

### **Pràctica 3: Servidors intermediaris**

Els objectius de la pràctica **m11uf2pr3** són:

- a) Coneixer els conceptes bàsics sobre servidors intermediaris
- b) Treballar amb el servidor intermediari **Squid**.

#### **DOCUMENTACIÓ**

##### 1- Definició:

Actua com intermediari entre un client i el servidor amb el qual vol connectar-se. Les peticions d'accés del client les rep el servidor intermediari i les canalitza cap al servidor al qual es fa la petició. Des del punt de vista del servidor extern, és el proxy qui ha fet la petició.

Els proxy a diferència dels routers, treballen normalment a nivell d'aplicació (HTTP, FTP, SSH...) o també ARP.

##### 2- Avantatges:

a) Múltiples peticions d'accés a un determinat recurs d'un servei des de múltiples clients es poden realitzar per mitjà del proxy. El proxy:

- a) Pot mantenir en memòria el recurs sol·licitat de manera que els clients accedeixen al recurs que es troba al proxy a velocitat de xarxa local i no es col·lapsa l'accés a internet
- b) Per distribuir dades a clients d'una xarxa, es pot descarregar una sola vegada al proxy i des del proxy, distribuïr-los als clients. Cas típic: Actualitzacions
- c) Millorar la velocitat de resposta dels serveis
- d) Filtratge: Accés recursos determinats, filtratge de correus, de perfils d'usuaris...
- e) Emmascarament d'identitat
- f) Continguts a demanda --> Modificació de la presentació de la informació. Per exemple, el proxy pot enviar les dades de manera diferent si el client és un mòbil, tauleta, PC, Firefox, Safari,....
- g) Registre d'esdeveniments

##### 3- Tipus més importants:

a) Servidors web proxy --> Fan de proxy per HTTP. Permeten tenir memòria cau, eviten una baixada de la velocitat d'internet quan es realitzen moltes connexions a la web i permeten millorar la velocitat d'accés al recurs web molt sol·licitat. S'ha d'anar amb compte d'actualitzar la memòria cau.

b) Servidor DNS proxy: Intermediari entre peticions dels clients i el servidor DNS extern. Té memòria cau.

b) Servidor intermediari proxy: Obert no només a un protocol sino també a altres protocols de nivell d'aplicació

c) Servidor intermediari transparent: Aquell que treballa sense que l'usuari hagi de realitzar cap configuració del client.

d) Serv. interm. invers --> intercepta el tràfic de l'exterior cap un servidor intern. Això permet augmentar la seguretat i millorar l'accés sumministrant balanceig de carrega per exemple. També pot tenir memòria cau.

##### 4- Diferència NAT-Proxy:

NAT treballa a nivell 3 (xarxa) model OSI (IP del TCP/IP) i proxy bàsicament a nivell d'aplicació (HTTP, SSH, FTP, DNS...). NAT requereix menys recursos però és menys flexible (menys configurable).

##### 5- Serv Proxy més coneguts: Squid, Ziproxy, Polipo, WinGate

##### 6- Squid:

Permet l'accés web a màquines privades que no estan connectades directament a Internet.

Registra el trànsit web que surt de la xarxa local.

Controla l'accés web utilitzant regles.

Funciona com a memòria cau de pàgines web.

Controla el contingut web consultat.

Controla les descàrregues que es realitzen.

Implementa una memòria cau per a les connexions fallides.  
Emmagatzema en la memòria cau les peticions DNS.  
És compatible amb el protocol ICP.  
Registra totes les peticions realitzades.

#### 7- Directoris i fitxers important de Squid

**/usr/bin/**: directori executable  
**/var/run/**: directori amb el PID del procés  
**/var/log/squid/**: directori de registres  
**/var/spool/squid/**: directori de memòria cau  
**/etc/squid/**: fitxers de configuració  
**/usr/lib/squid/**: complements  
**/usr/share/doc/squid/**: documentació

