**Securepoint GmbH**
Bleckeder Landstraße 28, 21337 Lüneburg
**Tel.: 0 41 31 / 24 01-0**
www.securepoint.de | info@securepoint.de

# Securepoint HOWTO
# Filterung von Office Dokumenten

V1.02 – Autor: Eric Kaiser – 24.02.2016

## Einstellungsempfehlung zur Abwehr des Verschlüsselungstrojaner „Locky“ oder ähnlichen Gefahren, die sich per Office-Dokumente verbreiten.

Bei korrekter Konfiguration der Securepoint NextGen UTM-Firewall wird Schadcode, wie der gefährliche Verschlüsslungstrojaner „Locky“, erkannt und aus E-Mails und HTTP-Anfragen gefiltert. Im Falle eines massiven Ausbruchs eines solchen Virus und bei hoher Mutationsgeschwindigkeit, kann es sinnvoll sein potentiell gefährliche Dateien generell aus dem Datenstrom heraus zu filtern. Die hierfür notwendigen Konfigurationsschritte werden im Folgenden Schritt für Schritt erklärt.

Diese Maßnahme ist lediglich eine zusätzliche Option aus einem ganzheitlichen Maßnahmenkatalog, die Sie für die Sicherheit bei Ihren Kunden anwenden. Eine Übersicht empfohlener Maßnahmen finden Sie z. B. bei Heise http://www.heise.de/security/meldung/Krypto-Trojaner-Locky-Was-tun-gegen-den-Windows-Schaedling-3112408.html

Mit der Securepoint UTM-Firewall lassen sich gefährdete Dokumente komplett aus dem Datenstrom für E-Mail und HTTP herausfiltern. Die folgende Anleitung zeigt Ihnen wie Sie dies auf der Securepoint NextGen UTM-Firewall (hier Version 11.6.2) realisieren.

