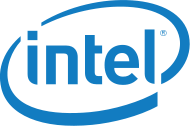
**Implementare practica :**

**Configurarea și testarea performanțelor certificatelor digitale utilizând serverul web NGINX și clientul Apache Benchmark pe platforma x86**



AB https client

WEB https server



**192.168.136.130**

**192.168.136.130**

**Figura 23** Reprezentarea clientului Apache Benchmark și a serverului web NGINX

Clientul Apache Benchmark este un client single threaded și este folosit, împreună cu serverul web NGINX pentru a testa performanțele certificatelor digitale. În cadrul acestei lucrări, serverul web NGINX va rula pe un singur core, distribuția pe multicore nefuncționând corect. Serverul web NGINX („engine x”) este caracterizat prin :

* Securitate
* Rapiditate
* Eficiență

În comparație cu Apache, Lighttpd sau thttpd, NGINX este mai eficient și oferă mai multe opțiuni pentru configurare [13].

Pentru atingerea scopului propus, adică pentru testarea performanțelor certificatelor digitale utilizând algoritmiul RSA, se generează o cheie privată de tip RSA și un certificat digital.

Este necesară configurarea serverului NGINX, localizat în /etc/nginx/nginx.conf, specificându-se portul https 443. Totodată este necesară specificarea numelui fișierelor unde este stocată cheia privată și certificatul digital. *SSL\_chiphers* în cazul utilizării algoritmului RSA este *AES128- SHA,* conform listei de ciphere care se poate accesa online [10]. *SSL\_protocols* specifică tipul de protocol utilizat, în acest caz TLSv1. În cadrul fișierului NGINX este specificat *worker\_processes* ca fiind *1* și *worker\_connections* ca fiind *10* ceea ce înseamnă

Configurarea serverului în cadrul fișierului nginx.conf se realizează astfel :

*events {*

*worker\_connections 10;*

*}*

*server {*

*listen 443;*

*ssl on;*

*ssl\_certificate server.crt;*

*ssl\_certificate\_key server.key;*

*ssl\_ciphers AES128-SHA;*

*ssl\_prefer\_server\_ciphers on;*

*ssl\_protocols TLSv1;*

*}*

După ce fișierul nginx.conf a fost configurat se verifică dacă serverul web este pornit utilizând comanda : *ps –ale | grep nginx.*

Comanda *nginx –c /etc/nginx.conf* menționează utilizarea fișierului nginx.conf la pornirea serverului NGINX.

Preluarea rezultatelor de performanță se va face utilizând clientul Apache Benchmark astfel :

ab –c 1 –n 50000 <https://192.168.135.130:443/file.out>

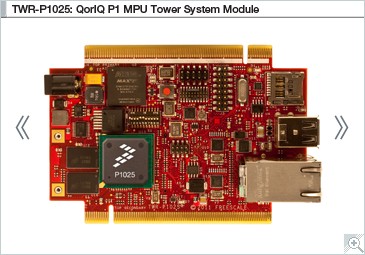
* -n → indică numărul de conexiuni, în acest caz fiind egal cu 50000.
* -c → indică concurența, în acest caz fiind egală cu 1.
* 192.168.135.130 → reprezintă adresa IP a serverului NGINX.
* 443 → portul specific pentru https.
* Fișierul file.out → reprezintă un fișier de dimensiune 1K, dimensiune folosită în cazul testelor de certificate.

Conform comenzii de mai sus, clientul AB generează 50000 de conexiuni securizate către serverul NGINX, rezultatele obținute fiind prezentate în tabelul ... din cadrul capitolului 4.3.

Pentru testarea performanțelor certificatelor digitale utilizând algoritmiul DSA, se generează o cheie privată de tip DSA de 2048 biți și un certificat digital.

Este necesară configurarea serverului NGINX, la fel ca în cazul utilizării algoritmului RSA însă în cazul utilizării algoritmului DSA *SSL\_chiphers* este *HIGH:!aNULL:!MD5,* conform listei de ciphere care se poate accesa online, conform [10].

