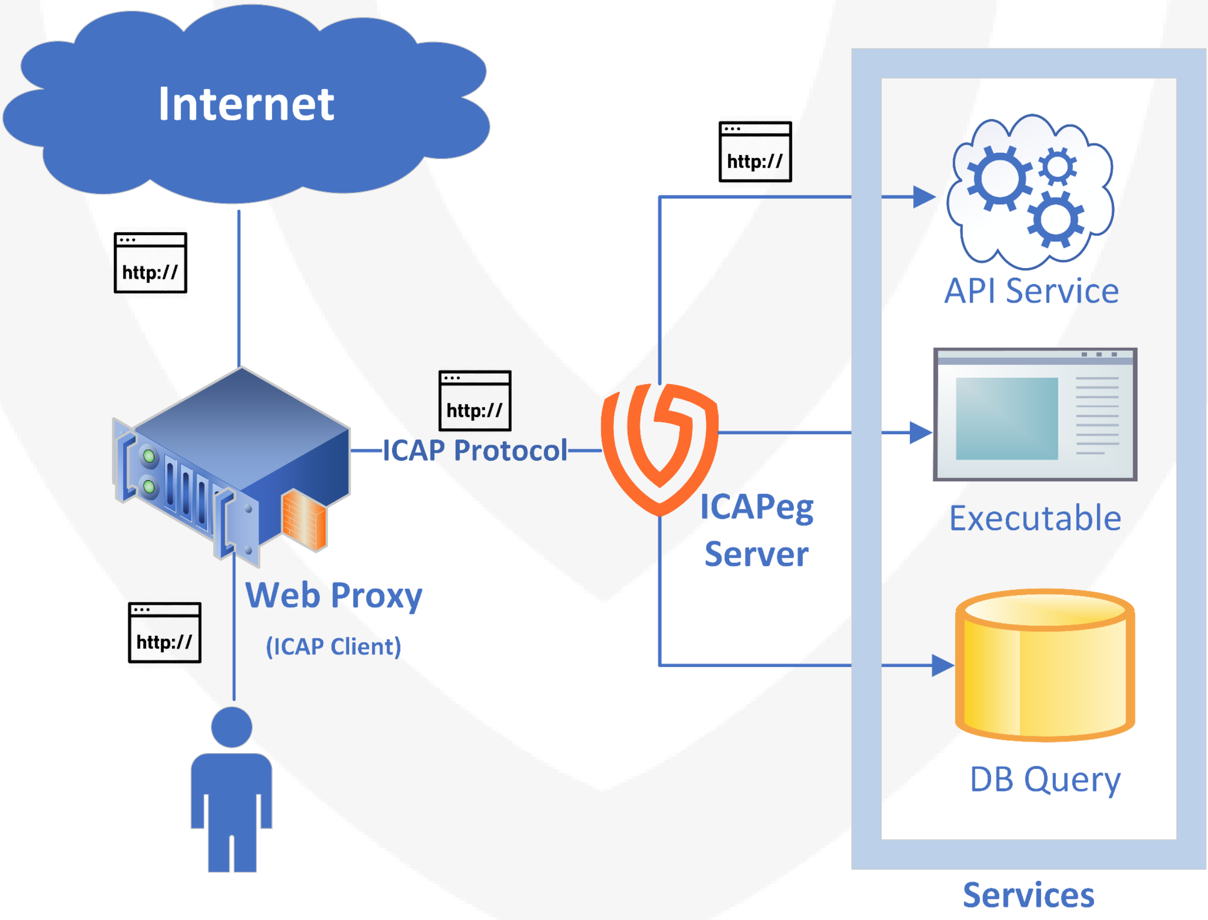
# ICAPeg ICAP Server Datasheet

## Introduction

The ICAP protocol is used to extend web proxies capabilities (ICAP clients). Consider a case when users of an application upload their CVs. These files could have viruses and malicious code. Here a Gateway Anti Virus Scanner (ICAP server) is useful to scan files before sending them to the server, ICAP protocol is the protocol overwhich a web proxy would be able to communicate with a gateway AV scanner.

