noSpamProxy® SERVER

noSpamProxy® CLOUD

# NoSpamProxy mit ICAP-Client und AVIRA ICAP-Server

Version 14

Net at Work
Building IT-Excellence.

## Rechtliche Hinweise



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



**DIESES DOKUMENT WURDE ZULETZT AM 31. MÄRZ 2023 ÜBERARBEITET.**

# Inhalt

# Allgemeine Informationen

## NoSpamProxy als ICAP-Client

NoSpamProxy Protection bietet die Funktionalität eines ICAP-Clients ab Version 11.1 an. Über den ICAP-Standard ist es möglich, Services zu nutzen, die ein ICAP-Server anbietet. Dies können Viren-Scanner, Inhaltsfilter oder ähnliche Funktionen sein. Prinzipiell sind alle Virenscanner geeignet, wenn Sie eine ICAP-Anbindung als ICAP-Server bieten, mit NoSpamProxy zusammenzuarbeiten. Stellen Sie in jedem Fall sicher, dass der Virenscanner das ICAP-Protokoll korrekt und im erforderlichen Funktionsumfang implementiert hat.

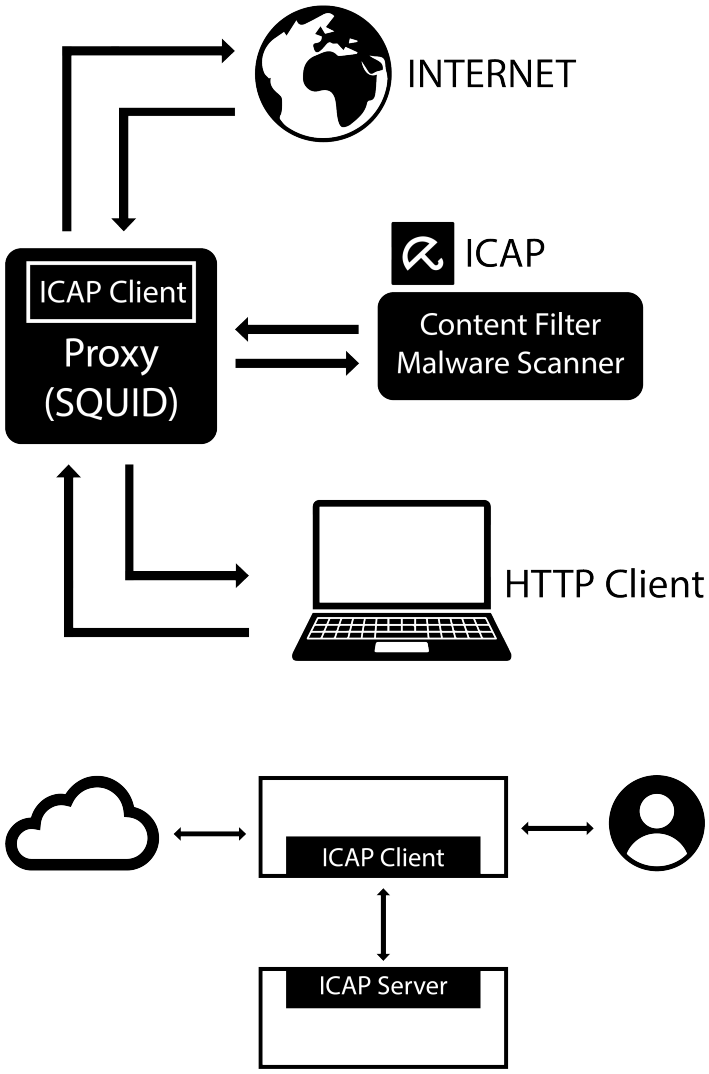
Der ICAP-Server von AVIRA wurde mit NoSpamProxy getestet und ist als Option für NoSpamProxy über Net at Work als OEM-Produkt bestellbar. Eine vorhandene Lizenz/Instanz von Avira av-icapd kann genutzt werden, so dass ein Neukauf nicht erforderlich ist.

Die ICAP-Client-Schnittstelle ist standardmäßig in NoSpamProxy Protection enthalten. Eine zusätzliche Lizenz oder Option ist nicht erforderlich.

E-Mail-Gateways wie NoSpamProxy sind ein Standardelement der Sicherheitsarchitektur eines Unternehmens. Sie sind für die immer komplexer werdende Verarbeitung ein- und ausgehender E-Mails zuständig. Neben der Prüfung auf Schadcodefreiheit werden die Spamabwehr und die Bearbeitung von Inhalten immer aufwändiger.

Zusätzlich werden Funktionen wie Virenprüfung auch von anderen Proxydiensten benötigt, so dass die zentrale Nutzung eines Scanner-Dienstes (und der Lizenz) auch wirtschaftlich sehr interessant ist.

Hierzu wurde das Internet Content Adaption Protocol (kurz: ICAP) als IETF-Standard entwickelt. Dabei kann der Proxyserver (hier: NoSpamProxy) als ICAP-Client Inhalte zur Prüfung an einen ICAP-Server senden und erhält von diesem das Prüfungsergebnis zurück.




