Network setup is for an enterprise called Insightful Pursuit, a missing person agency that specializes in locating and reuniting missing individuals with their families. The agency uses advanced technology and databases to assist in their search and communication efforts. Here's how the network setup might align with the agency's operations:

Devices: 5 employee workstations (PCs\ laptops), 3 Smartphones, 1 printer, 1 video conferencing device, 1 public web server, NS server, Syslog server. Networking equipment (routers, switches)

- The devices connect to the LAN both wired and wirelessly. The public web server has a wired connection.
- Two routers and two switches to be used (all CISCO products) as well as a DNS server, webserver and syslog server for the internal network. One switch and a server with DNS and DHCP will be in the external network.
- IP addressing scheme for your internal network:
    - Intelligence Dept (Subnet 1): 192.168.1.1 - 192.168.1.62
    - IT and Cybersecurity (Subnet 2): 192.168.1.65 - 192.168.1.126
    - VLAN 30 (Subnet 3): 192.168.1.129 - 192.168.1.190
    - DMZ network: 192.168.2.2 - 192.168.2.253
- Subnetting is used to allocate IP addresses efficiently to each department and the DMZ zone. DHCP is configured to automatically assign IP addresses to host devices, simplifying network management.
- Four network segments: three internal subnets and one DMZ network. The internal network segments and the DMZ network will be separated by routers.
- The company connects to the Internet through a NAT router that connects the internal network and the DMZ network to the external network.
- Services provided on the network:
    - DHCP: A DHCP server has been configured to automatically assign IP addresses to devices on the internal network.
    - DNS: A DNS server has been configured to resolve domain names to IP addresses for both internal and external access.
    - Packet sniffing: A network monitoring tool or device may be used to analyze network traffic for security and troubleshooting purposes
- The internal network is divided into three VLANs for each department, providing segmentation and security.
- 3 departments: Intelligence (vlan10), IT Cybersecurity (vlan20) and a Secret department (vlan30).
- Each department has a wireless network for the users.
- Host devices in the network obtain IPv4 address automatically.
- Devices in all departments can communicate with each other, allowing for collaboration and sharing of resources.

- NAT is used to enable internet access for internal devices while preserving public IP addresses.
- Routing and External Connectivity:
    - RIP is enabled for dynamic routing, allowing the internal router to exchange routing information with other RIP-enabled routers, including the external router.
    - The setup facilitates communication between the internal network, the DMZ, and the external network or the internet, ensuring connectivity for all network segments.
- Security:
    - An ACL named NAT_ACL is used to control which internal IP addresses can use NAT, providing an additional layer of security. ACL BLOCK_MALICIOUS has a list of known malicios ip and is set to block.
    - A banner message of the day (MOTD) is set to warn against unauthorized access, enhancing security awareness.
    - Backups: cloned devices in a daily routine for backup.
    - To access the CLI you will need the password cisco@123 and cisco.
    - **Enhanced Security Features: Configured IOS Intrusion Prevention System (IPS)**

  The `externalrouter`, has been configured using the Intrusion Prevention System (IPS) to enhance network security by detecting and preventing malicious traffic. Here's how IPS is configured and used in this setup:

  1. IPS Configuration: IPS Packet Scanning

  The IPS rule named iosips is configured. The iosips rule is applied to inbound traffic on the GigabitEthernet0/0 interface and outbound traffic on the GigabitEthernet0/1 interface.

  The fail-closed mode is enabled, meaning that if the IPS encounters an error, it will block all traffic to prevent potential security threats from slipping through.

  General SEAP Config: The Global Deny Timeout is set to 3600 seconds, meaning that if an attack is detected, the offending traffic will be blocked for this duration. Both Global Overrides and Global Filters are enabled, allowing for customization of signature behavior and filtering of events.

  IPS Syslog and SDEE Notification Status:Event notification through both syslog and SDEE (Security Device Event Exchange) is enabled, allowing for logging and monitoring of IPS events.