ICAPeg is an Open Source implementation of ICAP server, designed to enable web proxies to utilize the function of API based services along with standalone executables and databases in order to provide content inspection and manipulation services.



## How does ICAP protocol work?

When a user connected to a Web Proxy browses the internet; if that web proxy is configured to use an ICAP server, and depending on its policy, if the user initiated a HTTP request that request will be forwarded to the ICAP server if it matches the Web Proxy policy criteria of doing so, the request will not reach its intended server till the Proxy hears back from the ICAP server. In that previous example, the Web Proxy acts as an ICAP client, ICAPeg acts as an ICAP server and the mode of operation of the ICAP protocol is called ICAP Request Modification (REQMOD).

Likewise, when a response is received from the web server it will be forwarded to the ICAP server if it matches the Web Proxy policy criteria of doing so, in this case the Web Proxy acts as an ICAP client, ICAPeg acts as an ICAP server and the mode of operation of the ICAP protocol is called ICAP Response Modification (RESPMOD).

The purpose of the ICAP protocol is to allow a third party to modify a HTTP message (Either Request , Response or both) before it reaches its intended recipient. Either a web server in the case of a HTTP request or the user in the case of HTTP response. And assuming that this HTTP communication is being handled by a Web Proxy server which supports ICAP protocol and configured to provide that functionality.

The Web Proxy might be configured to send all the requests and responses it is processing to the ICAP server, but usually there would be a criteria defined as a policy on the Proxy Server to only send specific traffic to the ICAP server that is in the interest of the latter. For example The Web Proxy might be configured to send executables downloads only to the ICAP server, and that executables downloads would be identified at the Proxy level by extension or HTTP mime-type.

## ICAP Request Modification

- User sends a request to the web proxy (ICAP client).
- web proxy initiates an ICAP request to the ICAP server.
- This ICAP request encapsulates the HTTP request that the user sent.
- ICAP server processes the ICAP request and decides to either modify the encapsulated request or not.
- Proxy receives the ICAP response with the potentially modified HTTP request.
- Proxy forwards the HTTP request to the Web server.

## ICAP Response Modification

- Proxy received a HTTP response of a user initiated HTTP request.
- web proxy initiates an ICAP request to the ICAP server.
- This ICAP request encapsulates the HTTP response that the proxy received.
- ICAP server processes the ICAP request and decides to either modify the encapsulated HTTP response or not.
- Proxy receives the ICAP response with the potentially modified HTTP response.
- Proxy forwards the HTTP response to the user.

# ICAPeg Services

ICAPeg is an open-source ICAP server written in Go/Golang. Developers can use it to integrate with any service interested in HTTP content inspection/manipulation as long as this service is being offered as: HTTP API service, standalone executable or a Database query.

ICAPeg is offering the possibility of developing custom modules/addons to integrate with a specific vendor's services and administrators can use to change, add or delete the parameters that affect the service.

To start using ICAPeg please refer to the project page at Github:
https://github.com/egirna/icapeg

# Use Cases

## Malware Detection and Inspection

ICAP can be used to redirect HTTP requests to a service that can perform:

- Malware Scanning.
- Sandboxing.
- Content Disarm and Reconstruction (CDR).

## Data Loss Prevention (DLP)

Protecting confidential data is a challenging problem. Consider a situation when an employee sends sensitive data accidentally to a place where it shouldn't be sent to. It would be a significant security concern. That's why organizations should consider data loss/leak prevention techniques to stop such scenarios. ICAP here can be used to capture the content sent. Then it redirects this content to a service where the content is analyzed to see if there is confidential data or any other data type that shouldn't be sent. After analyzing the request, ICAP then responds with an error page to let the user know that it's confidential data or it can allow sending this data if it's allowed.

## CONTENT FILTERING

There are content categories on the web which are undesirable or unappealing. These types of content need somehow to be flagged and blocked. First, a service can be programmed to analyze and categorize web page content. It does that based on the text, pictures, and URLs in it. ICAP then can be used to prevent specific categories of these contents.