May 2021

SYN Flood Attack Mitigating System

punarjeewa abeysekera

SYN Flood Attack Mitigating System

ABSTRACT

This disclosure describes a method to mitigate the type of denial-of-service attack called the SYN flood attack on the web servers. The mitigating system consists of a group of client computers, a group of proxy computers, a group of web servers and a search engine. Each client computer can access only one particular proxy computer in this system and cannot access any other computer in this system. The client computers surf the web while downloading and uploading content via the proxy computers and the search engine. Even with the capability of the client computers to execute a SYN flood attack as in the conventional settings, the system will prevent the client computers from doing so. This is achieved by restricting the reach of the client computers only up to the proxy computers. If ever there could be any SYN flood attack in the system, it will be only between the internet link of the attack executing client computer and its corresponding internet gateway proxy computer. In which case only the internet gateway of the attacking client computer gets obstructed and the rest of the system remains unaffected.

KEYWORDS

SYN flood attack

Denial of service

Client computer

Proxy computer

Search engine

Web servers

Download

Upload

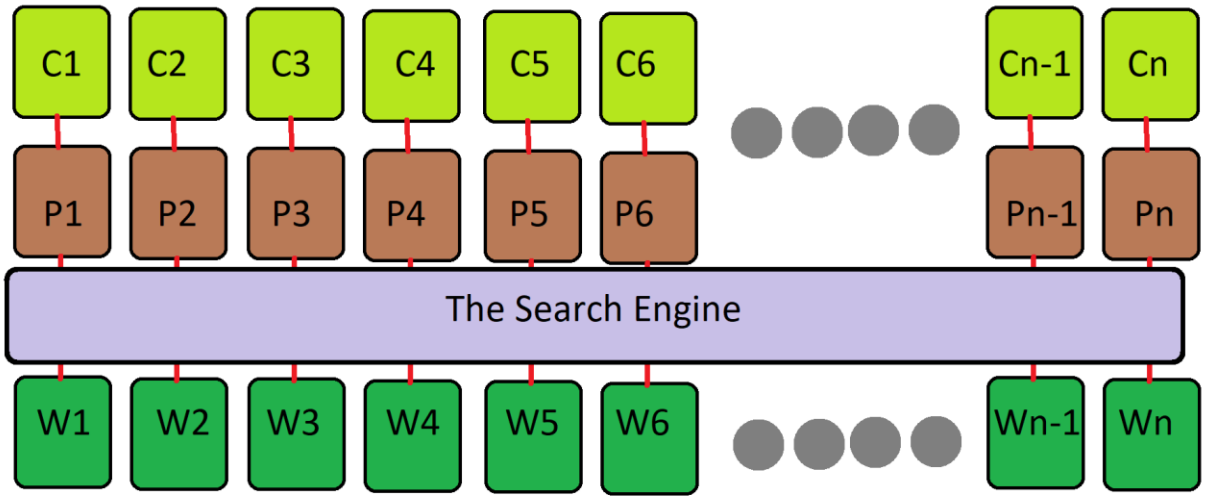
Internet gateway

BACKGROUND

SYN flood attack is a type of denial -of -service attack which will consume all available web server resources. The result of this is making the web server unavailable to legitimate traffic. Several methods of mitigating this type of attack exists. Nevertheless, SYN flood attack remains a challenging denial -of – service attack to handle in the cyber realm.

DESCRIPTION

This paper disclosures a method to mitigate the type of denial-of -service attack called the SYN flood attack. The mitigating system consists of a group of client computers, a group of proxy computers, a group of web servers and a search engine. The logical structure of the system is given below.



The description of the diagram is given below.

The light green color C labelled round rectangles = the group of client computers.

The brown color P labelled round rectangles = the group of proxy computers.

The dark green color W labelled round rectangles = the group of web servers.

Light purple long round rectangle = the search engine

The red links = the network connections between the computing devices in the system.

the entities in the method are given below.

Entity one:

The client computer

The client computer in this system can only access one particular other computer in this system. That is only the corresponding proxy computer. A particular client computer has a pre-installed software which contains only the IP address of one particular proxy computer in the system. And that client computer does not posses any knowledge about IP addresses of other computers (including that of the search engine) in the system.

Entity two:

The proxy computer

The proxy computer in this system is the type of computing entity that can communicate with both the search engine and the web servers. It is also the main internet gateway of the client computer.

Entity three:

The search engine

The search engine does the web search and provides the search results. In addition to that it coordinates the content delivery process.

Entity four:

The web servers

The webservers hold the content that will be delivered to the client computers via the proxy computers.

Requirements for the system:

Requirement one

All the IP addresses of the computers in this system needs to be bitwise large enough so that they cannot be discovered by brute forcing computational methods in a feasible amount of time.

Requirement two

At the beginning of a process, the web servers or the web sites does not have their IP addresses known to any computer both within the system and outside the system except the search engine in the system. In essence this means that except the search engine who knows all the IP addresses of the web servers, any other computer cannot access the web servers since they do not know the IP addresses of the web servers.

Requirement three

The search engine stores the index of all the information of web pages on the web servers for information (search results) providing purposes.

Requirement four

The search engine knows all the proxy computers IP addresses.

Requirement five

Each proxy computer knows the particular IP address of the search engine, they use to connect with the search engine.

Requirement six

Each client computer knows only the IP address of the corresponding proxy computer it is allowed to connect as its internet gateway. Other than that, they do not know any IP address of any other computer in this system.

Requirement seven

Each proxy computer knows only the IP address of the corresponding client computer to which it acts as the internet connecting gateway.

The method consists of two main procedures. They are the download procedure and the upload procedure. They are described below.

