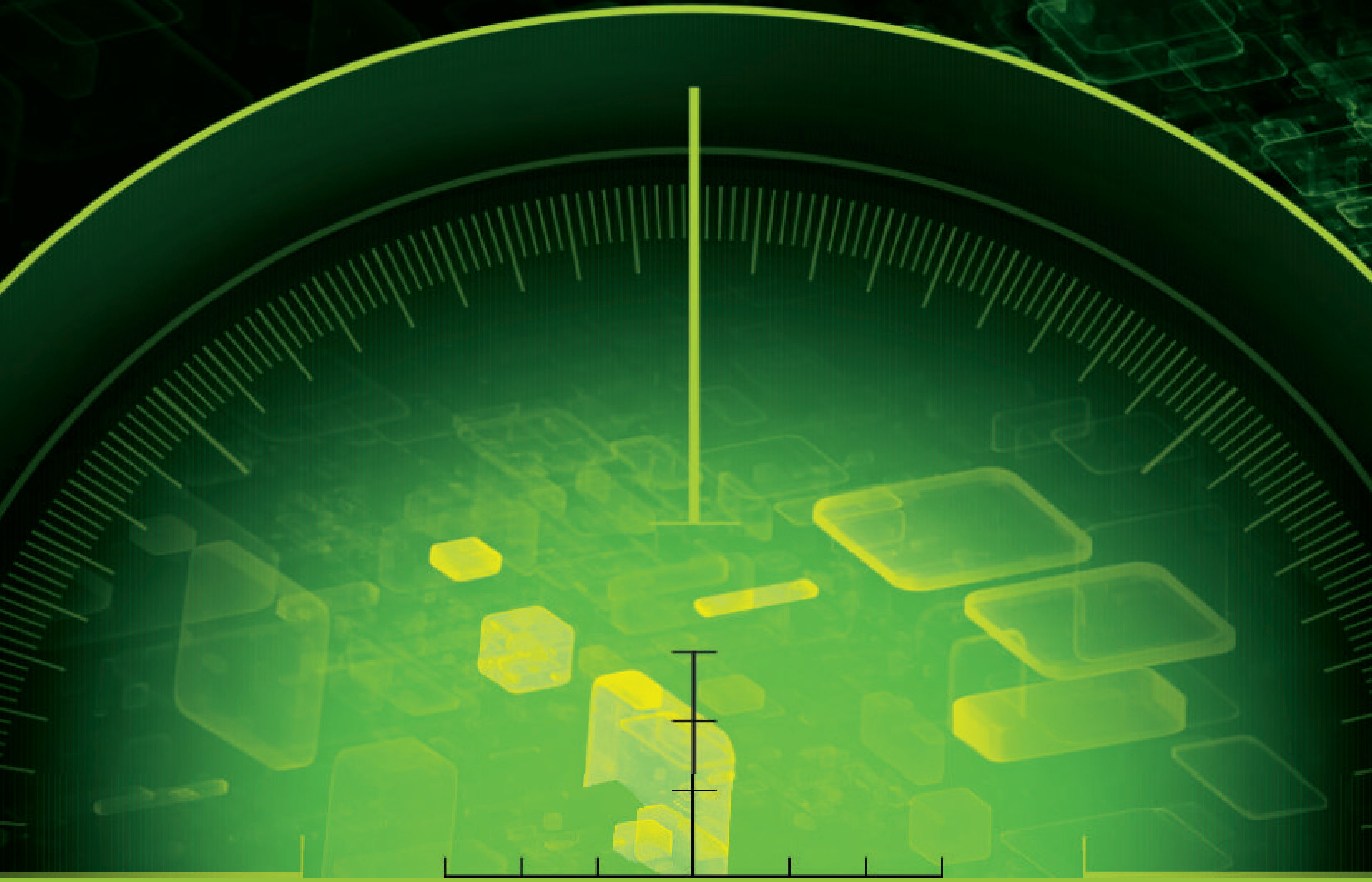
'eScan™

Anti-Virus & Content Security

eScan for Squid Proxy
(with ICAP Support)



Document Version - ICAP_MW_V14.1

www.escanav.com

MicroWorld Anti-Virus for Proxy Server with ICAP

INTRODUCTION

MicroWorld Anti-Virus for Proxy Server provides anti-virus protection for network traffic routed through proxy servers

which support the Internet Content Adaptation Protocol (ICAP).

