Step 1: Understand the current network.

Devices:

- 10 office computers
- 3 servers (Sensitive data).
- 15 employee smartphones and tablets
- 20 IoT (Internet of Things) devices, including printers, security cameras, and smart TVs

Finance department:

- 4 additional computers (Sensitive data).

Step 2: Determine network segments.

Based on the identified devices, we propose dividing the network into four segments:

1. **Corporate Segment:** This segment will include the 10 office computers and potentially some of the employee smartphones/tablets used for general work purposes.
2. **Server Segment:** This critical segment will house the 3 servers containing sensitive data. It will be strictly isolated for maximum security.
3. **Finance Segment:** The 4 finance department computers handling highly confidential financial information will be placed in a separate segment with the highest security measures.
4. **IoT Segment:** This segment will group all 20 IoT devices (printers, security cameras, smart TVs) due to their potential vulnerabilities and limited access needs.

Step 3: Network Segmentation Plan

Segmentation Implementation: Each network segment will be isolated using VLANs (Virtual LANs). VLANs logically separate devices on the same physical network, creating secure broadcast domains.

Firewall Protection: Firewalls will be implemented at the following points:

- Internet Gateway: A primary firewall will filter all incoming and outgoing traffic at the internet gateway, protecting the entire network from external threats.
- Inter-segment Firewalls: Additional firewalls will be placed between segments to control traffic flow. Traffic will be allowed only based on predefined rules. For example, the Server and Finance segments might only allow access from authorized devices within the network. The Corporate segment firewall might allow access to the internet and specific resources on the Server and Finance segments based on user permissions.
- DMZ (optional): If needed, a Demilitarized Zone (DMZ) can be established to host specific servers that require controlled access from the internet, further enhancing security for critical resources.

Step 4: Potential Benefits and Drawbacks

Benefits:

- Enhanced Security: Segmentation isolates sensitive data and critical systems (servers, finance) from everyday activities on the corporate network. This reduces the attack surface and potential damage from breaches.
- Improved Performance: Separating traffic can optimize network performance by reducing congestion, especially with bandwidth-intensive devices like security cameras.
- Compliance: Segmentation can help meet industry regulations and data privacy requirements for handling sensitive information.

Drawbacks:

- Increased complexity: Managing multiple segments and firewalls requires additional expertise and resources.
- Potential communication limitations: Careful firewall rule configuration is necessary to ensure authorized communication between segments while maintaining isolation.

Step 5: Summary

This network segmentation plan proposes dividing Sam's Scoops headquarters network into four segments: Corporate, Server, Finance, and IoT. VLANs and strategically placed firewalls will create secure boundaries between segments. While some increase in management complexity is expected, the significant security benefits and potential performance improvements outweigh the drawbacks. This plan provides a solid foundation for a more secure and efficient network infrastructure.

Additional Considerations:

- User Access Control: Implementing strong user authentication and authorization mechanisms is crucial to control access to sensitive data and resources within each segment.
- Network Monitoring: Continuous monitoring of network activity within each segment is essential for early detection of suspicious behavior or potential security breaches.
- Security Awareness Training: Educating employees about cyber threats and best practices for secure network usage is vital for a holistic security strategy.

Following this plan and incorporating these additional security measures will significantly enhance the overall security posture of Sam's Scoops network.