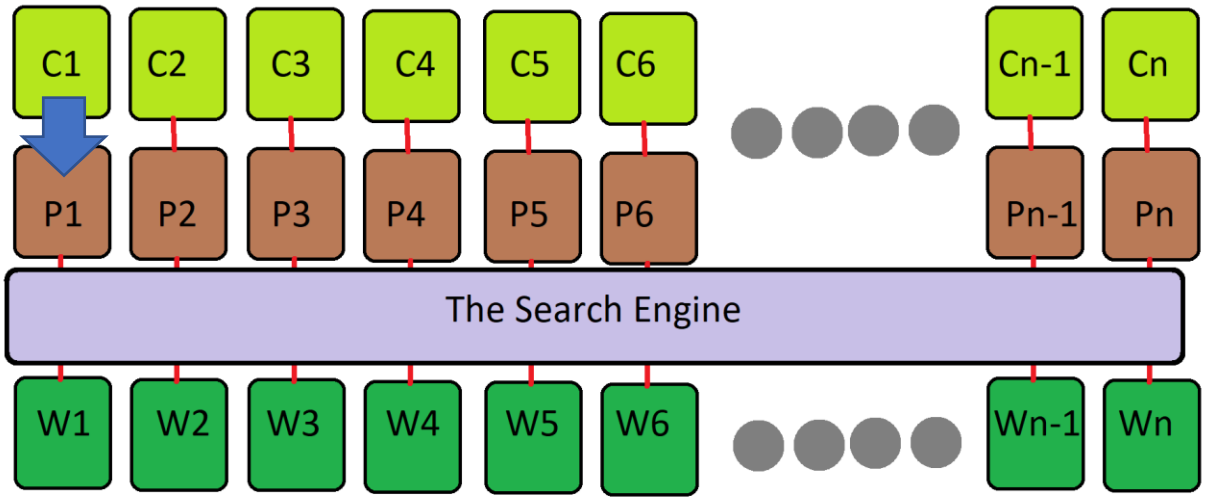
Procedure one:

The download procedure

The series of steps in the download procedure is described below.

Step one:

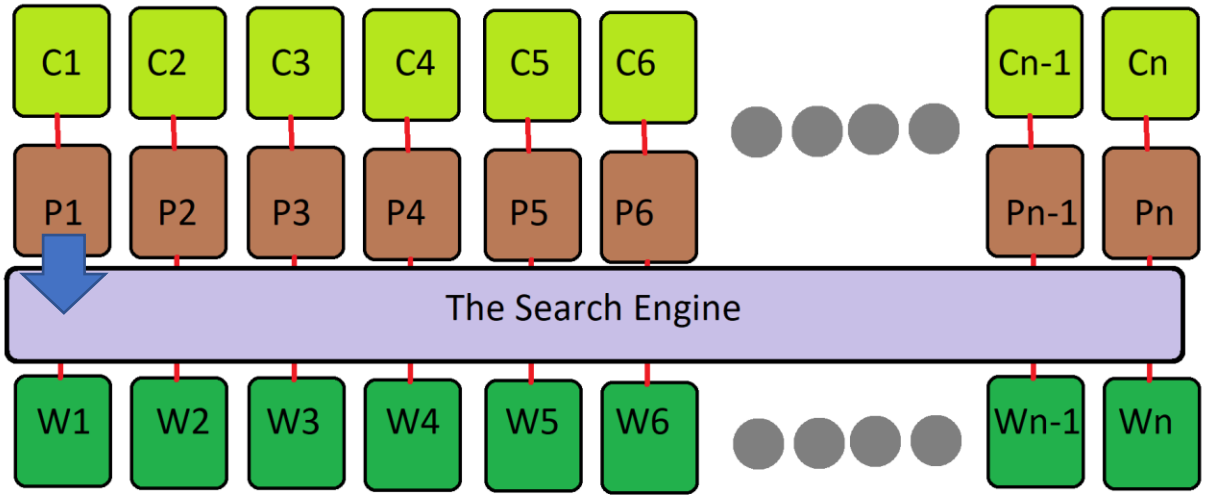
The client computer C1 connects with its corresponding proxy computer P1 and provide it with the search query it (the client computer C1) had made.



As given by the diagram the client computer C1 connects to the corresponding proxy computer it was logically linked to which is P1. The client computer only has the IP address of the proxy computer P1 known to it. It does not have any other computers IP address. Effectively this means that the client computer C1 can only connect to the proxy computer P1 in this system. After connecting with the proxy computer P1, the client computer C1 types its web search query and sends it to the proxy computer P1.

Step two:

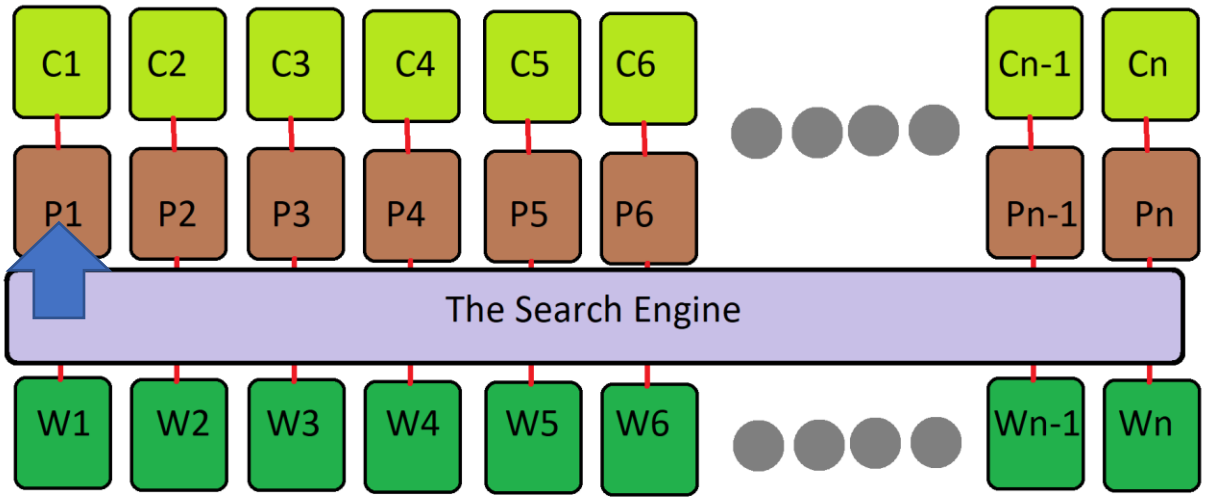
The proxy computer P1 forward the search query to the search engine.



