entering IP, port and passphrase. If the handshaking process is not completed (e.g. mismatching passphrase), the "listener" is closing the connected socket immediately, so it is not possible to receive the encrypted bits without knowing the passphrase.

Network Communication

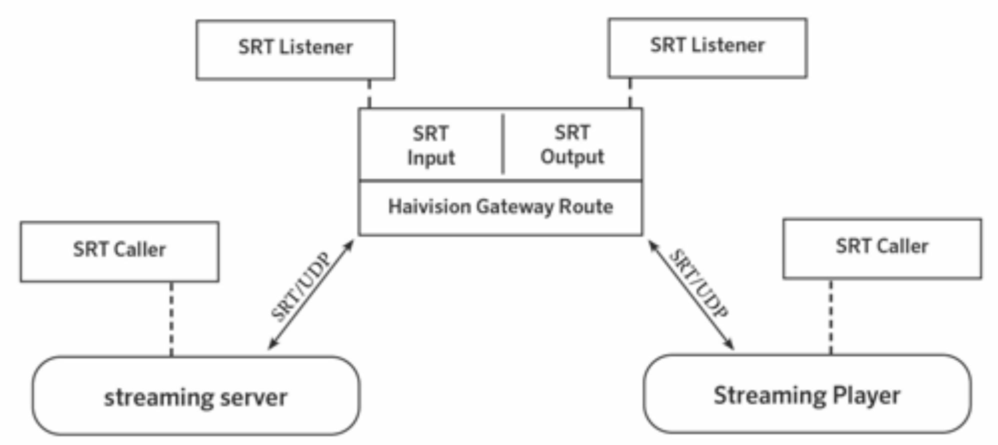
Streaming from the Colorfront Streaming Server requires a single UDP port to be open for the bi-directional data transfer (data and control flow over the same socket). Streaming server and client both can work in listener or caller mode, the mode controls the direction of the connection establishment. Always the caller initiates the connection to the listener. After the socket connection is established a handshake process will be initiated, during this process both parties exchange authentication information based on passphrase configured on both sides. If the handshaking is successful the listener accepts the connection and starts to deliver the encrypted data, otherwise the connection is rejected.

Without correct passphrase there is no way to retrieve the encrypted stream data as there is no stream data distribution without successful handshake. When utilizing the four channel capability of the server, four individual ports are assigned to the four independent streams. Port numbers are configurable. These are all based on the industry standard SRT (Secure Reliable Transport) protocol.

Network Diagram



Direct Streaming



Streaming via the SRT Gateway

Streaming Server Network Connections

- UDP ports (up to 4) for SRT stream, *calling* the Gateway. By default ports 8888, 8889, 8890, 8891. (when using direct stream, these ports need to be accessed from the client in *listening* mode)

- Optionally Streaming Server firewall can be configured so users can access the Web UI Controller page via HTTPS at port port 443

The Web Controller interface is a web page hosted on the Streaming Server via Apache. In case local network access is required for this interface, the 443 port needs to be opened for HTTPS access.

SRT Gateway Network Connections

- The Streaming Server as the caller establishes UDP connection(s) to the Gateway, to its configurable input ports. We recommend whitelisting the IP range where the server is expected to establish connection and deny any other incoming traffic.
- The Gateway can be configured to have a flexible number of routes, each with its adjustable port number. These will be *called* from the client application to establish the UDP connection for the stream.

Client Application Connections

The Streaming Player client is running on the client computer with some public internet connection via some ISP. Client computer firewall rules need to be configured so the client can call either the Streaming Server (direct streaming) or the output port of the SRT Gateway.

Content Watermarking

Forensic Video Watermarking

Colorfront Streaming utilizes NexGuard forensic watermarking technology for PreRelease Content (aka. NGPR/G2). For every new Streaming Session a random Payload ID is inserted into the video essence, which can be retrieved later from the video content, even if it was resampled, re-encoded or re-captured. Payload ID is logged along with all the metadata describing the Streaming Session.

