Task 01: Networking | Streaming to the cloud

1. Port Forwarding:

- **Technical Assumptions**: Assumes that the router supports port forwarding and the cameras are accessible via RTSP over the local network.
- **Shortcomings**: Exposes cameras directly to the internet, increasing security risks such as unauthorized access or exploitation. Limited scalability for multiple cameras.
- **Mitigation Strategies**: Implement strict access control lists (ACLs) to restrict access to trusted IP addresses. Regularly update firmware and monitor for security vulnerabilities. Consider using VPNs for secure remote access.

2. VPN (Virtual Private Network):

- **Technical Assumptions**: Assumes the ability to set up a VPN server/router and that cameras support VPN client connections.
- **Shortcomings**: Requires additional configuration and maintenance overhead. May introduce latency and bandwidth constraints. Limited scalability for large camera deployments.
- **Mitigation Strategies**: Implement VPN encryption and authentication mechanisms to secure communication channels. Optimize network infrastructure for minimal latency. Use load balancing and redundant VPN servers for high availability.

security requirements, scalability, and performance, a **Virtual Private Network (VPN) solution would likely be the best choice for enabling access to RTSP streams** from IP cameras within the local network for integration with cloud-based analytics. Here's why:

1. **Security Requirements:**

- VPNs provide a secure and encrypted connection between the local network and the cloud-based analytics platform. This ensures that data transmitted between the IP cameras and the cloud is protected from interception or tampering by unauthorized parties.
- VPNs also offer authentication mechanisms to verify the identity of users or devices accessing the network, enhancing security.

2. **Scalability:**

- VPN solutions can be scaled to accommodate a large number of IP cameras and users. VPN servers can be deployed in a distributed manner to handle increased traffic and connections.
- As the number of IP cameras or users grows, additional VPN servers can be added to the network to maintain performance and reliability.

3. **Performance:**

- VPN connections typically have low latency and high throughput, especially when deployed using modern encryption protocols and optimized network configurations.
- By establishing direct connections between the local network and the cloud-based analytics platform, VPNs minimize the overhead associated with data transmission and processing, resulting in improved performance.