The program allows:

- Perform anti-virus scans on objects transferred through the proxy server.
- Cure infected objects, or block access to infected objects if disinfection fails.
- Use group settings to define filtration parameters that are applied depending on the address of the user requesting an object, and the object's address (URL).
- Log activity statistics, including information about anti-virus scanning and its results, and application errors and warnings.
- Update the anti-virus databases. By default the application uses MicroWorld update servers as the source of updates. The anti-virus databases are used in the detection and disinfection of infected objects. The application uses database records to analyze every object, checking it for virus presence: its content is compared with code typical for specific viruses.

Please be aware that new viruses appear every day, and therefore you are advised to maintain the anti-virus databases in an up-to-date state.

HARDWARE AND SOFTWARE SYSTEM REQUIREMENTS

In order for MicroWorld Anti-Virus to operate, the system must meet the following hardware and software requirements:

- Minimum hardware requirements:

  a. Processor Intel Pentium® II 400 MHz or higher;

  b. 1 GB RAM;

  c. 500 MB of disk space for MicroWorld Anti-Virus setup.

  d. 200 MB of available disk space for temporary files.

  e. Software requirements:
  Currently we support Ubuntu 14.04 64.bit OS, as per the client requirement the required os build will be provided.

HOW THE MicroWorld ANTI-VIRUS WORKS

MicroWorld Anti-Virus performs anti-virus scanning of HTTP traffic using two modes of proxy operation: REQMOD and RESPMOD.

In the RESPMOD mode, the application checks objects requested by users via a proxy server. In the REQMOD mode it scans objects transmitted by users through the proxy.
In the RESPMOD mode, the application uses this algorithm to scan internet traffic

1. The user requests an object through a proxy via HTTP.

2. If the requested object is available within the proxy cache, it will be returned to the user. If the object is not found in the cache, the proxy accesses a remote server and downloads the requested object from it.

3. The proxy uses ICAP to transfer the received object to MicroWorld Anti-Virus for an anti-virus scan.

4. The application assigns a specific status to a scanned object on the basis of the anti-virus scan results. Access
   to objects with a specific status is granted or blocked according to the processing group parameters.

5. If access to an object has been granted, MicroWorld Anti-Virus allows the proxy to cache the object and transmit
   it to users. If access to an object is blocked, MicroWorld Anti-Virus prevents the proxy from caching the object or delivering it to users. Instead of receiving the requested object, the user will be notified that access to the object has been blocked.