sa

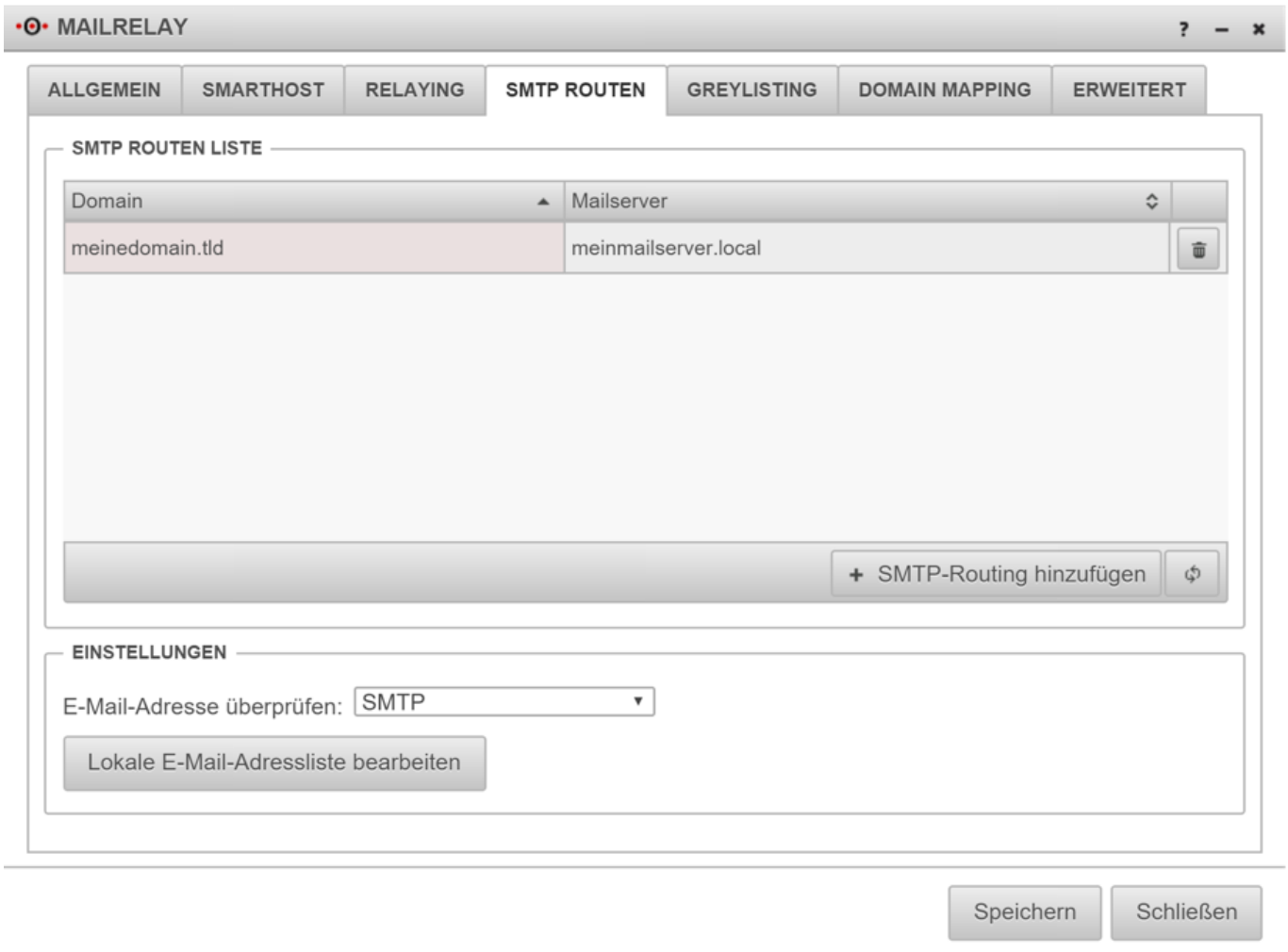
## E-Mail

***Empfehlungen für SMTP***
Wir empfehlen, wo immer möglich, SMTP als Zustellungsmethode für E-Mail zu wählen.

Bei SMTP-E-Mail-Zustellung sind folgende Einstellungen wichtig:

Unter „Anwendungen" -> „Mailrelay" achten Sie bitte auf folgende Einstellungen:

Im Reiter SMTP-Routen achten Sie darauf, dass Sie die E-Mail-Adressprüfung aktiv haben.

