

EXERCICI 1 –RESOLUCIÓ- (25%)

- a. Descriu en què consisteix la segmentació de xarxa i què aporta en termes de seguretat. Amb aquesta arquitectura i les funcionalitats d'aquests equipaments. (20%)**

La segmentació de la xarxa és una tècnica de seguretat de la xarxa que consisteix en dividir-la en diferents subxarxes més petites, que permeten als equips de xarxa compartimentar-les i atorgar controls i serveis de seguretat únics a cada una.

Segmentar la xarxa limita l'extensió d'un atac i redueix la superfície d'atac.

La segmentació proporciona una manera lògica d'aïllar un atac actiu abans que es propagui per la xarxa. Per exemple, la segmentació garanteix que un programa maliciós en un segment no afecti els sistemes d'un altre.

Quan una xarxa àmplia es divideix en subxarxes més petites i s'aïlla el trànsit entre aquestes, es redueix la superfície d'atac i impedeix el desplaçament lateral. Per tant, si es vulnera el perímetre de la xarxa, els segments de la xarxa eviten que els atacants es desplacen lateralment a l'interior.

- b. Desenvolupa una estratègia de segmentació de xarxa que incrementi la seguretat. (80%)**

Amb aquest equipament es pot implementar una estratègia de segmentació de xarxa utilitzant la funcionalitat ACL ("Acces Control List") al router de distribució. (4/10)*

Una ACL és una llista seqüencial d'instruccions *permit* (permetre) o *deny* (denegar), conegudes com a "entrades de control d'accés" (ACE) o "instruccions d'ACL". El router que ha d'encaminar el tràfic ho fa en funció d'un procés denominat filtratge de paquets, i només encamina el tràfic que està permès, descartant el denegat. (2/10 descripció de la funcionalitat ACL)

Al switch/router de distribució es poden crear ACLs per cada departament/VLAN/xarxa IP classe C, de manera que només estigui permès el tràfic cap als servidors necessaris o cap a internet, denegant el tràfic cap a la resta de departaments/VLANs o xarxes C. (2/10 descripció del mecanisme a implementar)

*És important que les ACLs es configurin al router de distribució. No es poden configurar als routers d'accés, perquè les funcions de capa L3 només estan al router de distribució segons l'enunciat, entre d'altres motius.