Virenscanner mit ICAP-Schnittstelle werden von den meisten AV-Herstellern angeboten. Auch der deutsche Hersteller AVIRA hat einen ICAP-Server im Programm und ist OEM-Partner von Net at Work.

## Trennung von Aufgaben und Performancesteigerung

Die Funktionen "Durchsetzen der Richtlinie" für NoSpamProxy einerseits und "Bewertung des Inhalts auf Virenfreiheit" auf dem ICAP-Server andererseits sind bewusst getrennt: Das Scannen des Inhalts auf Viren verursacht in der Regel eine höhere Last. Mit der Auslagerung erreicht man eine Entlastung des Gateways. Zur Steigerung des Durchsatzes in größeren Unternehmen kann ein Proxyserver meist auch mehrere Scanner-Server nutzen: Die Last wird auf noch mehr Schultern verteilt. Auch ist das Gesamtsystem besser gegen Ausfall eines Servers geschützt. Wirklich große Installationen nutzen meist zusätzlich Loadbalancer, um die Leistung der Proxyserverfarm noch weiter zu steigern.

## Besondere Vorteile

Der AVIRA ICAP-Server kann nicht nur die Daten scannen, sondern auch noch bewerten: Je nach Kategorie der Schadsoftware kann NoSpamProxy dann entscheiden, was zu tun ist.

Eine weitere besondere Funktion ist das Trickeling: Wenn eine große Datenmenge zu prüfen ist, meldet sich der Scanner mit einer Antwort beim einliefernden Server zurück, so dass die Verbindung nicht abreißt. Kleine Datenhäppchen werden schon zurückgegeben, während der Scanner im Hintergrund noch arbeitet. NoSpamProxy weiß so, dass seine Anfrage immer noch bearbeitet wird und läuft nicht in ein Timeout. Parallel kann die Bearbeitung der nächsten E-Mails in NoSpamProxy weiterlaufen.

# Installation und Inbetriebnahme

## Installation des AVIRA ICAP-Servers

Der AVIRA ICAP-Server wird von Net at Work als Virtuelle Appliance auf der Basis von Debian 8 (LTS bis 05/20) Linux ausgeliefert. Es handelt sich dabei um ein gehärtetes Betriebssystem, auf dem nur der ICAP-Dienst läuft.

> **HINWEIS:** Der SSH-Dienst ist standardmäßig deaktiviert und kann nur vom Support aktiviert werden.

1. Erstellen Sie einen neuen, leeren virtuellen Computer in Hyper-V, VMWare ESXi oder Citrix Xen.

   > **HINWEIS:** Vergeben Sie mindestens einen CPU-Kern sowie 2GB RAM. Unsere Empfehlung ab 2500 E-Mails pro Stunde sind 4GB RAM sowie zwei CPU-Kerne.

2. Binden Sie das vorgefertigte HDD-Image des AVIRA ICAP-Servers in den leeren virtuellen Computer ein.

   > **HINWEIS:** Sollten Sie Hyper-V einsetzen, wählen Sie bitte bei der Erstellung **Gen 1**. Alle optionalen Tools zur Virtualisierung sind bereits installiert.

Das HDD-Image enthält bereits Ihren Lizenzierungscode. Dies gilt sowohl für die 30 Tage gültige Testlizenz als auch für erworbene Lizenzen. Zur Sicherstellung der Kompatibilität wird das HDD-Image auf einer IDE-HDD ausgeliefert.

Alle wichtigen Betriebsystemupdates werden jede Nacht automatisch installiert. Alle 10 Minuten wird auf das Vorliegen neuer Virensignaturen oder Updates zum ICAP-Dienst geprüft. Diese Virensignaturen werden automatisch bezogen, falls vorhanden.

> **HINWEIS:** Für die Betriebssystemupdates benötigt der virtuelle Computer eine Verbindung über Port 80 ins Internet. Für die Aktualisierung der Virensignaturen wird eine Verbindung über Port 443 auf **avira.nospamproxy.de** benötigt.

> **HINWEIS:** Avira verwendet für die Verbindung den TCP-Port 1344 sowie den Dienst **service_scanner**.

# Inbetriebnahme des AVIRA ICAP-Servers

### Einrichtung des ICAP-Servers

1. Schalten Sie den virtuellen Computer ein.
2. Loggen Sie sich mit den folgenden Daten ein:
   User: **nsp**
   Passwort: **nsp**
3. Setzen Sie ein neues Passwort für den User NSP, indem Sie folgenden Aufruf ausführen:
   `nsp@avira:~$ passwd`