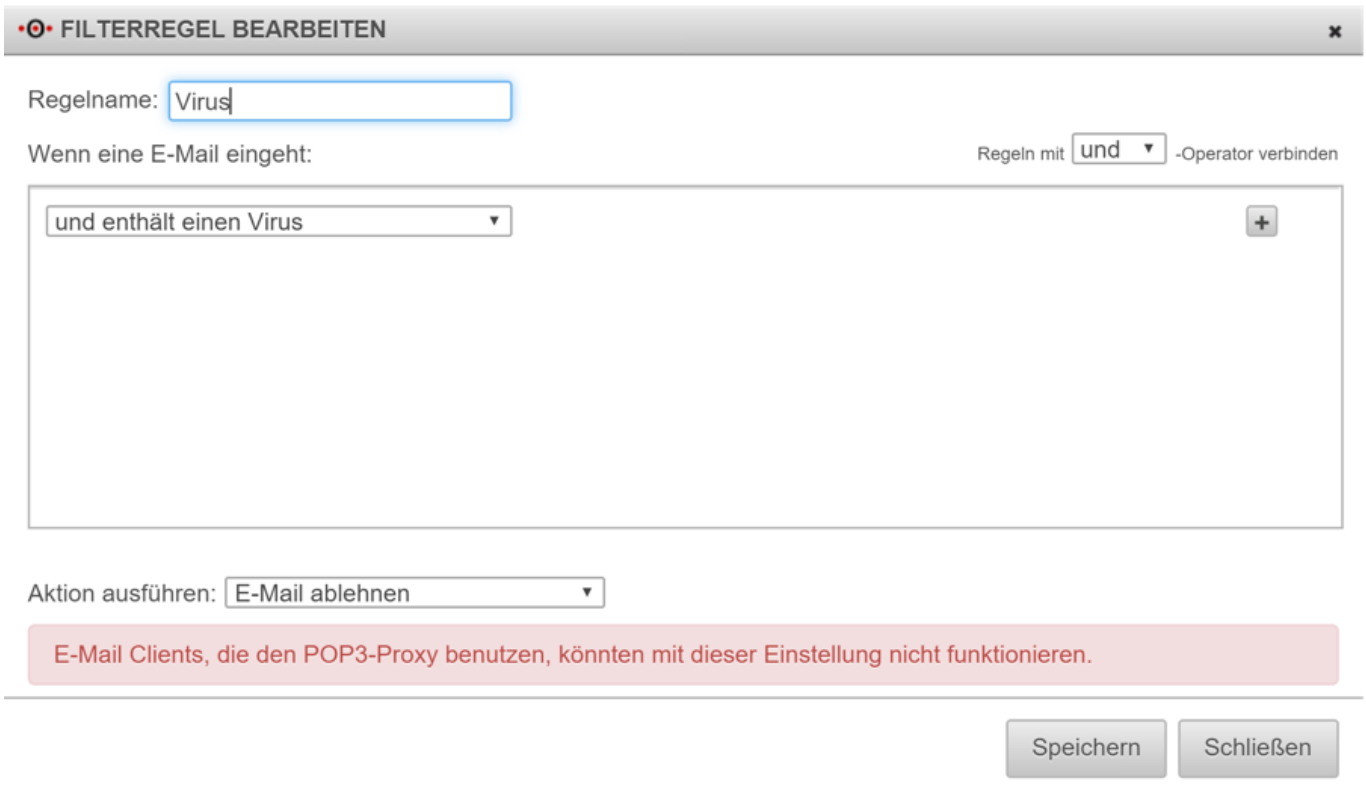


Im Reiter „Erweitert" aktivieren Sie bitte den Punkt „Recipient flooding verhindern".


Außerdem wird empfohlen, Greylisting zu verwenden.

Im Mailfilter sind folgende Einstellungen notwendig.

Erstellen Sie eine Regel, die Viren ablehnt oder verwirft:

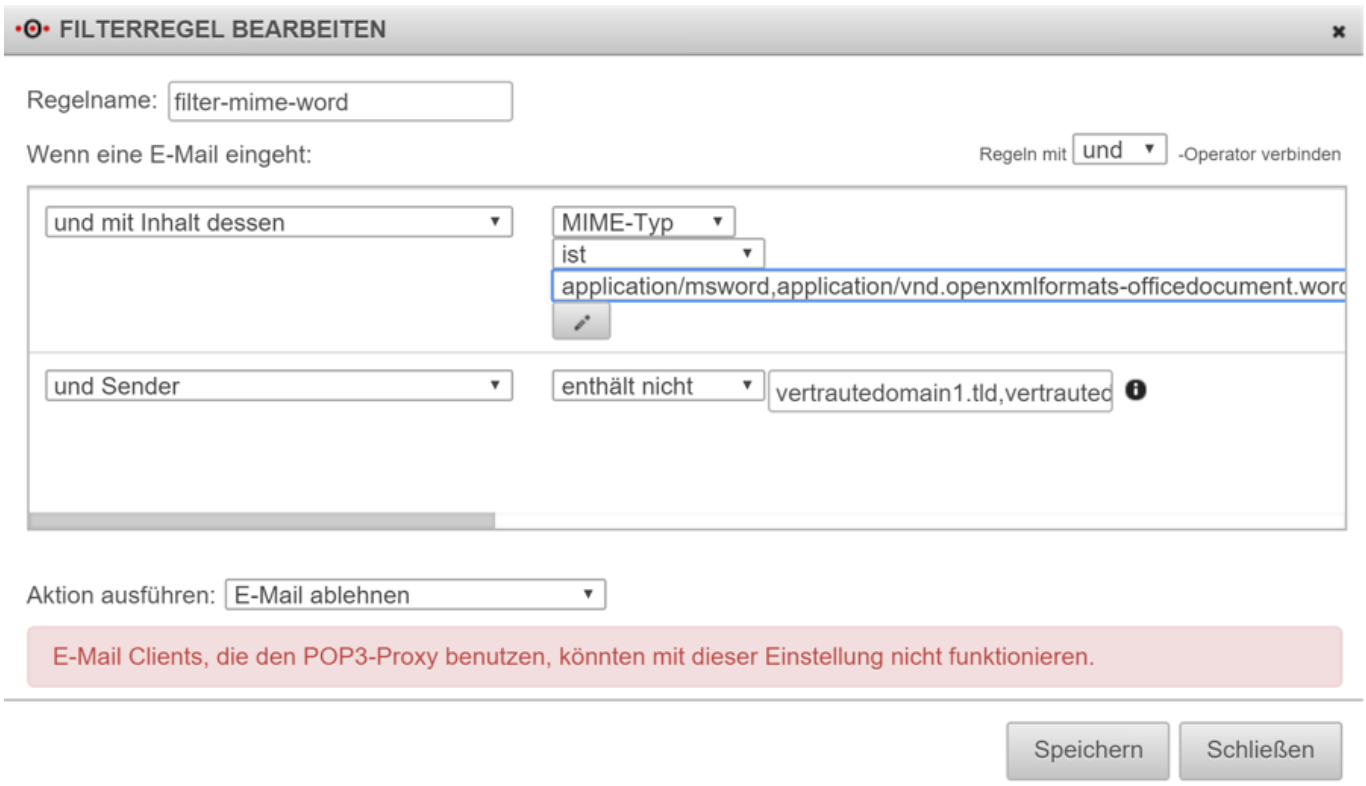


Wie oben schon beschrieben, kann es einem massiven Virenausbruch oder einer hohen Mutationsrate eines Virus sinnvoll sein, alle gefährdeten Dateien aus den E-Mail und HTTP-Datenströmen zu filtern.
Dies kann auf Basis des MIME-Types einer Datei und auf Basis der Dateiendung erfolgen.

**Ablehnen von Word-Dokumenten auf Basis des MIME-Types**
Legen Sie einen neuen Filter an. Bei MIME-Type klicken Sie auf das Stift-Symbol und geben folgende Liste ein:

```
application/msword,application/vnd.openxmlformats-
officedocument.wordprocessingml.document,application/vnd.openxmlformats-
officedocument.wordprocessingml.template,application/vnd.ms-
word.document.macroEnabled.12,application/vnd.ms-word.template.macroEnabled.12
```

