NoSpamProxy

PROTECTION. ENCRYPTION. LARGE FILES.

Produktbeschreibung ICAP-Client und AVIRA ICAP-Server

Inhalt

NoSpamProxy als ICAP-Client

NoSpamProxy® 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. Es ist jedoch im Einzelfall zu testen oder beim Hersteller zu erfragen, ob der Virenscanner das ICAP-Protokoll korrekt und im erforderlichen Funktionsumfang implementiert hat.

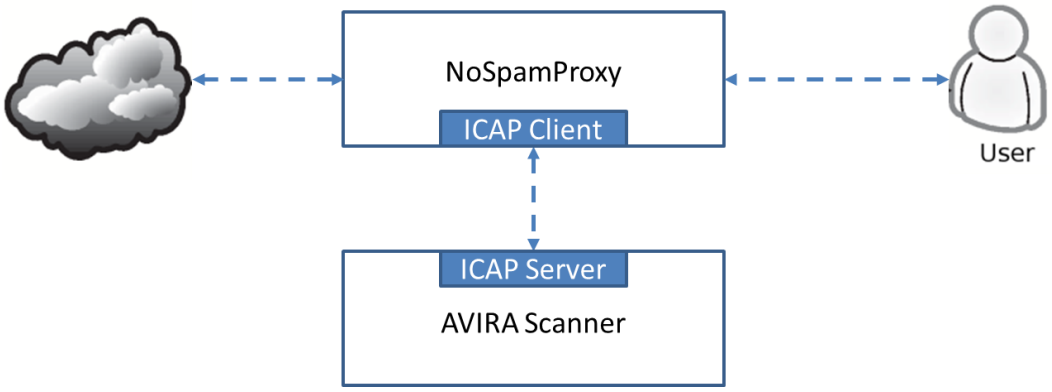
Der ICAP-Server von AVIRA wurde mit NoSpamProxy getestet und ist als Option für NoSpamProxy über Net at Work als OEM-Produkt bestellbar. Eine vorhandene Lizenz/Instanz von Avira av-icapd kann genutzt werden und ein Neukauf ist nicht erforderlich.

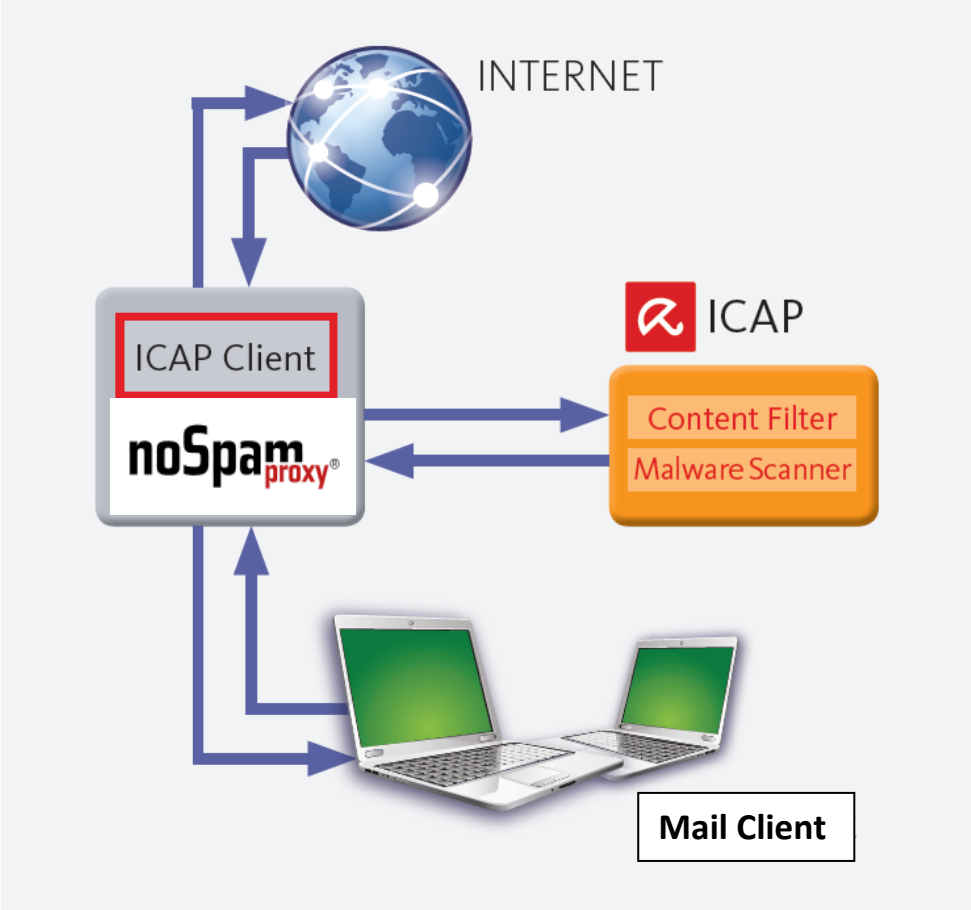
Alle NoSpamProxy-Module (Protection, Encryption, Large Files) enthalten die ICAP-Client-Schnittstelle. Eine zusätzliche Lizenz oder Option ist nicht erforderlich. Eine Einschränkung besteht bezüglich Large Files: Dateien, die im Web-Portal liegen, können nicht durch den ICAP Server geprüft werden.