**Configurarea și testarea performanțelor certificatelor digitale utilizând serverul Web NGINX și clientul Apache Benchmark pe platforma P1025**



AB https client

WEB https server



**192.168.1.3**

**192.168.1.1**

**Figura 23** Reprezentarea clientului Apache Benchmark și a serverului web NGINX

Pentru testarea performanțelor certificatelor digitale utilizând serverul Web NGINX și clientul Apache Benchmark pe platforma P1025 este necesară configurarea platformei QorIQ P1025 astfel încât să fie permisă accesarea unui server https://. Se va realiza configurarea serverului web pe placă, la fel ca și în cazul testelor pe platforma x86, și se vor copia certificatul și cheia privată corespunzătoare. Pe platforma x86 va rula clientul Apache Benchmark și se vor prelua rezultatele de perfomanță în urma rulării astfel :

ab –c 1 –n 50000 <https://192.168.1.1:443/file.out>

Conform comenzii de mai sus, clientul AB generează 50000 de conexiuni securizate către serverul NGINX, rezultatele obținute fiind prezentate în tabelul ... din cadrul capitolului 4.3.

**Rezultate experimentale :**

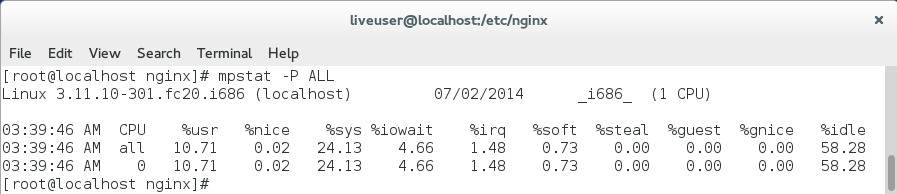
**Testarea performanțelor certificatelor digitale folosind web serverul NGINX și Apache Benchmark**

Pentru testarea performanțelor certificatelor digitale folosind serverului web NGINX și clientul Apache Benchmark s-au urmărit timpii necesari pentru teste. Au fost realizate măsurători pentru un număr de conexiuni egal cu 50000, utilizând diverse dimensiuni ale cheii private generate. Testele de performanță au fost efectuate atât pe platforma Freescale QorIQ P1025E, care folosește un Core la 500 MHz, cât și pe o platformă x86 care folosește un procesor Intel(R) Core(TM) i7-6362QM la 2,2 GHz.

Datorită performanțelor înalte oferite de NGINX instalarea serverului web în cadrul Fedora 13 nu este posibilă și de aceea este necesară utilizarea mașinii virtuale Fedora 20 pentru realizarea testelor pe platforma x86.

**Fedora 20 :**

Încărcarea medie pe procesor, preluată cu comanda *mpstat* (Fedora 20)  *:*



În tabelul 3 s-au obținut rezultatele experimentale, în urma rulării pe o platformă x86, utilizând algoritmul RSA pentru diferite dimensiuni de chei : 1024, 2048 și 4096 și s-au efectuat măsurători pentru un număr diferit de conexiuni egal cu 50000.

**Tabel 3** Rezultatele experimentale obținute pe platforma x86 utilizând RSA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Numărul de conexiuni | **Concurența** | **Timpul necesar pentru teste** | **Request per second** | **Time per request** |
| *RSA 1024* | | | | |
| 50000 | 1 | 259.952 s | 192.34 | 5.199 ms |
| *RSA 2048* | | | | |
| 50000 | 1 | 426.618 s | 117.20 | 8.532 ms |
| *RSA 4096* | | | | |
| 50000 | 1 | 3709.344 s | 11.50 | 86.941 ms |

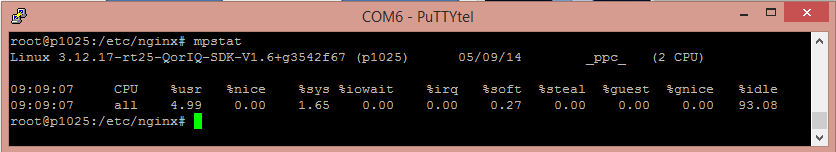
În tabelul 4 s-au obținut rezultatele experimentale, în urma rulării pe o platformă x86, utilizând algoritmul DSA pentru diferite dimensiuni de chei : 1024, 2048 și 4096 și s-au efectuat măsurători pentru un număr diferit de conexiuni : 1000, 5000, 10000 și 50000.

