## Design Goal:

The objective of this network is to create a secure, reliable, and efficient network infrastructure for a small-to-medium enterprise. This set up ensures easy connectivity among departments while also enforcing access controls. The network is also designed for scalability by using modular architecture and subnetting techniques.

## Assumptions:

* The organization has three departments: IT, HR, and Infrastructure.
* Each department requires its own subnet and VLAN for segmentation and security.
* A basic firewall is implemented using an ASA 5505 to separate internal and external networks.
* Devices are statically assigned IPs where needed; DHCP may be configured in the future.
* Users require access to internal resources (like printers, DNS) but limited internet exposure.

## Network Overview:

The core of the network consists of:

* **Router (R1)**: Cisco 2911, provides gateway and routing between subnets.
* **Switches (S1 & S2)**: Cisco 2960s assigned to VLAN 10 (HR) and VLAN 20 (IT) respectively.
* **Firewall (ASA1)**: Cisco ASA 5505 with inside (G1/1) and outside (G1/2) interfaces securing traffic flow.
* **End Devices**: PCs, printers, laptops, and smartphones spread across VLANs.
* **Server**: DNS server to support name resolution within the local network.

A diagram of a computer network

AI-generated content may be incorrect.

Security Objectives:

* **Segmentation**: VLANs restrict broadcast domains and segment departments logically.
* **ACLs**: Standard or extended ACLs control access between VLANs and the outside world.
* **Port Security**: Enabled on S1 and S2 to prevent unauthorized MAC addresses from connecting.
* **Secure Management**: SSH access to R1 and switches configured with encrypted passwords for CLI access.
* **Firewall Rules**: ASA1 uses access rules to inspect and control inbound/outbound traffic, ensuring only permitted services pass through.

## Additional Notes:

* DNS is operational for name resolution, vital for connectivity and ease of access.
* Wireless connectivity is available through a WAP, supporting mobile devices like SmartPhone1.

## Summary:

This network design delivers a secure, reliable, and scalable infrastructure. It provides logical segmentation through VLANs, secure access control via ACLs and firewall rules, and strong administrative protection with SSH and encrypted credentials. The modular layout allows for future expansion, whether through new departments, IoT integration, or cloud connectivity. The design aligns with cybersecurity best practices and prepares the organization for both current operations and future demands.