Hajoca Corporation Network

Larry Baucum and Timothee Andre

Bowie State university

CTEC 345

Dr. Latson

Addressing scheme

HQ: 28.185.0.1

Warehouse: 28.185.32.1

Subsidiary example:28.185.64.1

DMZ:28.185.4.1

Subnet 255.255.0.0

HQ Departments

28.185.5.0, 28.185.6.0, 28.185.7.0, …

Endpoints

Desktops, tablets, phones, and VOIP

Network devices

Next generation firewall, edge routers, isp routers, core switches, department switches, and access points.

Servers

DNS, DHCP, RAS, NPS, IPAM, DFS, and web servers.

Layout of the entire network

A computer screen shot of a diagram

Description automatically generated

A diagram of a network

Description automatically generated

A diagram of a computer network

Description automatically generated

A diagram of a computer network

Description automatically generated

A diagram of a router

Description automatically generated

To design a network for a company with 1,800 employees, 400 subsidiaries, and over 500 suppliers, with a focus on security, HQ, and a product warehouse, along with different departments and customer segments, we need to create a network architecture that ensures efficient communication, scalability, and security. Below is a proposed network architecture:

**Network Architecture Overview:**

* **HQ Location**: Headquarters with different departments and executive offices.
* **Product Warehouse**: Central location for product storage and distribution.
* **Subsidiaries**: 400 subsidiary locations that need to communicate with HQ.
* **Suppliers**: Over 500 suppliers who may need access to specific resources.
* **Customer Segments**: Residential, Entrepreneurial, and Industrial customers.

**Network Segmentation:**

1. **HQ Network**:
   * **Subnets**: Divide into subnets for each department (executives, sales, operations, marketing, finance, HR, IT, customer service, product management, quality assurance, legal).
   * **IP Addressing**: Assign IP addresses based on subnetting scheme (e.g., 10.0.0.0/24 for each department).
   * **Intermediary Devices**: Core switches, routers, firewalls.
   * **Security Appliances**: Next-generation firewalls (NGFW), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS).
2. **Product Warehouse Network**:
   * Similar to HQ network structure with appropriate subnets and security measures.
   * Separate subnets for inventory management, logistics, and security cameras.
3. **Subsidiary Networks**:
   * **VPN Connectivity**: Use VPN tunnels for secure communication with HQ.
   * Each subsidiary to have its own subnet and security measures.
4. **Supplier Networks**:
   * **DMZ**: Create a demilitarized zone (DMZ) for suppliers to access specific resources.
   * Secure VPN connections for remote suppliers.
   * Separate subnet(s) for supplier access.
5. **Customer Segments**:
   * Separate subnets for residential, entrepreneurial, and industrial customers.
   * Limited access to internal resources based on customer segment.

**End Devices and Intermediary Devices:**

* **End Devices**: PCs, laptops, servers, printers, IP phones, etc.
* **Intermediary Devices**: Core switches, distribution switches, routers, firewalls, access points.