As given by the diagram the corresponding proxy computer P1 will forward the C1 client computer send search query to the search engine. The proxy computer P1 can perform this operation because it knows its allocated IP address of the search engine.

Step three:

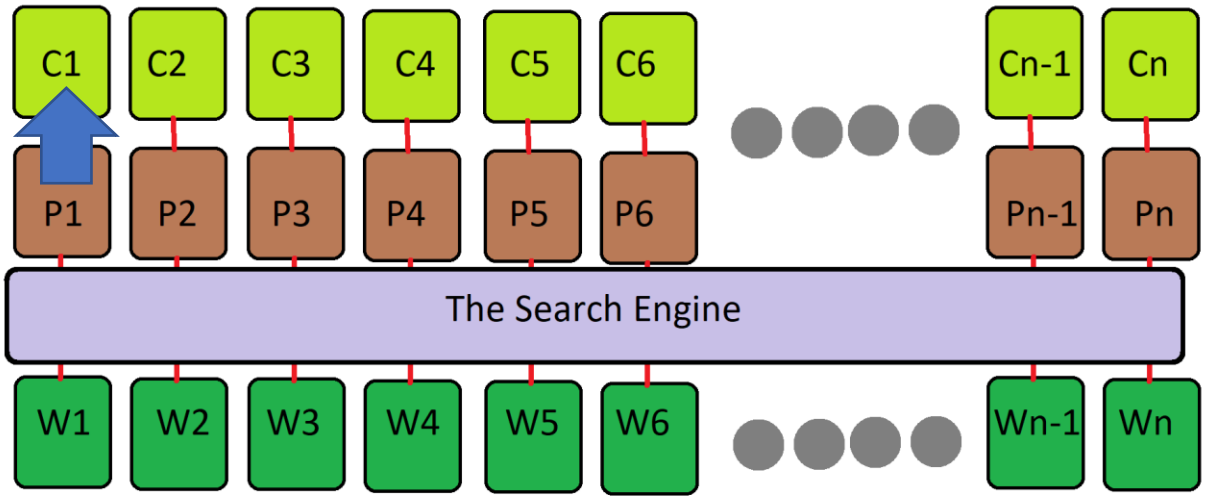
The search engine does the search web index operation and returns the search results to the proxy computer P1.



As given by the diagram the search engine performs the web site content search operation and returns the search results to the proxy computer P1. The search engine could do this search results handing operation because it knows the IP address of the proxy computer P1.

Step four:

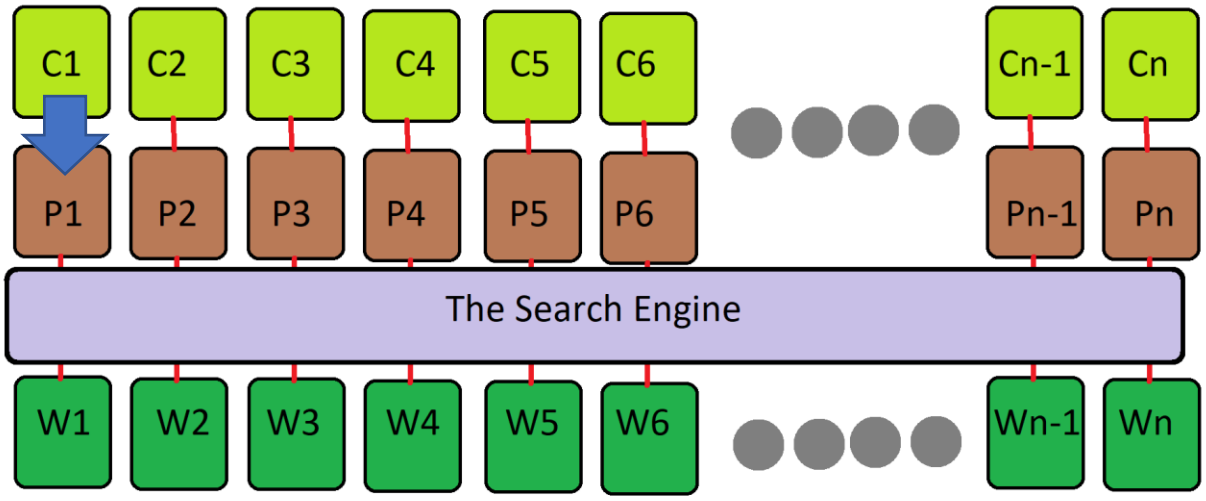
The proxy computer P1 handing the search results to the client computer C1.



As given by the diagram the proxy computer P1 handing the search results to the client computer C1. The proxy computer P1 could do this operation because it knows the IP address of the client computer C1.

