Benyahir Y. Martínez Hermina R00624824

Actividad 3 – Modulo 4 – Lección 3

Instrucciones:

1. Análisis de un Escenario: Imagina que eres el encargado de diseñar la seguridad de red de una empresa que tiene un centro de datos y empleados que trabajan de forma remota. Describe los componentes de seguridad en red que implementarías y explica por qué son necesarios en este caso.

   Componentes de seguridad que se estarían implementando:

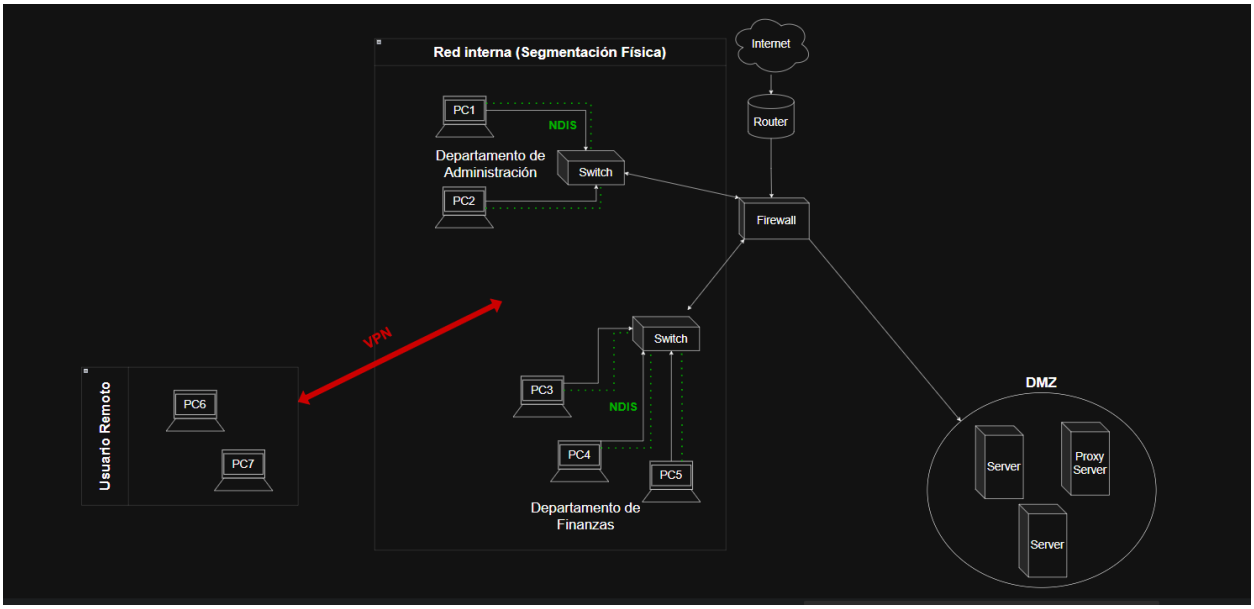
   - Firewalls: Este sistema monitorearía y controla el tráfico de que entra y salen en base a unas reglas establecidas. Protegería la red interna de la empresa de cualquier acceso no autorizado que proviene del internet.

   - VPN: Les ofrece a los empleados de la empresa que trabajan de manera remota una forma de conectarse a los sistemas de esta mediante una comunicación encriptada a través de redes públicas.

   - DMZ: Esta subred dividiría las redes internas de las externas de la empresa lo que les facilitaría proveer ciertos servicios específicos a sus empleados sin que alguna amenaza entre directamente a la red interna.

   - NIDS: Servicio que monitorea el tráfico que entra al sistema para detectar la amenaza que está afectando a la empresa para que esta pueda tomar las acciones necesarias para detenerla.

2. Diagrama de Arquitectura Segura: Dibuja un diagrama básico que incluya los componentes que utilizarías para proteger la red de una empresa, incluyendo firewall, VPN, DMZ, segmentación de red y NIDS. Puedes hacer el diagrama a mano y luego digitalizarlo.



3. Evaluación de Amenazas: Investiga las posibles amenazas de red para una empresa pequeña. Describe tres tipos de ataques de red que podrían afectar la seguridad y qué medidas implementarías para mitigarlos.

    - DoS/DDoS: Amenaza que satura el servicio lo que bloquea el intento de accesos válidos. Para mitigar este tipo de amenaza se utilizaría firewalls configurados para limitar el tráfico que produce esta amenaza.

    - Malware y ransomware: Este tipo de amenaza infectan los sistemas para robar los datos que están adentro de estos y a veces pedir dinero para la recuperación. La medida que utilizaría para mitigar la amenaza viene en la forma de un antivirus que detecta y elimina software malicioso que se encuentra en el sistema.

    - Phishing y spear phishing: Viene en la forma de emails engañosos que son utilizados para robar la información de los usuarios que responden a estos. La mitigación de esta involucraría el entrenamiento de los empleados para lidiar con esta situación, filtros de antispam y sistemas de autentificación de multifactor.