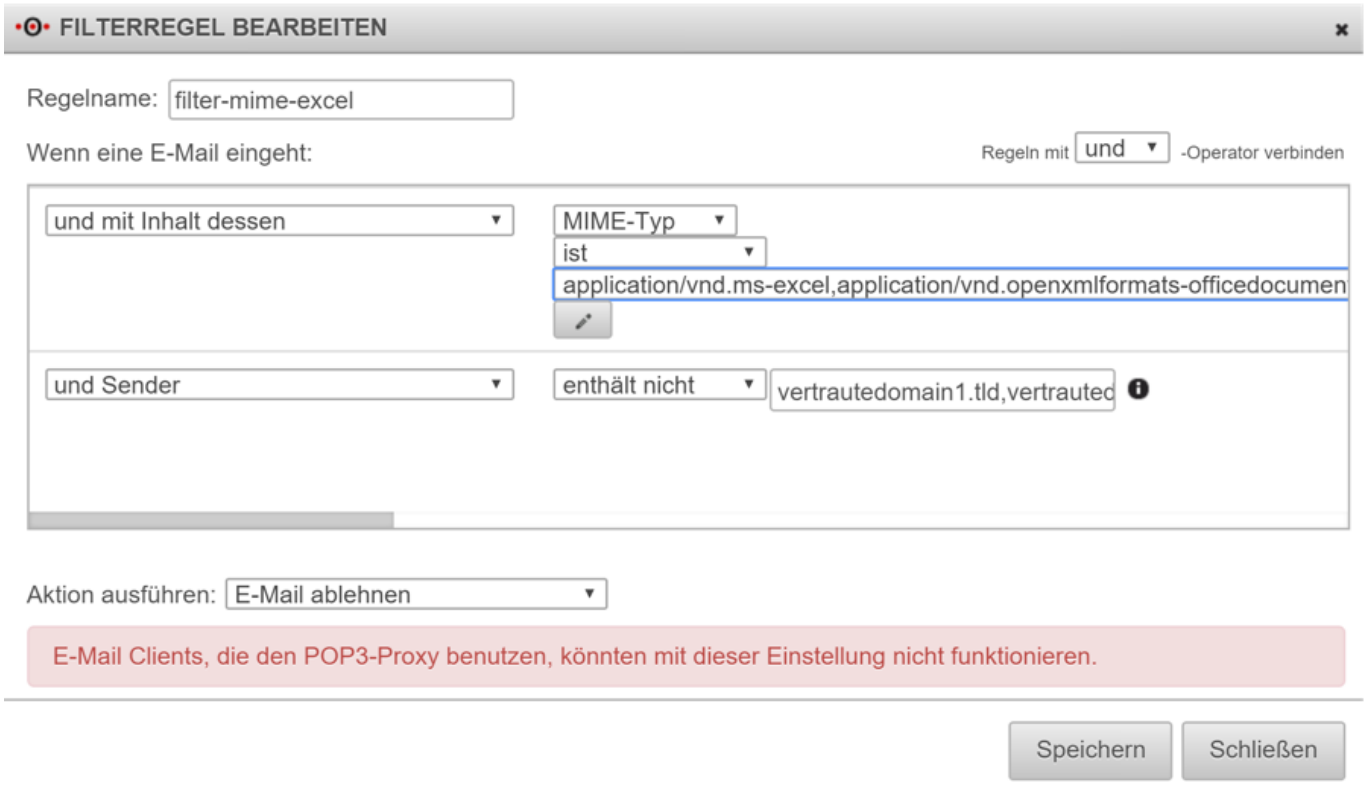
Wenn Sie von definierten Domains doch E-Mails mit dem aufgelisteten MIME-Type empfangen wollen, dann müssen Sie dies wie unten angezeigt einstellen. Hier können Sie mehrere Domains angeben - diese müssen mit einem Komma voneinander getrennt werden.



**Ablehnen von Excel-Dokumenten auf Basis des MIME-Types**
Legen Sie einen neuen Filter an. Bei MIME-Type klicken Sie auf das Stift Symbol und geben folgende Liste ein:

```
application/vnd.ms-excel,application/vnd.openxmlformats-
officedocument.spreadsheetml.sheet,application/vnd.openxmlformats-
officedocument.spreadsheetml.template,application/vnd.ms-
excel.sheet.macroEnabled.12,application/vnd.ms-
excel.template.macroEnabled.12,application/vnd.ms-
excel.addin.macroEnabled.12,application/vnd.ms-excel.sheet.binary.macroEnabled.12
```