Step five:

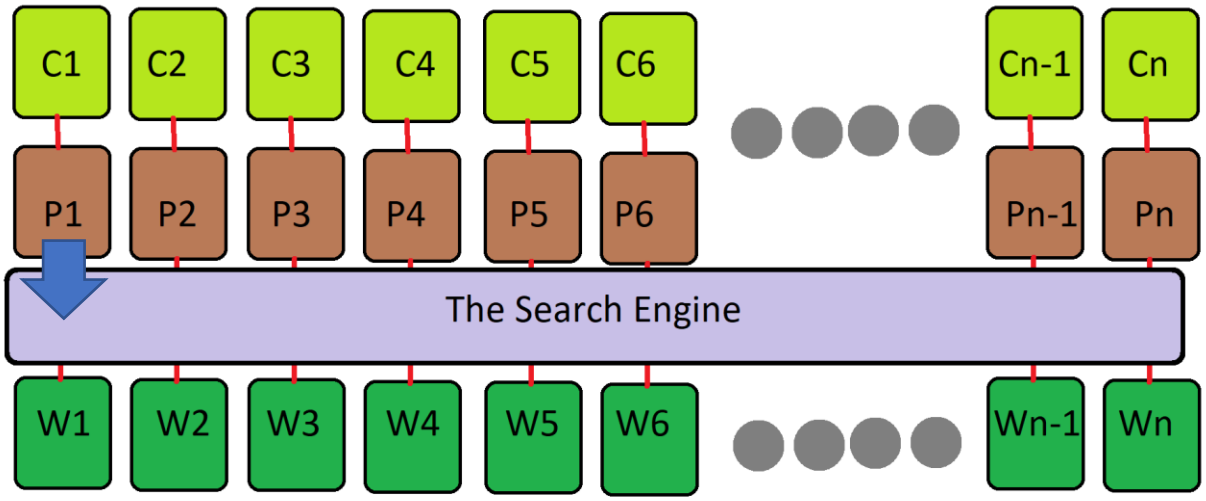
The client computer C1 sending the selected website to the proxy computer P1.



As given by the diagram the client computer C1 will select a website of its choice from the provided search results. And C1 will then send it (the selected web site) to the proxy computer P1.

Step six:

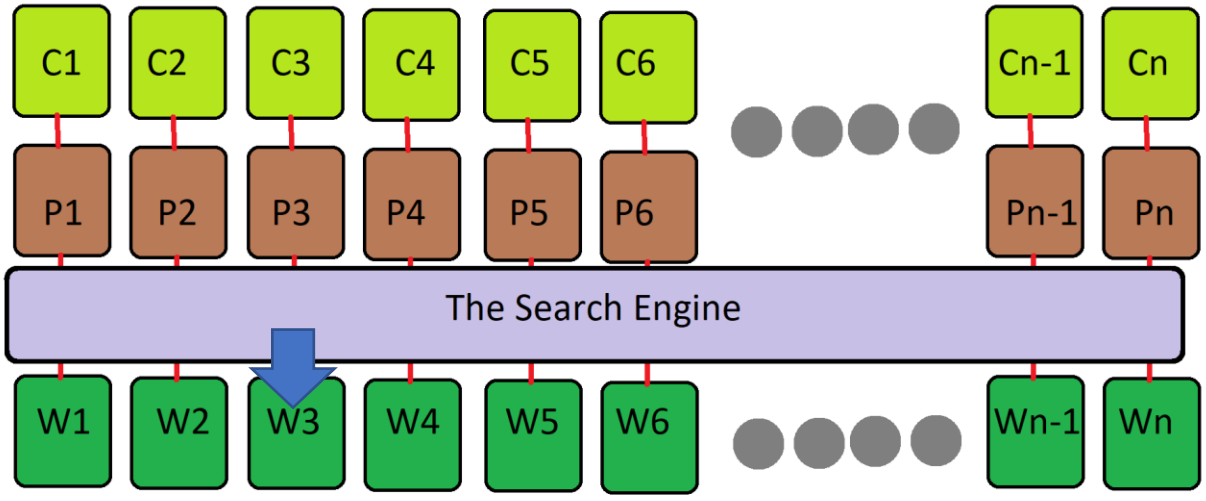
The proxy computer P1 sending the C1 client computer selected website to the search engine.



As given by the diagram the proxy computer P1 after receiving the C1 client computer selected website, will forward that result to the search engine.

Step seven:

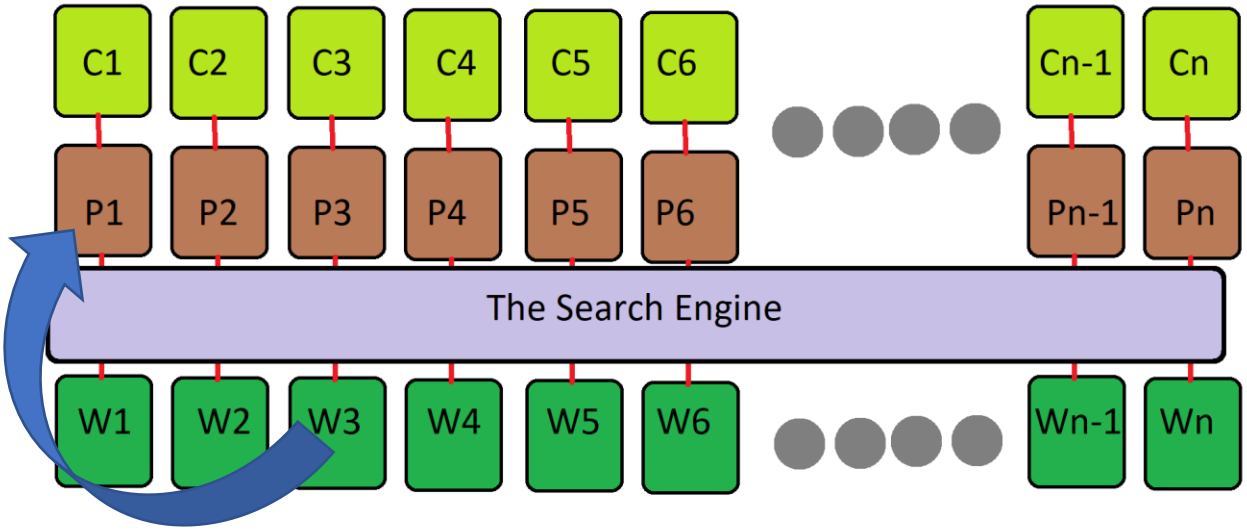
The search engine sending the web server which contains the selected website the message to send a copy of the webpage of the website the client computer C1 selected to the proxy computer P1.