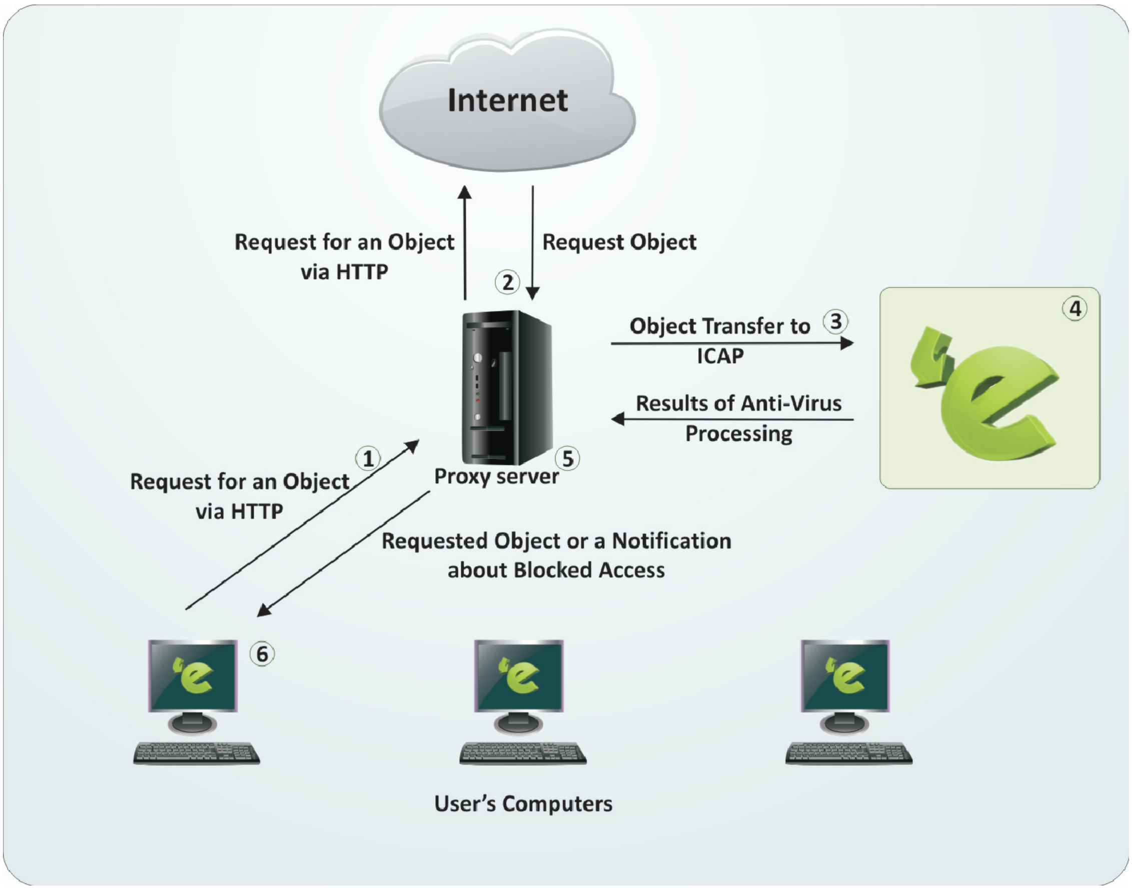

Internet
Request for an Object via HTTP
2
Request Object
Object Transfer to ICAP
3
4
Results of Anti-Virus Processing
1
Request for an Object via HTTP
Proxy server
5
Requested Object or a Notification about Blocked Access
6
User's Computers

Figure 1. Anti-Virus scanning of traffic in the RESPMOD mode

In the REQMOD mode, the application uses the following algorithm to scan internet traffic

1. The user sends an object using HTTP via a proxy.

2. The proxy uses ICAP to transfer the received object to MicroWorld Anti-Virus for an anti- virus scan.

3. After anti-virus check the product assigns a certain status to the scanned object; transfer of that object will be allowed or prohibited in accordance with the status. Access to objects with a specific status is granted or blocked according to the processing group parameters

4. If transfer is allowed, the proxy transmits the object sent by the user. If transfer is prohibited, the proxy does not transmit the object and instead notifies the user that the transfer has been blocked.

