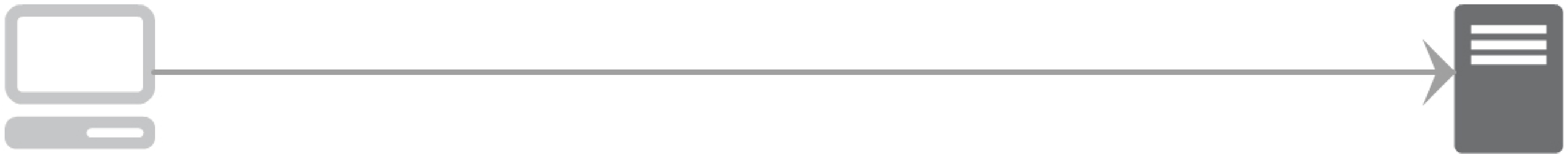
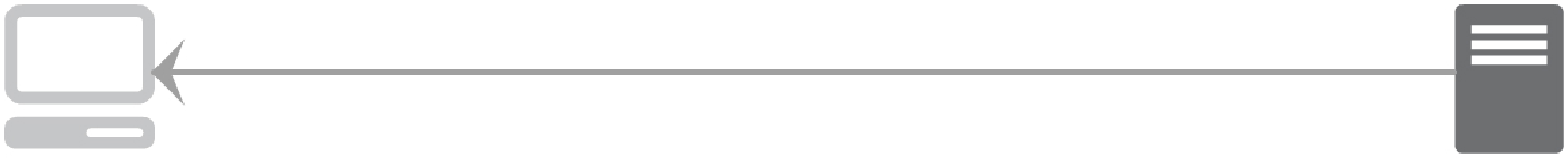
Host starts communication by on Port 135 to connect to client on RPC on TCP protocol. 3 way handshake is completed and then the Host asks the Client for the WMI port.



HOST
Windows OS
Inbound Rules: Port 135 :TCP
Outbound Rules: Port 135: TCP
Outbound Rules: All Ports between
8000 and 65535: TCP

CLIENT
Windows OS
Inbound Rules: Port 135 :TCP
Outbound Rules: Port 135: TCP
Outbound Rules: All Ports between
8000 and 65535: TCP

Client sends back the port number for WMI communication. By default, Windows is configured to initiate WMI communication on any port between ~8000 to 65535(This is known as dynamic port allocation). To change it to static port, follow the guide in github wiki.



Host and Client communicate over the agreed port for the rest of WMI communication. For a new WMI connection, a new port is allocated by the Client.