Departmental Computers and Central Switch

- IT, Sales, Marketing, and R&D Computers: These are individual workstations or computers that are designated for the respective departments within an organization. Each department's computer is connected to a central networking switch, which allows them to communicate with each other and with servers and other devices on the network.
- Central Switch: This is a device that connects multiple computers on a local area network (LAN). It receives, processes, and forwards data to the destination device. In this topology, it serves as a focal point for the department computers and the servers, facilitating intra-network communication and connectivity to the servers.

Servers Connected to the Central Switch

- "Orthanc" - Windows 2019 Server: This is likely the primary server for the network, running Windows Server 2019. It could be hosting a variety of services such as file sharing, print services, domain services, or applications specific to the needs of the organization.
- Server with Wireshark on Kali VM: This server is running Kali Linux, a distribution designed for digital forensics and penetration testing, and it has Wireshark installed on a virtual machine (VM). Wireshark is a network protocol analyzer used to monitor network traffic in real-time or to inspect packets from a saved file. It's a key tool for network troubleshooting and security analysis. This setup indicates that the network has a dedicated resource for monitoring and analyzing network traffic to ensure security and proper functioning.

Satellite Office pfSense Router

- Satellite Office pfSense Router: This router, equipped with pfSense software, provides network routing, firewall protection, and possibly other network services such as VPN, DHCP, and DNS to the local network. pfSense is known for its reliability and a broad range of features.

VPN Tunnel and Remote Connectivity

- VPN Tunnel: A Virtual Private Network (VPN) tunnel is established between the Satellite Office pfSense Router and an unspecified router at a remote location. This encrypted tunnel ensures that data transmitted over the internet between these two points is secure from eavesdropping or interception. It's typically used to connect different sites of an organization securely over the internet or to allow remote access to the organization's internal network.

Remote Site Infrastructure

- Router at Remote Site: The diagram doesn't label this device, but it's the termination point for the VPN tunnel on the remote side. It would handle routing and security policies for the network at this location.
- "Minas Morgul" - AWS VPC: This server is part of an Amazon Web Services Virtual Private Cloud, which is a segmented portion of the AWS cloud dedicated to the organization. It can be

configured much like a traditional network that you would operate in your own data center but with the benefits of the AWS cloud infrastructure such as scalability and availability.

- Corporate Backup Server: This server is responsible for backing up the organization's critical data. It suggests a disaster recovery and business continuity strategy by maintaining copies of important data off-site, which in this case, seems to be in a location connected through the VPN tunnel, potentially also within AWS.