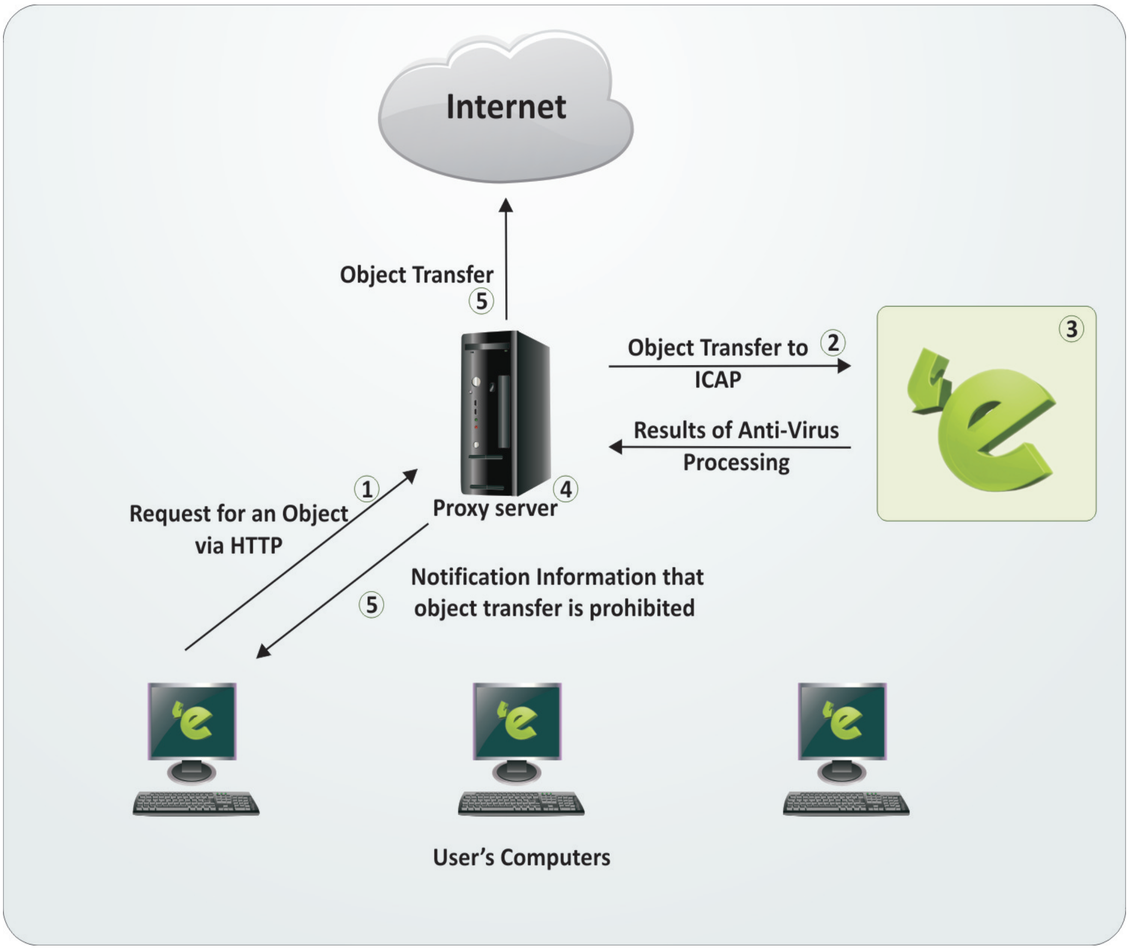

Internet
Object Transfer
5
Object Transfer to ICAP
2
3
Results of Anti-Virus Processing
1
Request for an Object via HTTP
Proxy server
4
5
Notification Information that object transfer is prohibited
User's Computers

Figure 2. Anti-Virus scanning of traffic in the REQMOD mode

ICAP REQUESTS PROCESSING ALGORITHM

During interaction with the proxy server, MicroWorld Anti-Virus acts as an ICAP server. The main ICAP server process controls child processes, which perform the following functions:

- receive and process requests from ICAP client (proxy server);
- interact with the anti-virus kernel: send requests for scanning and receive scan results;
- collect statistical information about scanning;
- transfer data from the anti-virus kernel to ICAP client.

INSTALLATION ON A DEDICATED SERVER

Installing the program on a dedicated server is recommended when the proxy server is heavily loaded, and also when MicroWorld Anti-Virus is used to process the traffic from several proxy servers. Since automatic configuration of the Anti-Virus and proxy is impossible in this deployment scenario, you will have to configure them manually.

CONFIGURING INTEGRATION WITH A SQUID PROXY

The following procedure is used to integrate MicroWorld Anti-Virus with a dedicated Squid server:

Icap Conf file- /opt/MicroWorld/etc/c-icap.conf

1. MicroWorld Anti-Virus will use to expect proxy requests for anti-virus scanning of accessed objects. By default, MicroWorld Anti-Virus expects requests at localhost:1344. you can chenge it in **Port** configuration in Icap Conf file.

Before changing the value of **Port** configuration parameter, stop MicroWorld Anti-Virus Service using the following command:

for Linux:

```
# /etc/init.d/mwav stop
```

Execute the following command to start the MicroWorld Anti-Virus service:

for Linux:

```
# /etc/init.d/mwav start
```

2. Make the following changes in the proxy server configuration file typically in

/etc/squild3/sqid.conf

```
icap_enable on

icap_send_client_ip on

icap_send_client_username on
icap_client_username_header X-Client-escan
icap_service service_req reqmod_precache bypass=1 icap://127.0.0.1:1344/avscan

adaptation_access service_req allow all
```

```
icap_service service_resp respmod_precache bypass=1 icap://127.0.0.1:1344/avscan

adaptation_access service_resp allow all
```

3. Restart the proxy.

Web management colnole is also provided with MicroWorld Antivirus it can be access by using following url
http://SERVER-IP:10080

By login into web management following task can be done.

1. Check the status of services ie Antivirus and ICAP server
2. Starting and Stopping of services
3. Update the antivirus signatures
4. Check the log of the server

Some handy backend command to check the ICAP and AV server

To start ICAP service

```
# /etc/init.d/c-icap start
```

To stop ICAP service

```
# /etc/init.d/c-icap stop
```

To show status of ICAP service

```
# /etc/init.d/c-icap status
```

To start Antivirus service

```
# /etc/init.d/mwav start
```

To stop Antivirus service

```
# /etc/init.d/mwav stop
```

To show status Antivirus of service

```
# /etc/init.d/mwav status
```

To start squid service

```
# /etc/init.d/squid3 start
```

To stop squid service

```
# /etc/init.d/squid stop
```

To show status of service

```
# /etc/init.d/squid status
```

When the virus is detected the page will be shown containing the file name which is to be uploaded or donloaded containing virus and the virus name returened from Antivirus engine. For example as below -

You try to upload/download the file - from
http://www.eicar.org/download/eicar.com.txt

that contain the virus: **EICAR-Test-File**

This message generated by MicroWorld - ICAP virus_scan module

You can modify the msg by changing to the files in following directory, it contain the files in html format according to the language .

/opt/MicroWorld/usr/share/c_icap/templates/virus_scan/