#### 8- Els paràmetres més importants de Squid són:

**http\_port**: indica el port que s'utilitzarà per escoltar el servidor. Per defecte aquest valor és 3128.

- **cache\_mem**: defineix la memòria RAM que s'utilitzarà per emmagatzemar les dades que més se sol·licitin.
- **cache\_swap\_low**: indica el nivell d'espai mínim que s'ha de mantenir en l'àrea d'intercanvi.
- **cache\_swap\_high**: indica el nivell d'espai màxim que s'ha de mantenir en l'àrea d'intercanvi.
- **maximum\_object\_size**: indica la mida màxima que poden tenir els objectes que s'emmagatzemen en la memòria cau.
- **hierarchy\_stoplist**: indica els caràcters que s'utilitzaran com a filtre. Si els caràcters es detecten en una adreça web es carrega directament el contingut des de la memòria cau.
- **visible\_hostname**: indica el nom de l'equip.
- **cache\_dir**: estableix la mida que es reservarà en el disc per a la memòria cau.
- **access\_log**: indica el directori en què s'emmagatzemaran els accessos a Squid.
- **cache\_log**: estableix la ruta en què s'emmagatzemaran els missatges de *log* d'Squid.

### **PRÀCTICA**

#### 1- Instal·la **Squid** sobre **Kali Linux**.

#### 2- Fes les següents tasques:

- a) Posa en marxa una màquina Ubuntu treballant amb xarxa interna i configura-la amb l'adreça IP 192.168.2.2 i màscara 255.255.255.0, IP del router 192,168.2.1 i DNS 80.58.0.33.
- b) Posa en marxa una màquina Windows treballant amb xarxa interna i configura-la amb l'adreça IP 192.168.3.2 i màscara 255.255.255.0, IP del router 192,168.3.1 i DNS 80.58.0.33.
- c) Comprova que els 2 equips poden navegar per mitjà de la connexió amb Kali i la configuració NAT del firewall ufw. Atura el firewall ufw i comprova que ara no poden navegar.
- d) Comprova que els 2 equips tenen dins del seu fitxer hosts el nom i adreça IP del servidor amb Squid

3- Inicia **Squid** i comprova quin és el seu port inicial. Canvia el port pel qual escolta **Squid** i fes que sigui el **8080**. Hauràs de modificar la directiva **http\_port** pel nou valor i reiniciar **Squid**. Compte que pot trigar uns **30-40** segons en reiniciar-se. Comprova que la nova configuració ha tingut efecte

4- A la secció de "**Recommended minimum configuration**" afegeix **ACLs** per **donar permís d'accés** als ordinadors de les xarxes **192.168.2.0/24** que serà identificada com **xarxalocal1** i **192.168.3.0/24** que serà identificada com **xarxalocal2**. Per treballar amb les regles de l'ACLs llegeix la seccions **2.3.4** i **2.3.5** de:

[https://ioc.xtec.cat/materials/FP/Materials/2251\\_ASIX/ASIX\\_2251\\_M11/web/html/WebContent/u3/a2/continguts.html](https://ioc.xtec.cat/materials/FP/Materials/2251_ASIX/ASIX_2251_M11/web/html/WebContent/u3/a2/continguts.html)

5- Configura el teu navegador d'Ubuntu i Windows per treballar amb el servidor intermediari Squid. Comprova:

- a) Que no tens connexió a **www.collados.org** i **www.binefa.cat**. Executa ping i comprova que no hi ha resposta.
- b) Fes una connexió des del navegador i comprova que pots accedir als 2 llocs esmentats per mitjà del servidor intermediari Squid.

6- Atura Squid. Comprova que ara no pots navegar i que no pots accedir als 2 llocs als qual si ho has pogut fer la vegada anterior. Comprova el missatge donat pel navegador.

7- Comprova l'estat del directori **/var/spool/squid/**. Troba dins de la memòria cau la web inicial de **www.collados.org** i **www.binefa.cat**.

8- Amb la informació que trobaràs a **2.3.5** de la documentació sobre proxys d'IOC o també [aquí](#), prohibeix l'accés al domini **fje.edu**. Comprova que no es pot accedir al domini indicat.

#### **Forma de lliurament**

1- Data: **24-3-17** a les **18.00h**

- a) **Comprovació 2 --> No connexió a internet dels 2 equips**
- b) **Comprovació port Squid**
- c) **Comprovació de navegació dels equips clients amb i sense configuració de proxy**
- d) **Comprovació de navegació dels equips clients amb el proxy iniciat i aturat**
- e) **Comprovació de la memòria cau**
- f) **Comprovació que a la memòria cau es troben les pàgines inicials de collados.org i binefa.cat**
- g) **Comprova que no es pot accedir cap web del domini de fje.edu.**