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

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 hier um ein gehärtetes OS, auf dem nur der ICAP-Dienst läuft. Der SSH-Dienst ist deaktiviert und kann nur vom Support aktiviert werden.

Im Hyper-V, VM Ware ESXi oder Citrix Xen wird eine leere VM Hülle erstellt. Hier müssen mindestens 1 CPU-Kern sowie 2GB RAM vergeben werden. Unsere Empfehlung ab 2500 Mails in der Stunde sind 4GB RAM sowie 2 CPU-Kerne.

Der AVIRA ICAP-Server wird als ein vorgefertigtes HDD-Image ausgeliefert, das auch bereits Ihren Lizenzierungscode enthält – dies gilt sowohl für die 30 Tage gültige Testlizenz, als auch für erworbene Lizenzen. Dieses muss dann lediglich in die leere VM Hülle eingebunden werden. Aufgrund der Kompatibilität haben wir uns für eine IDE HDD entschieden. Sollten Sie Hyper-V einsetzen so wählen Sie bitte bei der Erstellung „Gen 1“. Alle optionalen Tools zur Virtualisierung sind bereits installiert.

Alle wichtigen Betriebsystemupdates werden jede Nacht automatisch installiert. Alle 10 Minuten wird auf das Vorliegen neuer Virensignaturen oder Updates zum ICAP-Dienst geprüft und bezogen. Für die Betriebsystemupdates benötigt die Maschine eine Verbindung über Port 80 ins Internet. Für die Aktualisierung der Virensignaturen wird eine Verbindung über Port 443 auf avira.nospamproxy.de benötigt.

Betrieb

Nach dem Einschalten der virtuellen Maschine können Sie sich mit folgenden Daten einloggen:

User: nsp

Passwort: nsp

Nach dem Login werden Ihnen die wichtigen Befehle mit roter Schrift angezeigt.

Bitte setzen Sie zunächst umgehend ein neues Passwort für den User: NSP! Dies machen Sie mit dem Aufruf: passwd

```
nsp@avira:~$ passwd
Changing password for nsp.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Darauf folgt die Einrichtung der Netzwerkkarte, dazu setzen Sie bitte diesen Befehl ab:

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

Hier gibt es dann zwei Möglichkeiten das Interface einzubinden: statisch oder per DHCP

DHCP:

```
auto eth0
iface eth0 inet dhcp
```

Statisch:

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

Wenn Sie die Einstellung gemacht haben, benutzen Sie bitte zum Speichern: STRG + O

Abschließend tragen Sie bitte einen DNS Server ein:

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

Nachdem alle Einstellungen vorgenommen wurden, starten Sie die Maschine neu:

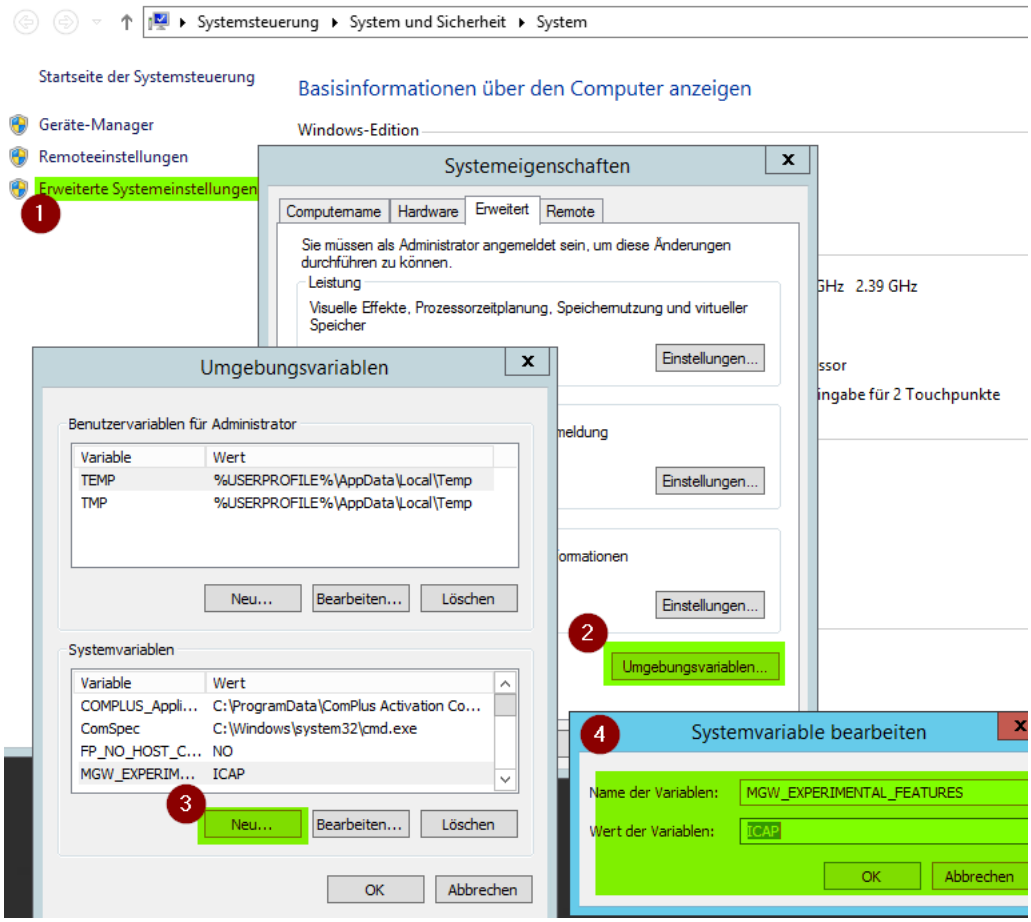
```
nsp@avira:~$ /sbin/reboot
```

Der AVIRA ICAP-Server ist nun bereit von NoSpamProxy als ICAP-Client angesprochen zu werden.

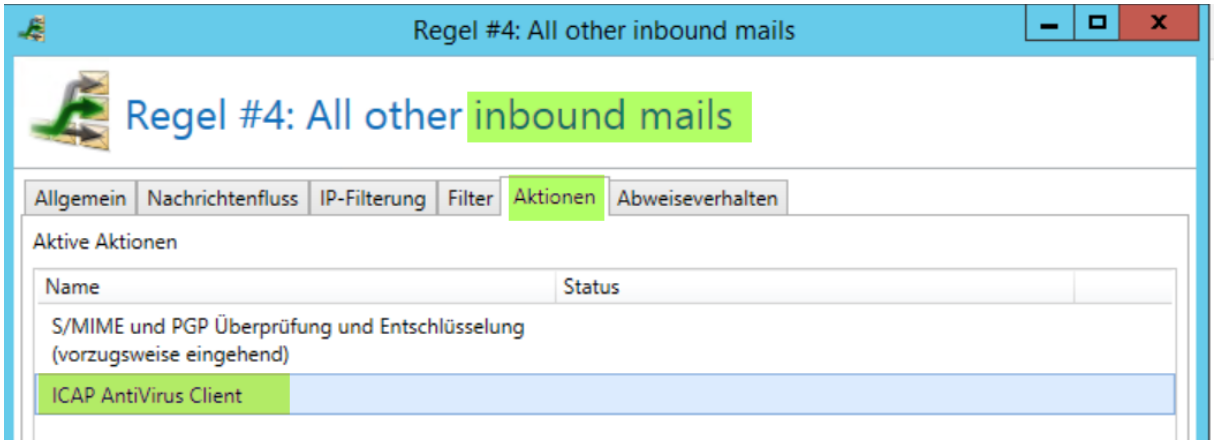
Anbindung im NoSpamProxy

Damit NoSpamProxy E-Mail-Anhänge zur Prüfung an einen ICAP-Server sendet, sind folgende Schritte erforderlich:

Aktivieren Sie bitte die ICAP-Variable:



Bitte fügen Sie in einer der eingehenden Regeln unter Aktionen dies hinzu:



- klicken dann auf speichern
- stoppen die Intranet Rolle über die MMC
- öffnen mit einem Editor, der Admin-Rechte hat:

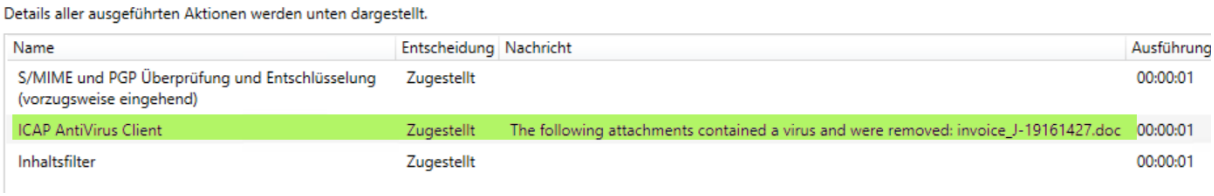
  %programdata%\Net at Work Mail Gateway\Configuration\Intranet Role.config

- suchen dort nach „icap“ und befüllen die leeren Felder.
  Bei der Action gibt es nun zwei Möglichkeiten:
  Remove: entfernt den Anhang, lässt die Mail durch
  Block: blockiert die Mail

