You are asked to create a Virtual Private Network (VPN) connectivity troubleshooting checklist for future use. Using the following information as a guide, create a detailed checklist that will help you and others resolve general VPN connectivity issues.

**End-to-End Connectivity Considerations**

Troubleshooting a VPN client connection follows similar checks and validations as any other network connectivity issue. You check basic connectivity indicators (i.e., Ping and traceroute), logically step through VPN client configuration and versioning, and process error logs on both ends of the connection.

Establish the necessary procedures and steps taken to remedy remote connection issues. Include VPN specific procedures when you have completed a basic connectivity check. Walk through the process of connecting and authenticating with VPN devices and any troubleshooting routines necessary on the corporate network side.

Consider the following:

* Is the VPN service active and functional?
* Does the client have basic connectivity?
* Does the client application launch?
* Can the client log in using the client application?

Each VPN setup proposes different challenges in troubleshooting end-to-end connectivity. Discuss the procedural steps that are necessary to verify correct client-side and server-side behaviors.

**Examine the Underlying Infrastructure**

Consider any points of network failure from routing problems to router failures. Connectivity and routing problems occur when the transport network fails to meet operational needs. A link may have insufficient bandwidth or capacity to sustain VPN traffic and defective or faulty routing hardware may fail to pass VPN traffic.

Establish network infrastructure sanity checks such as:

* Does the network have sufficient bandwidth?
* Does the network use supportive services?
* Does the network impose any restrictions on passing VPN traffic?
* Does the network connectivity slow or spotty?

Define ways to explore faults and failures in the network and any implications that come from having limited or no control over the underlying network infrastructure.

**Complex Configurations Demand Complex Solutions**

Complex VPN configurations require more sophisticated analytical methods and processes, such as a routing protocol encapsulated into Internet Protocol Security (IPsec). Troubleshoot checkpoints may occur at several layers depending on how deeply packets are encapsulated and how well embedded protocols route. You may have to check several log file sources including appliances, firewalls, routers, and system services.