NoSpamProxy Server with ICAP Client and AVIRA ICAP Server

Version 14

Legal information

Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn
Germany

THIS DOCUMENT WAS LAST EDITED ON NOVEMBER 27, 2023.

Content

General Information

NoSpamProxy as ICAP client

NoSpamProxy Protectionoffers the functionality of an ICAP client from version 11.1. Using the ICAP standard, it is possible to use services that an ICAP server offers. These can be virus scanners, content filters or similar functions. In principle, all virus scanners can be used in NoSpamProxy if they offer an ICAP connection as an ICAP server. In any case, make sure that the virus scanner has implemented the ICAP protocol correctly and in the required functional scope.

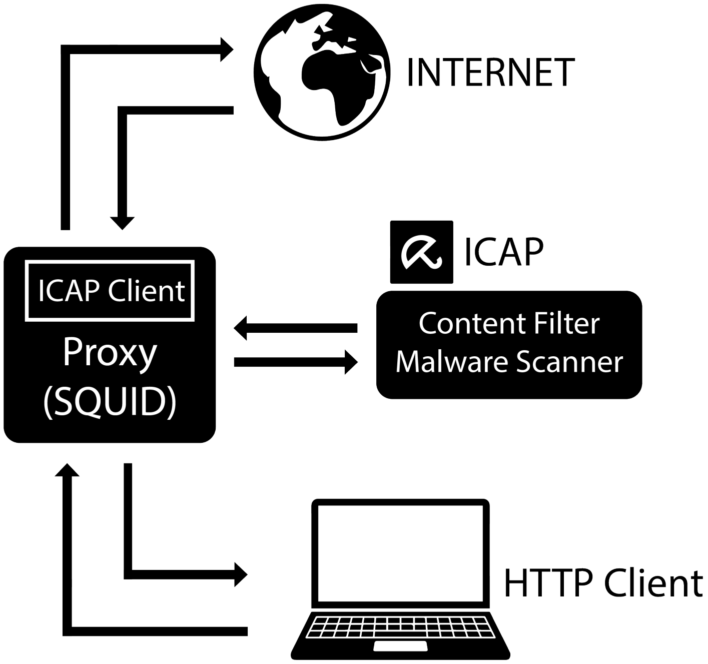
AVIRA's ICAP server has also been tested for use with NoSpamProxyand can be ordered as an optional add-on for NoSpamProxy as an OEM product via Net at Work. An existing license or instance of Avira av-icapd can be used; purchasing a new license may not be necessary.

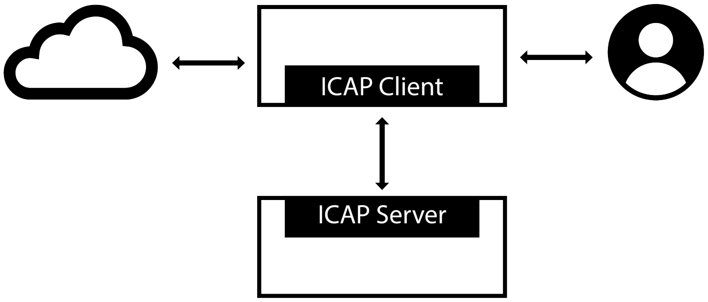
The ICAP client interface is included in NoSpamProxy Protection by default. An additional license or option is not required.

Email gateways such as NoSpamProxyare a standard element of an organisation's security architecture. They are responsible for the increasingly complex processing of incoming and outgoing e-mails. In addition to analysing emails for the existence of malicious code, spam protection and content processing are becoming increasingly complex.

Also, functions such as virus scans are also required by other proxy services, so that the central use of a scanner service (and the license) is economically very interesting.

For this purpose, the Internet Content Adaption Protocol (ICAP for short) was developed as an IETF standard. The proxy server (in this case NoSpamProxy), acting as an ICAP client, can send content to an ICAP server for analysis and receives the scan result from this server.





Virus scanners with ICAP interface are offered by most AV manufacturers. The German manufacturer AVIRA also has an ICAP server in its portfolio and is an OEM partner of Net at Work.