  2. IPS Application to Interfaces:

  interface GigabitEthernet0/0: The IPS rule `iosips` is applied to inbound traffic on this interface (`ip ips iosips in`). Additionally, Context-based Access Control (CBAC) is also applied to inspect HTTP traffic (`ip inspect ALLOWED_TRAFFIC in`).

  interface GigabitEthernet0/1: The IPS rule `iosips` is applied to outbound traffic on this interface (`ip ips iosips out`). CBAC is also applied to inspect HTTP traffic (`ip inspect ALLOWED_TRAFFIC out`). Furthermore, an Access Control List (ACL) named `BLOCK_MALICIOUS` is applied to inbound traffic to block specific malicious IP addresses.

  3. Security Features to Prevent Attacks:

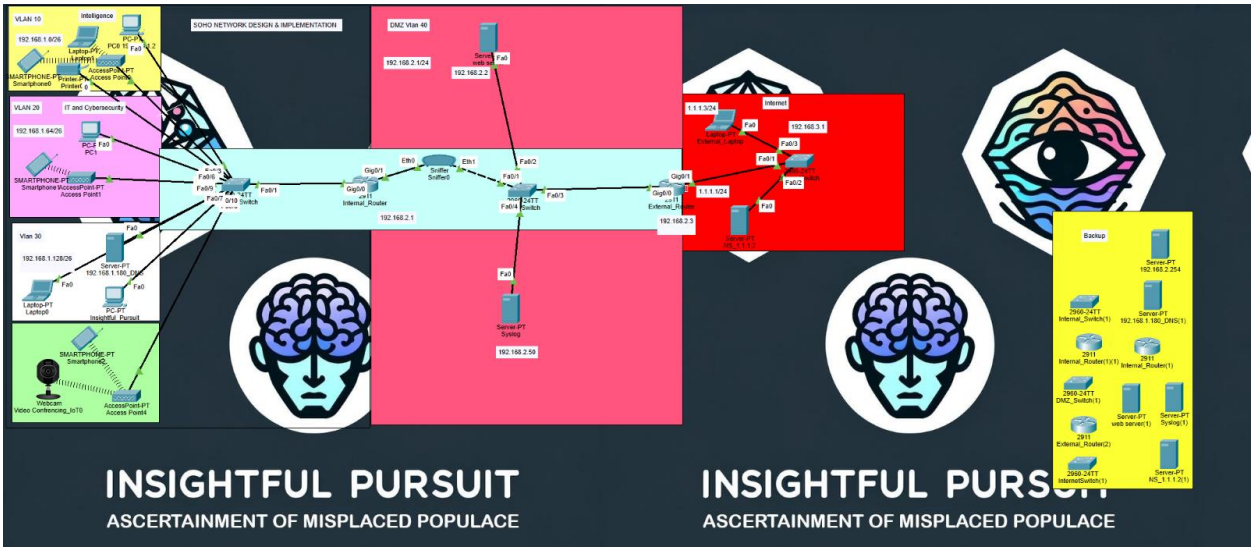
  IPS: The IPS (`iosips`) monitors traffic for malicious patterns based on its active signature category (`ios_ips basic`) and takes action to block or alert on detected threats, providing real-time protection against attacks.

  IP inspect Context-based Access Control CBAC is configured to inspect HTTP traffic for security purposes, helping to protect against web-based threats.

ACLs: The `BLOCK_MALICIOUS` ACL blocks traffic from specific known malicious IP addresses, reducing the risk of attacks from these sources. The `ALLOW_ICMP_HTTP` ACL allows ICMP echo replies and HTTP traffic while blocking other types of traffic, limiting potential attack vectors.

By combining IPS, CBAC, and ACLs, this configuration provides a multi-layered security approach to detect, prevent, and mitigate various types of attacks, including DDoS attacks, without significantly compromising network performance.

Network Design:



All devices can access the company's webpage using the URL of http://www.company.com.