NOTE: NexGuard forensic watermarking requires a license from NAGRA to be installed on the server

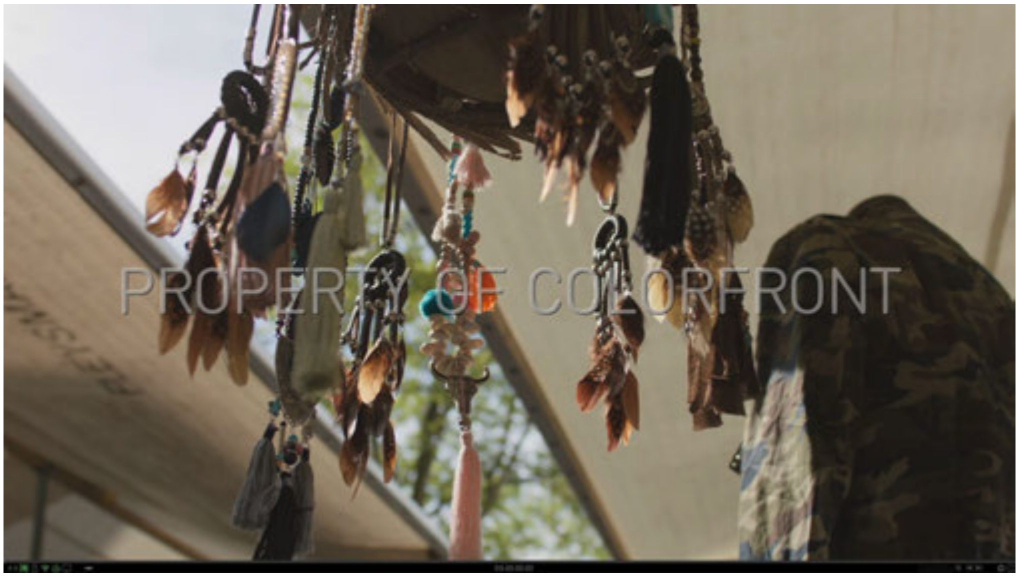
Audio Watermarking

Colorfront Streaming utilizes NexGuard Audio Watermarking technology. For every new Streaming Session a random Payload ID is inserted into the audio essence, which can be retrieved later from the audio content, even if it was resampled, re-encoded or re-captured. Payload ID is logged along with all the metadata describing the Streaming Session.

NOTE: NexGuard forensic watermarking requires a license from NAGRA to be installed on the server

Visible Watermarking

The video stream may have visible watermarking which is burnt into the video frames at the server, upon encoding the HEVC video payload. The Streaming Server product has four (4) output channels, each of these can be assigned its own unique visible watermark.



Watermark burnt into the image

Deployment and Change Management

Installing the System

The Colorfront Streaming Server is an appliance with all necessary components pre-installed. The software is running on a Windows Supermicro workstation, thus the IT department has the ability to implement any necessary user access restriction or OS level security hardening.

The SRT Gateway is a product of Haivision, Colorfront is not involved in the deployment of it. The Gateway is available in the AWS Marketplace.

The Streaming Player client application is available as Windows or Mac software, links to the installers are either provided by the support agents or are published in Colorfront's Help Center page. Licenses are provided by Colorfront or by the product's reseller.

Version Updates

There is no automatic, continuous update process, new versions have to be installed manually. This is due to the stability needs of productions already using the system. New versions will be posted in the Colorfront Help Center and can be securely downloaded and installed as a standard software update. There is an option to request the latest version, and also there is a version control for the stream, that prohibits earlier versions of the application to receive a newer version of the stream sent by the latest server.

Details Release Notes are posted for each stable release, any security related changes will be detailed there.
New versions are tested internally at Colorfront both automatically and manually.

Logging

Server Logs

Streaming Server logs events into a secure database hosted within the facility infrastructure. Events include start of Streaming Session, end of Streaming Session, client connection/disconnection. A unique Session ID, timestamp, stream characteristics, client IP and Port, Watermarking Payload ID are logged for later review.

Gateway Logs

The SRT Gateway generates a number of different logs providing system, diagnostic and application messages. The Haivision Gateway log is saved on the system locally and administrators can access them on the Report panel of the web interface, and can be queried by the Streaming Server via a secure REST API, so information can be securely logged.

Streaming Player Client Logs

The Streaming Player application saves a daily log file for diagnostic purposes to the local file system with all activities logged with a timestamp.

Customised Logging

Colorfront works with customers to integrate secure logging of events into customer-specific logs. Most often this is performed using a customer-specific Restful API, but can be other methods as needed. The Streaming Server can be constrained, to allow streaming only if such secure logging is performed.