```
<icapAV action="Remove" hostName="172.8.0.7" port="1344" serviceName="service_scanner" />
```

- **Wichtig:** speichern Sie nun die Datei und schließen den Editor, da sonst die Datei im Schreibschutz verbleibt!
- Staren Sie die Intranet Rolle über die MMC.
- Als letztes gehen Sie noch einmal über die GUI in die geänderte Regel, öffnen diese und klicken auf Speichern. Dadurch wird die Replikation auf die Gateway-Rollen ausgelöst.

Sofern alles korrekt eingebunden ist und ein Virus gefunden wurde, sehen Sie in der Nachrichtenverfolgung unter den ausgeführten Aktionen folgendes:


Details aller ausgeführten Aktionen werden unten dargestellt.

Name	Entscheidung	Nachricht	Ausführung
S/MIME und PGP Überprüfung und Entschlüsselung (vorzugsweise eingehend)	Zugestellt		00:00:01
ICAP AntiVirus Client	Zugestellt	The following attachments contained a virus and were removed: invoice_J-19161427.doc	00:00:01
Inhaltsfilter	Zugestellt		00:00:01

Auf dem ICAP-Server finden Sie direkt ein Log und öffnen dies mit dem Befehl:

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

Hier würde dann der Befall der Mail ebenfalls im Log stehen:

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

Sie können auch direkt nach allen Befunden suchen lassen:

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

Kontakt

Sie haben noch Fragen zum Produkt, zur Technik oder zu Preisen? Sprechen Sie uns jederzeit gerne an!

Vertrieb:

Tel. 05251-304-600

sales@nospamproxy.de

Support:

Tel.: 05251-304-636

support@nospamproxy.de

Net at Work GmbH
Am Hoppenhof 32a
33104 Paderborn