**Tabel 4** Rezultatele experimentale obținute pe platforma x86 utilizând DSA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Numărul de conexiuni | **Concurența** | **Timpul necesar pentru teste** | **Request per second** | **Time per request** |
| *DSA 1024* | | | | |
| 50000 | 1 | 1300.636 s | 38.44 | 26.013 ms |
| *DSA 2048* | | | | |
| 50000 | 1 | 1494.034 s | 33.47 | 29.881 ms |
| *DSA 4096* | | | | |
| 50000 | 1 | 3087.932 s | 16.19 | 61.759 ms |

**Placa :**

În figură este redată încărcarea medie pe procesor, preluată cu comanda *mpstat :*



În tabelul 5 s-au obținut rezultatele experimentale, în urma rulării pe platforma QorIQ P1025, utilizând algoritmul RSA pentru diferite dimensiuni de chei : 1024, 2048 și 4096 . S-au efectuat măsurători pentru un număr de conexiuni egal cu 50000.

**Tabel 5** Rezultatele experimentale obținute pe platforma P1025 utilizând RSA

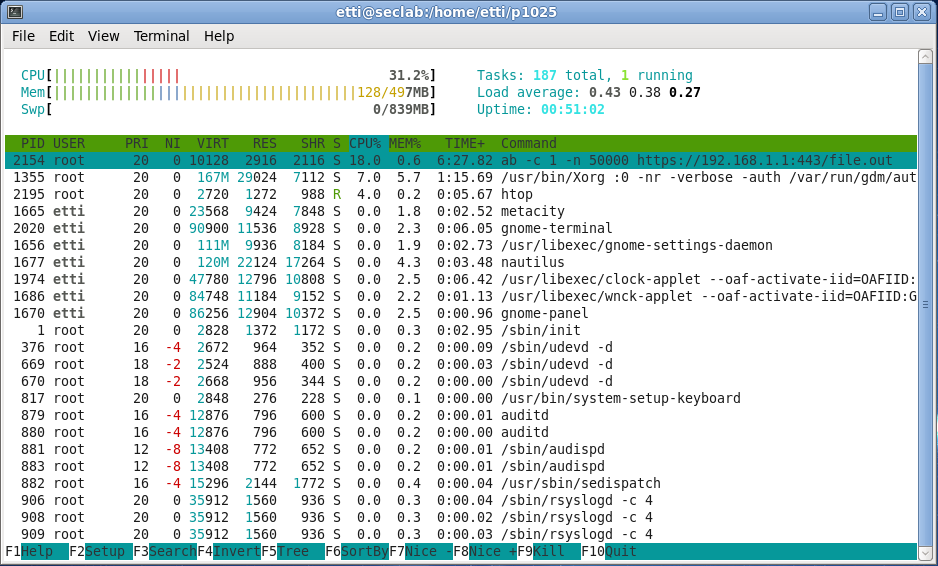
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Numărul de conexiuni | **Concurența** | **Timpul necesar pentru teste** | **Request per second** | **Time per request** |
| *RSA 1024* | | | | |
| 50000 | 1 | 936.217 s | 53.41 | 18.724 ms |
| *RSA 2048* | | | | |
| 50000 | 1 | 4661.913 s | 10.73 | 93.238 ms |
| *RSA 4096* | | | | |
| 50000 | 1 |  |  |  |

În tabelul 6 s-au obținut rezultatele experimentale, în urma rulării pe platforma QorIQ P1025, utilizând algoritmul DSA pentru diferite dimensiuni de chei : 1024, 2048 și 4096 . S-au efectuat măsurători pentru un număr de conexiuni egal cu 50000.

**Tabel 6** Rezultatele experimentale obținute pe platforma P1025 utilizând DSA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Numărul de conexiuni | **Concurența** | **Timpul necesar pentru teste** | **Request per second** | **Time per request** |
| *DSA 1024* | | | | |
| 50000 | 1 | 5505.247 s | 9.08 | 110.105 ms |
| *DSA 2048* | | | | |
| 50000 | 1 | 7220.395 s | 6.92 | 144.408 ms |
| *DSA 4096* | | | | |
| 50000 | 1 |  |  |  |

Rezultatele preluate din Fedora 13 în timpul rulării serverului NGINX utilizând comanda *htop* :

****