As given by the diagram the search engine sends the webserver W3 a message. The web server W3 is the webserver which contains the webpage of the website the client computer C1 needs. The search engine knows this because it holds all the web pages of each website in all the webservers in an index in its (search engine's) database. The search engine in this step sends the message to the webserver W3 instructing it to send a copy of the web page of the website the client computer C1 requested to the proxy computer P1. Additionally, the search engine provides the IP address of the proxy computer P1 to the web server W3 in the message. The search engine also keeps a copy of the client computer C1 requested web page's information (the index number of that particular web page of that particular website) in its database for future use.

Step eight:

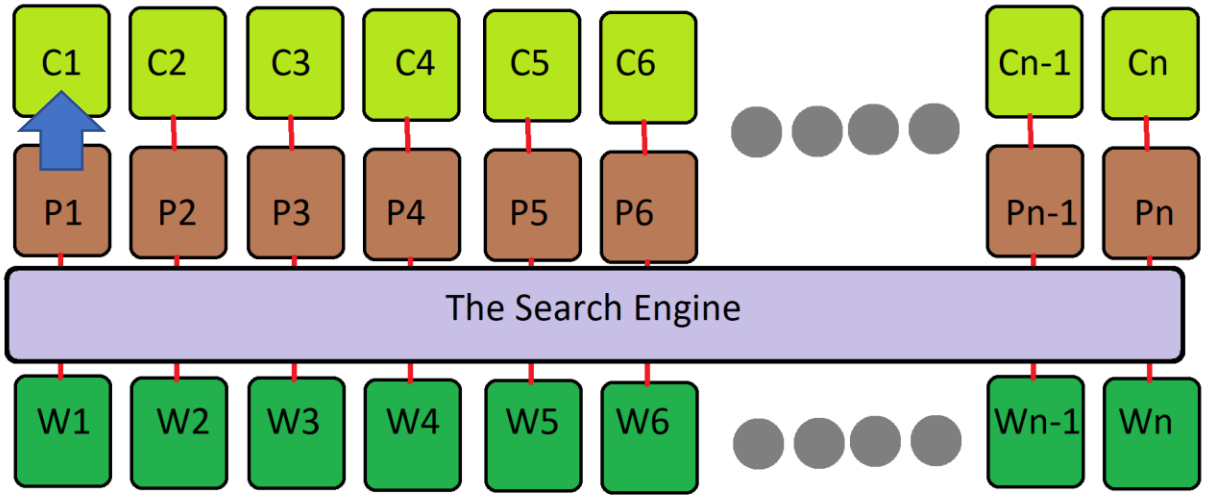
The web server W3 sends the copy of the web page of the website the client computer C1 requested to the proxy computer P1.



As given by the diagram the web server W3 sends the copy of the web page of the website the client computer C1 requested to the proxy computer P1. The web server W3 could perform this operation because it was already provided with the IP address of the proxy computer P1 by the search engine. after performing this operation, the web server W3 will delete the IP address information of the proxy computer P1 from its (web server W3's) memory.

Step nine:

The proxy computer P1 providing the client computer C1 with the web page of the website it (client computer C1) selected in the search results selection step.



As given by the diagram the proxy computer P1 after obtaining the copy of the web page of the website the web server W3 send it, forward that web page to its corresponding client computer C1. Now the client computer C1 has essentially downloaded the copy of the web page of the website it wants to view. After performing this operation, the proxy computer P1 will delete the IP address information of the web server W3 from its (proxy computer's) memory.

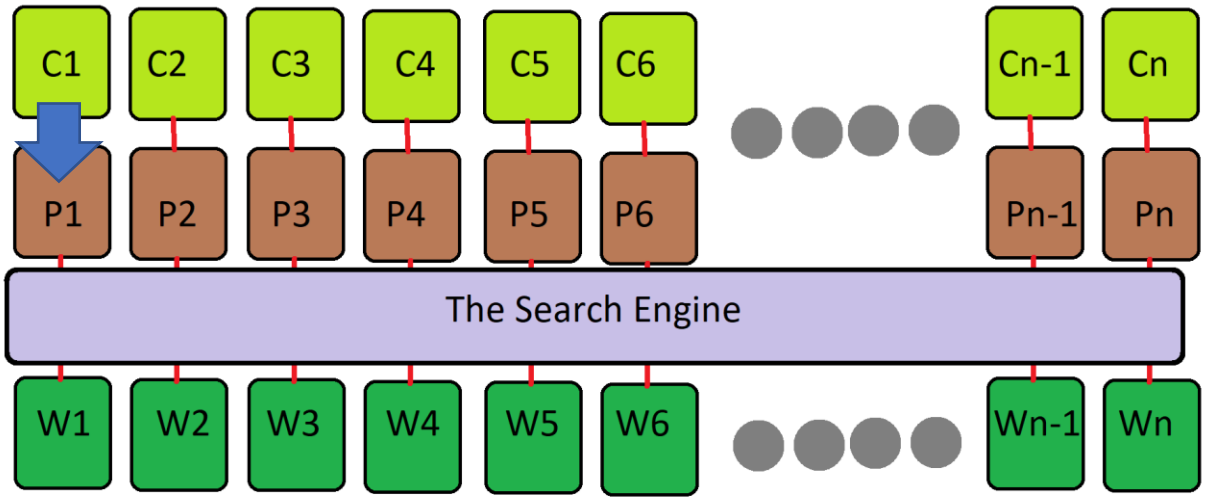
The upload procedure

This procedure contains two main steps. They are getting permission from the web server for uploading process and the uploading process.

