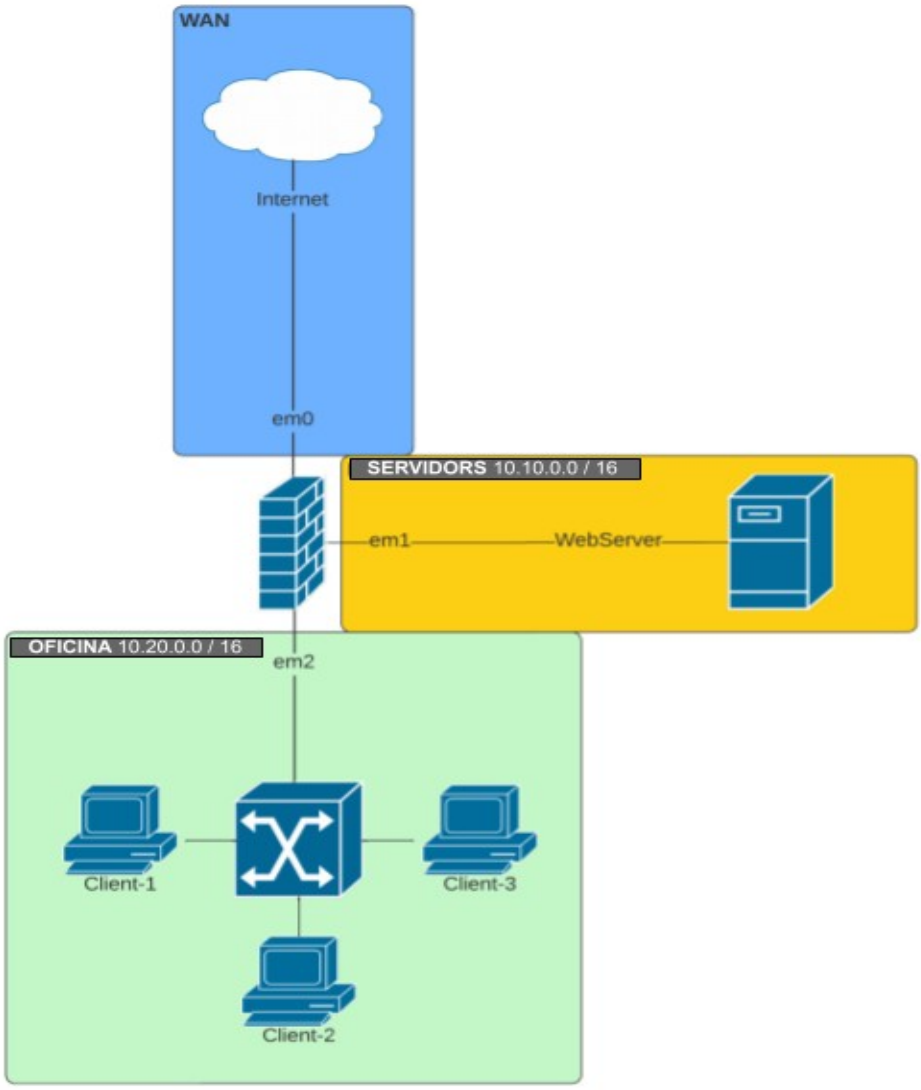
RECUPERACIÓ UF3 (pfSense)

ESTUDIS:	ASIX			CURS:	2n
MATÈRIA:	Seguretat i Alta Disponibilitat	GRUP:	A	DATA:	
ALUMNE:					

L'objectiu és configurar un firewall pfSense amb polítiques de seguretat estrictes i assegurar que només el trànsit autoritzat pugui passar.

Inclou captures de pantalla on es mostri la feina feta, les captures han de mostrar que s'ha fet i la validació de que funciona. Inclou explicacions clares de cada procediment i justificacions de les decisions preses.



Serveis necessaris pel servidor:

- ➔ Web (HTTP/HTTPS): Instal·la Apache o Nginx.
- ➔ SSH: Instal·la i activa OpenSSH.