### Einrichtung der Netzwerkkarte

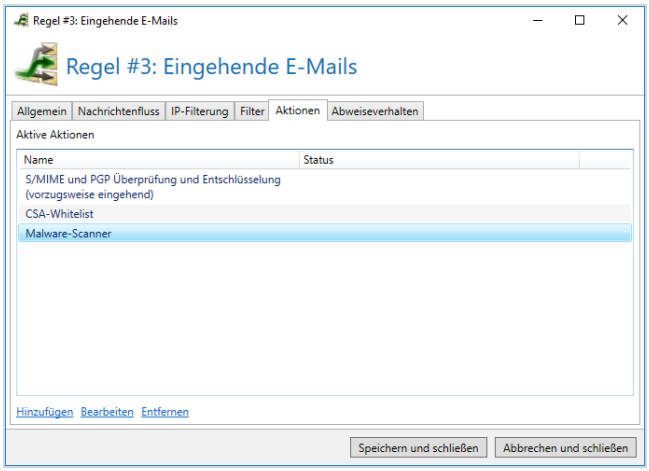
1. Setzen Sie folgenden Befehl ab:
   `root@avira:~# nano /etc/network/interfaces`
2. Binden Sie das Interface nun entweder statisch oder per DHCP ein.
   - statisch:
     ```
     auto eth0
     iface eth0 inet static
     address 172.8.0.7
     netmask 255.255.0.0
     gateway 172.8.0.1
     ```
   - DHCP:
     ```
     auto eth0
     iface eth0 inet dhcp
     ```
3. Speichern Sie die Einstellungen mit **STRG + O**.
4. Tragen Sie einen DNS-Server ein:
   `root@avira:~# nano /etc/resolv.conf`
5. Starten Sie den virtuellen Computer neu:
   `nsp@avira:~$ /sbin/reboot`

Der AVIRA ICAP-Server kann nun von NoSpamProxy als ICAP-Client angesprochen werden.

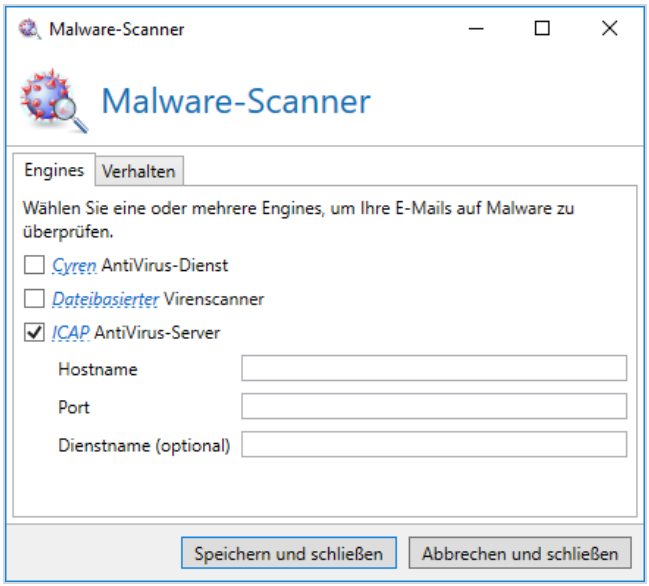
# Anbindung in NoSpamProxy

Damit NoSpamProxy® E-Mail-Anhänge zur Prüfung an einen ICAP-Server senden kann, müssen Sie den ICAP AntiVirus-Server in der entsprechenden Regel aktivieren:

1. Öffnen Sie die gewünschte Regel für eingehende E-Mails.




2. Öffnen Sie die Aktion **Malware-Scanner**.




3. Setzen Sie auf der Registerkarte **Engines** das Häkchen bei **ICAP AntiVirus-Server**.

4. Geben Sie die erforderlichen Daten ein.
5. Klicken Sie **Speichern und schließen**.

Auf dem ICAP-Server finden Sie nun ein Log. Um dieses Log zu öffnen, geben Sie den folgenden Befehl in die Kommandozeile ein:

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

Der Befall einer E-Mail würde ebenfalls im Log stehen:

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

Um nach allen Befunden zu suchen, geben Sie den folgenden Befehl ein:

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

# Hilfe und Unterstützung

### Knowledge Base

Die **Knowledge Base** enthält weiterführende technische Informationen zu unterschiedlichen Problemstellungen.

### Website

Auf der **NoSpamProxy-Website** finden Sie Handbücher, Whitepaper, Broschüren und weitere Informationen zu NoSpamProxy.

### NoSpamProxy-Forum

Das **NoSpamProxy-Forum** gibt Ihnen die Gelegenheit, sich mit anderen NoSpamProxy-Anwendern auszutauschen, sich zu informieren sowie Tipps und Tricks zu erhalten und diese mit anderen zu teilen.

### Blog

Das **Blog** bietet technische Unterstützung, Hinweise auf neue Produktversionen, Änderungsvorschläge für Ihre Konfiguration, Warnungen vor Kompatibilitätsproblemen und vieles mehr. Die neuesten Nachrichten aus dem Blog werden auch auf der Startseite des NoSpamProxy Command Center angezeigt.

### YouTube

In unserem **YouTube-Kanal** finden Sie Tutorials, How-tos und andere Produktinformationen, die Ihnen das Arbeiten mit NoSpamProxy erleichtern.

## NoSpamProxy-Support

Unser Support-Team erreichen Sie

- per Telefon unter **+49 5251304-636**
- per E-Mail unter **support@nospamproxy.de**.