The series of steps in the getting permission from the web server for uploading process are given below.

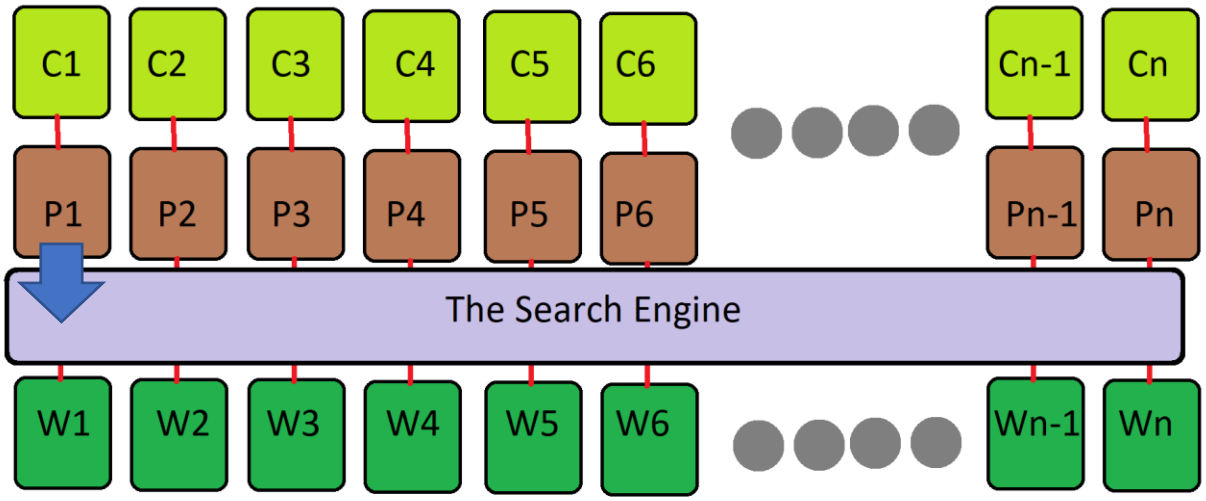
Step one:

The client computer C1 who wants to upload content to web server- in this case web server W4. Before proceeding to this step, the client computer C1 have to be surfing the website to which it wants to upload content into. Therefore, in this scenario C1 client computer have already being surfing the web site of its choice stored on the web server W4. Also, C1 have come across the interface on the particular web page where it (C1 client computer) could interact and get permission to upload. Therefore, C1 will perform the interaction needed to request to permission as provided by the interface (example: an upload button click) and will send that result to the proxy computer P1 to which the client computer is logically connected to. (as a matter of fact, P1 proxy computer is the only computer in the system the client computer C1 can directly access). This is given by the diagram below.



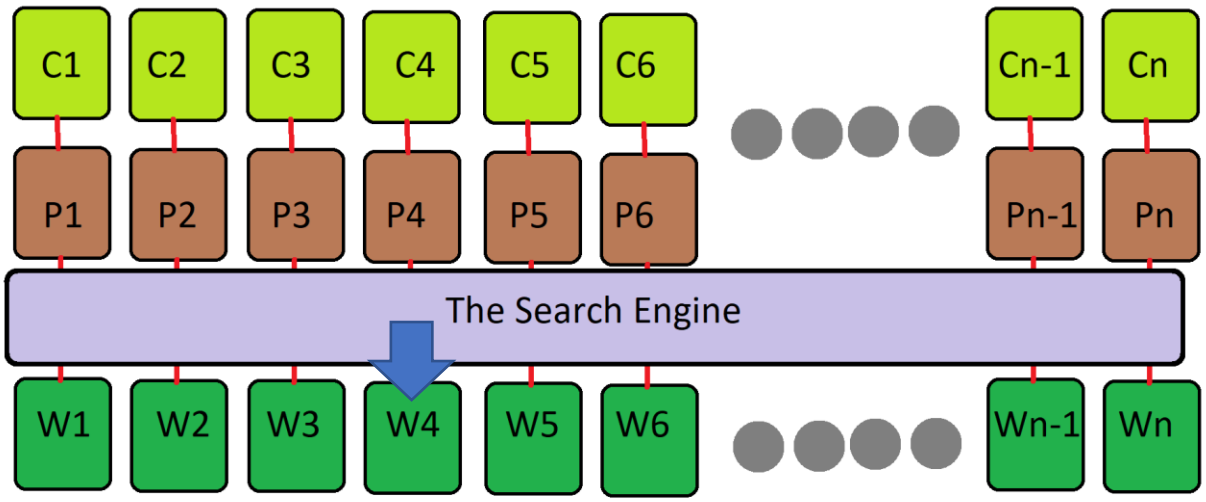
Step two:

The proxy computer P1 will forward the information (permission to upload) C1 client computer send to the search engine.