RECUPERACIÓ UF3 (pfSense)

1. Mostra la configuració de xarxa realitzada a tots els equips des de la seva respectiva terminal. Assigna el hostname indicat a cada equip.

   Mostra la configuració de zones des del PfSense.

2. Crea un nou usuari. El username ha de ser el teu nom, ha d'incloure descripció i ha de pertànyer al grup «admins».

   Crea un grup per usuaris amb permisos limitats a la comprovació de l'estat de la interfície de xarxa, crea un segon usuari i afegeix-lo a aquest grup.

3. Utilitza àlies en lloc d'IPs per centralitzar les dades fa més mantenible el sistema. Afegeix i usa l'àlies «Server1» per identificar el servidor de la zona «SERVIDORS» a les regles.

4. Configura el servidor DHCP de la zona OFICINA perquè assigni IPs entre 10.20.1.20 i 10.20.1.200.

   Per qüestions de seguretat incorporem les següents mesures:

   - Restringim les MAC que es poden connectar a la xarxa. Demostra-ho.
   - Impedim l'accés a la xarxa amb IP estàtica. Demostra-ho.

   Demostra que has obtingut una IP a través de DHCP.

   Quin avantatge creus que té bloquejar MACs no autoritzades?

   A «Client-3» assigna-li una IP estàtica adequada, dins del rang de la xarxa però fora del rang del servidor DHCP.

5. Afegeix inspecció de paquets i logs:

   - Configurar pfSense per registrar el tràfic rebutjat i analitzar logs.
   - Com poden detectar intents d'accés no autoritzats?

6. Simula un atac de força bruta al servidor (per exemple amb nmap).

   Quin és el resultat? Ho pots detectar des del PfSense? Com pots protegir la xarxa?

7. pfSense té un bloqueig implícit dels paquets que no encaixen en cap regla. Realitza un bloqueig explícit dels paquets que no encaixen en cap regla.

   - Configura pfSense per permetre els següents fluxos de trànsit:
     - Accés web intern
       - Permetre HTTP (port 80) des de OFICINA al servidor de SERVIDORS.
       - Permetre HTTPS (port 443) des del Client-3 de OFICINA al servidor de SERVIDORS.
     - Accés SSH restringit
       - Només el client autoritzat Client-3 de OFICINA pot accedir via SSH (port 22) al servidor de SERVIDORS.
     - Monitorització entre servidors
       - SERVIDORS pot fer ping (ICMP) a OFICINA per verificar connectivitat.
     - Accés extern a serveis interns
       - Des de WAN, permetre accés HTTP (80) i ICMP només al servidor de SERVIDORS.
     - Navegació a Internet
       - OFICINA només pot sortir a Internet via HTTPS (port 443).
     - Diagnòstic des de SERVIDORS
       - SERVIDORS pot fer ping (ICMP) a servidors externs a través de la WAN per provar la connectivitat.
     - Accés d'administració des de WAN
       - Només el PC amfitrió de la WAN pot accedir a la pàgina de configuració de pfSense (port 443 o 80).
   - Afegir bloquejos explícits per assegurar la seguretat de la xarxa:
     - Client-3 de OFICINA no pot accedir a WAN per cap protocol.
     - Tot el que no s'indiqui com a permès ha d'estar prohibit. Utilitzarem «Block» per les comunicacions on intervingui la WAN i «Reject» quan només intervingui OFICINA/SERVIDORS. Per què creus que fem servir "Block" per la WAN i "Reject" per OFICINA/SERVIDORS?

   Demostra la connectivitat o bloqueig de paquets que provoca cada regla. Per comprovar que les regles funcionen, realitza aquestes proves i adjunta captures:

   - ping per validar connexions ICMP.
   - curl o wget per provar connexions HTTP/HTTPS.
   - ssh per verificar connexió remota entre equips.
   - nmap per detectar serveis accessibles des de les zones OFICINA, SERVIDORS i WAN.