Separating tasks and performance increase

The functions "Policy Enforcement" for NoSpamProxy on the one hand, and "Evaluation of the content for freedom from viruses" on the ICAP server on the other hand, are deliberately separated: Scanning the content for viruses usually causes a higher load. With the swapping out you achieve a relief of the gateway. To increase throughput in larger companies, a proxy server can usually use several scanner servers: the load is distributed over even more shoulders. The entire system is also better protected against server failure. Large installations usually use additional load balancers to further increase the performance of the proxy server farm.

Advantages

The AVIRA ICAP server can not only scan the data but also evaluate it: Depending on the category of malware, NoSpamProxy can then decide what to do.

Another special function is trickling: If a large amount of data needs to be checked, the scanner reports back with a response to the submitting server so that the connection does not break down. Small data snippets are already returned while the scanner is still working in the background. This way NoSpamProxy knows that its request is still being processed and does not run into a timeout. The processing of the next emails in NoSpamProxy can continue in parallel.

Installation and start-up

Installing the AVIRA ICAP server

The AVIRA ICAP server is delivered by Net at Work as a virtual appliance based on Debian 8 (LTS to 05/20) Linux. It is a hardened operating system on which only the ICAP service runs.

> **NOTE:** The SSH service is disabled by default and can only be enabled by our support team.

1. Create a new, empty virtual machine in Hyper-V, VMWare ESXi or Citrix Xen

   > **NOTE:** Assign at least one CPU core and 2GB RAM. Our recommendation for 2500 emails per hour or more is 4GB RAM and two CPU cores.

2. Mount the ready-made HDD image of the AVIRA ICAP server into the empty virtual machine.

   > **NOTE:** If you are using Hyper-V, please select **Gen 1**when you create it. All optional virtualization tools are already installed.

The HDD image already contains your license code. This applies both to the 30-day test license and to purchased licenses. To ensure compatibility, the HDD image is delivered on an IDE HDD.

All important operating system updates are installed automatically every night. Every 10 minutes the system checks for new virus signatures or updates to the ICAP service. These virus signatures are obtained automatically, if available.

> **NOTE:** For the operating system updates, the virtual computer requires a connection to the Internet via port 80. To update the virus signatures a connection via port 443 on **avira.nospamproxy.de** is required.

> **NOTE:** Avira uses TCP port 1344 and the service **service_scanner**for the connection.

Starting up the AVIRA ICAP server

Setting up the ICAP server

1. Turn on the virtual machine.
2. Log in with the following data:

   User: **nsp**

   Password: **nsp**
3. Set a new password for the user NSP by executing the following call:

   ```
   nsp@avira:~$ passwd
   ```

Setting up the network card

1. Issue the following command:

   ```
   root@avira:~# nano /etc/network/interfaces
   ```

2. Now integrate the interface either statically or via DHCP.

    - static:

      ```
      car eth0
      iface eth0 inet static
      address 172.8.0.7
      netmask 255.255.0.0
      gateway 172.8.0.1
      ```

    - DHCP:

      ```
      car eth0
      iface eth0 inet dhcp
      ```

3. Save the settings with **CTRL + O**.

4. Enter a DNS server:

    ```
    root@avira:~# nano /etc/resolv.conf
    ```

5. Restart the virtual machine:

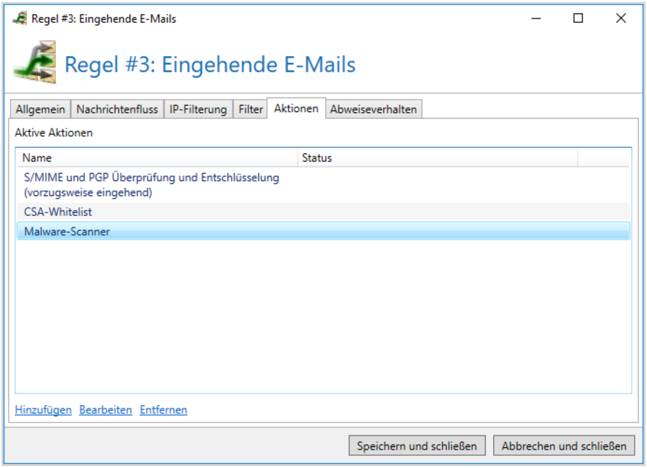
    ```
    nsp@avira:~$ /sbin/reboot
    ```

The AVIRA ICAP server can now be addressed by NoSpamProxy as an ICAP client.