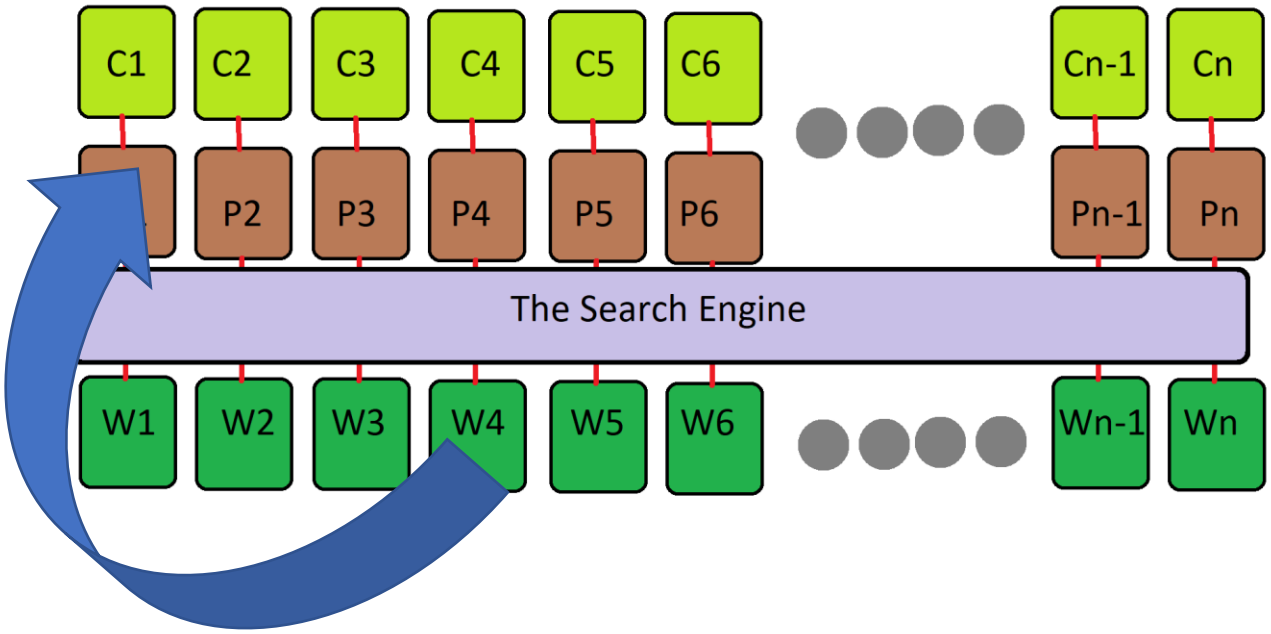
Step three:

The search engine will send the upload permission information to the web server W4 where the website to upload it located. This action was made possible because the search engine maintains a recent activities of the client computer C1 in its database. thereby the search engine will know it is to web server W4 is the web server to which it should forward the upload permission information to.



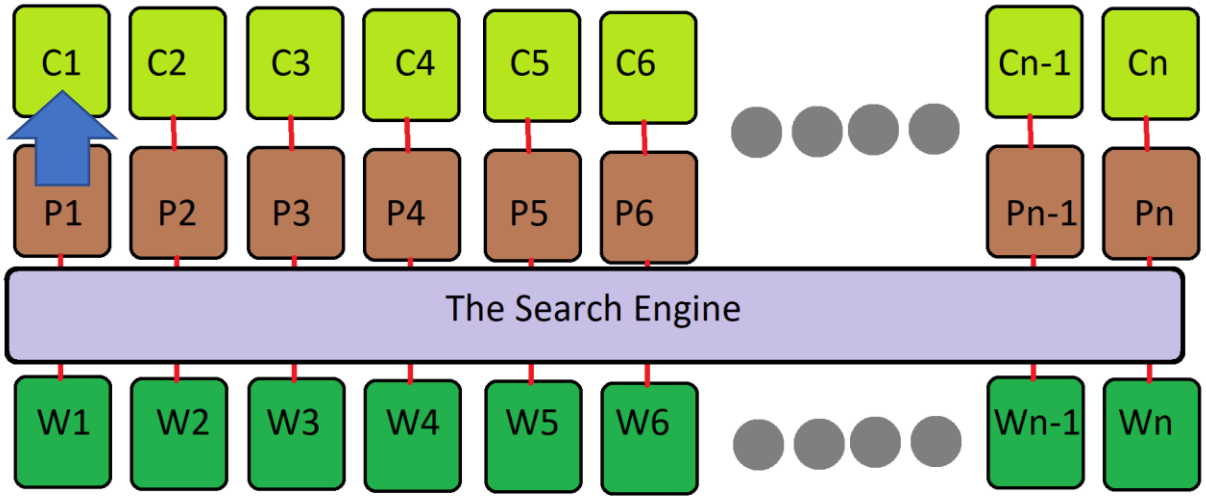
Step four:

the website that was requested permission in this scenario will give permission to upload. This permission to upload information will be send to the client computer C1 via the proxy server P1. The information sending process to proxy computer P1 by the web server W4 where the website is located is given by the diagram below.



Step five:

The proxy computer P1 will forward this permission granted information to the client computerC1.

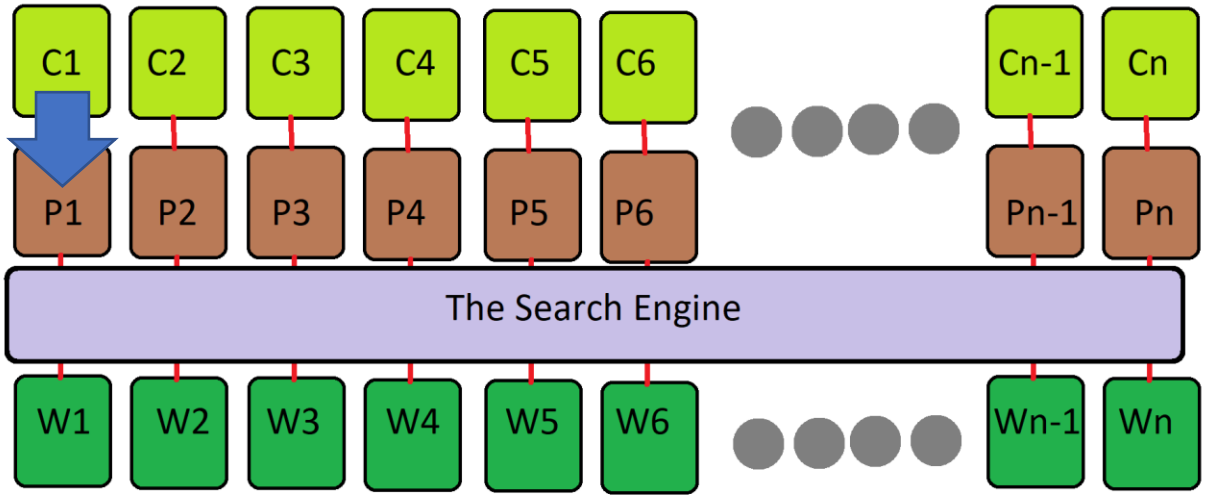


Now that the client computer C1 got permission to upload the content it can send the uploading content to the web server W4 where the relevant web site is located.

The uploading procedure is described below.

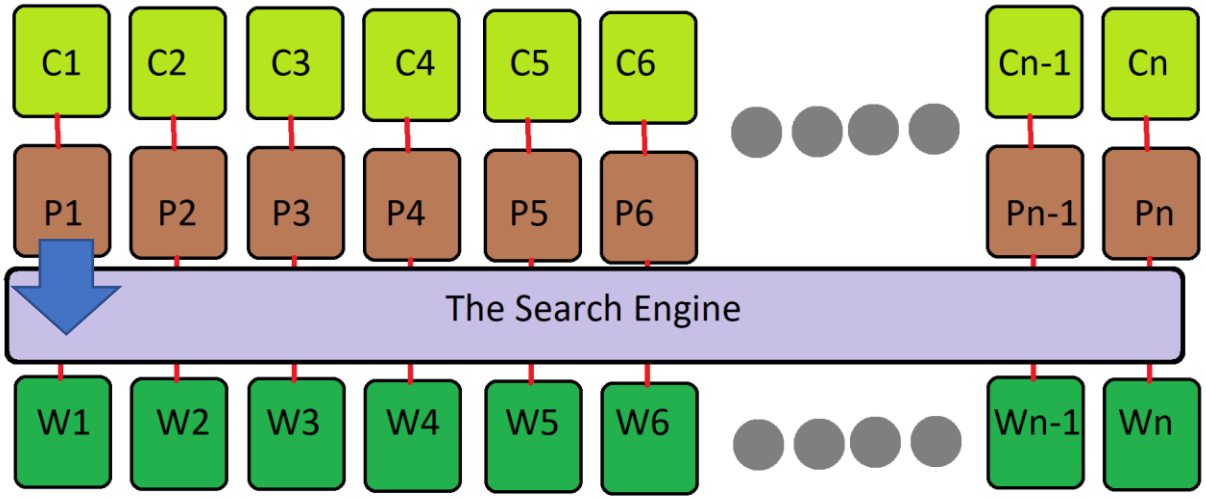
Step one:

The client computer C1 will send the uploading content to the proxy server P1.



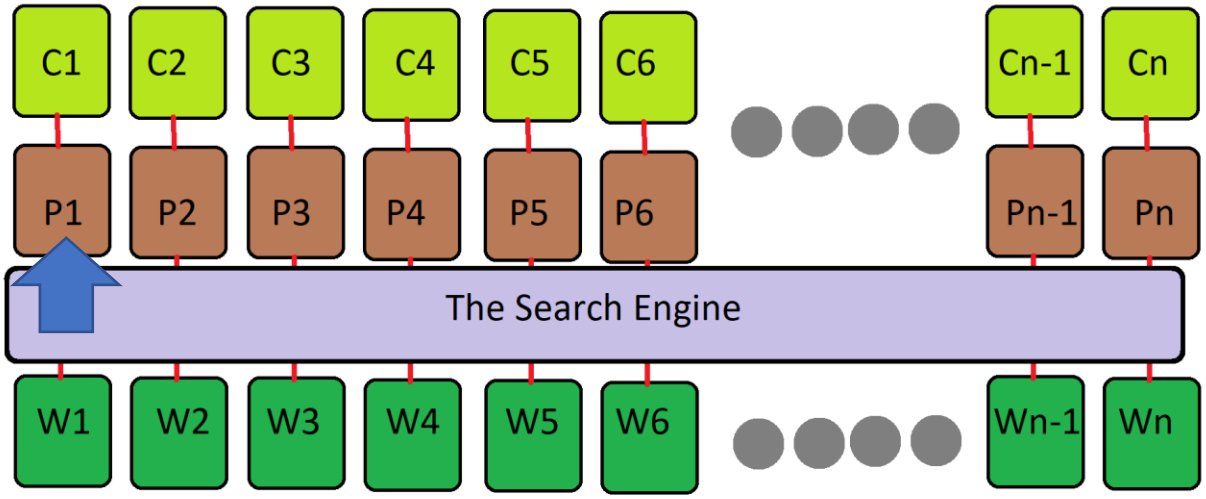
Step two:

The proxy computer P1 will get the IP address of the web server W4 where the web site to upload content into is located. This is made possible because as mentioned in the step three of getting permission procedure, the search engine keeps a record of the recent activities of the C1 computer with it. The process of requesting for the IP address of the web server W4 is given by the diagram below.



Step three:

The search engine will provide the proxy computer P1 with IP address of the web server W4 where the web site to upload content into is located.



Step four:

The proxy computer P1 will send the uploading content to the web server W4 where the website of interest is located for content uploading.