Integration into NoSpamProxy

To enable NoSpamProxy® to send email attachments to an ICAP server for scanning, you must enable the ICAP AntiVirus server in the corresponding rule:

1. Open the desired rule for inbound emails.

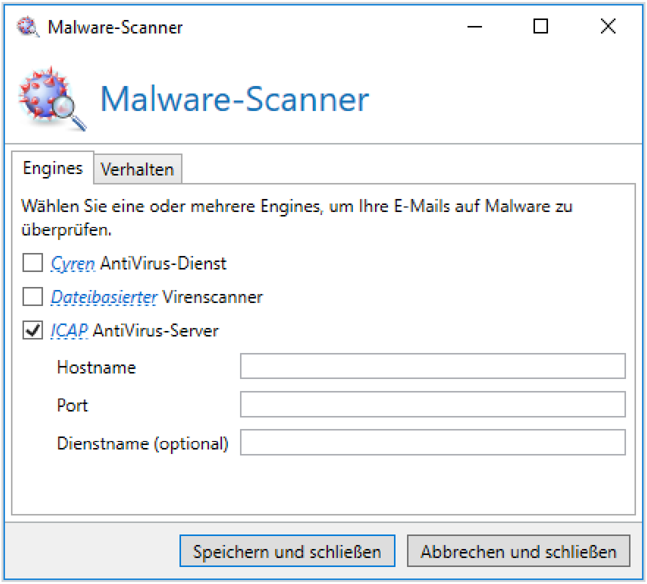


Regel #3: Eingehende E-Mails

Aktive Aktionen

Name	Status
S/MIME und PGP Überprüfung und Entschlüsselung (vorzugsweise eingehend)	
CSA-Whitelist	
Malware-Scanner	

2. Open the **Malware scanner** action .



Malware-Scanner

Wählen Sie eine oder mehrere Engines, um Ihre E-Mails auf Malware zu überprüfen.

☐ Cyren AntiVirus-Dienst

☐ Dateibasierter Virenscanner

☑ ICAP AntiVirus-Server

Hostname

Port

Dienstname (optional)

3. On the **Engines** tab, tick the **ICAP AntiVirus server** checkbox.

4. Enter the required data.
5. Click **Save and close**.

You will now find a log on the ICAP server. To open this log, enter the following command on the command line:

```
nsp@avira:~$ less icap. log
```

The infestation of an email would also appear in the log:

```
ALERT: [service_scanner]malware info: 'W2000M/Donoff.aipbpa ; virus
; Contains code of the macro virus W2000M/Donoff.aipbpa'.
```

To search for all findings, enter the following command:

```
nsp@avira:~$ grep -HRN "Infected file" icap.*
```

Help and support

Knowledge Base

The **Knowledge Base** contains further technical information on various problems.

Website

The **NoSpamProxy website** contains manuals, white papers, brochures and other information about NoSpamProxy.

NoSpamProxy Forum

The **NoSpamProxy forum** gives you the opportunity to exchange information with other NoSpamProxy users, get tips and tricks and share them with others.

Blog

The **blog** offers technical support, tips on new product versions, suggestions for changes to your configuration, warnings about compatibility problems and much more. The latest news from the blog is also displayed on the start page of the NoSpamProxy Command Center.

YouTube

On our **YouTube** channel you will find tutorials, how-tos and other product information that will make working with NoSpamProxy easier.

NoSpamProxy Support

You can reach our support team

- by phone at **+49 5251304-636**
- by email at **support@nospamproxy.de**.