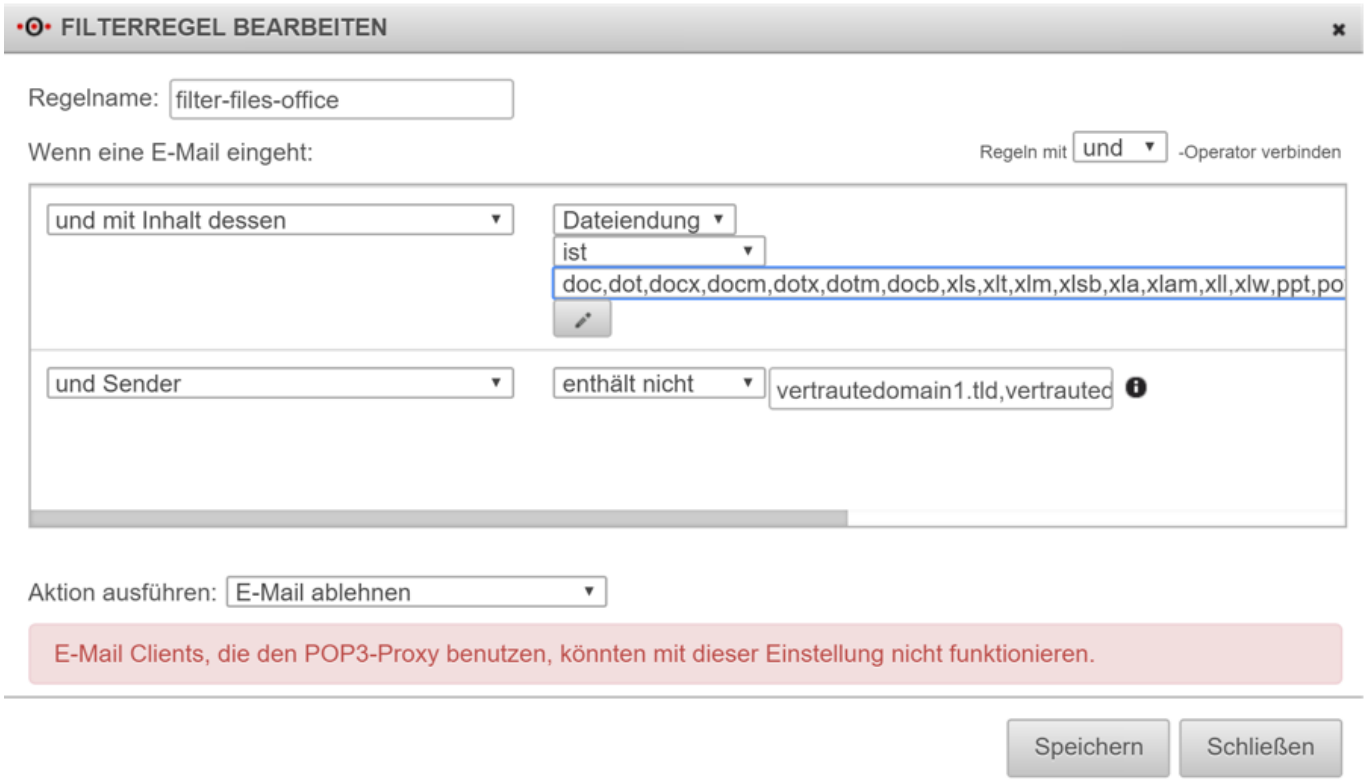
Wenn Sie von definierten Domains doch E-Mails mit dem aufgelisteten MIME-Type empfangen wollen, dann müssen Sie dies wie unten angezeigt einstellen. Hier können Sie mehrere Domains angeben - diese müssen mit einem Komma voneinander getrennt werden.



**Zusätzlich ist es angebracht, Dokumente auch auf Basis der enthaltenen Dateiendung zu verwerfen. Hier das Beispiel, um eine Liste von Office-Dokumenten zu sperren**
In diesem Beispiel wurde bei Dateiendung die folgende Liste verwendet - diese können Sie natürlich Ihren Anforderungen entsprechend anpassen:

```
doc, dot, docx, docm, dotx, dotm, docb, xls, xlsx, xlt, xlm, xlsb, xla, xlam, xll,
xlw, ppt, pot, pps, pptx, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, pub
```

Wenn Sie von definierten Domains doch E-Mails mit dem aufgelisteten Dateierweiterungen empfangen wollen, dann müssen Sie dies wie unten angezeigt einstellen. Hier können Sie mehrere Domains angeben - diese müssen mit einem Komma voneinander getrennt werden.

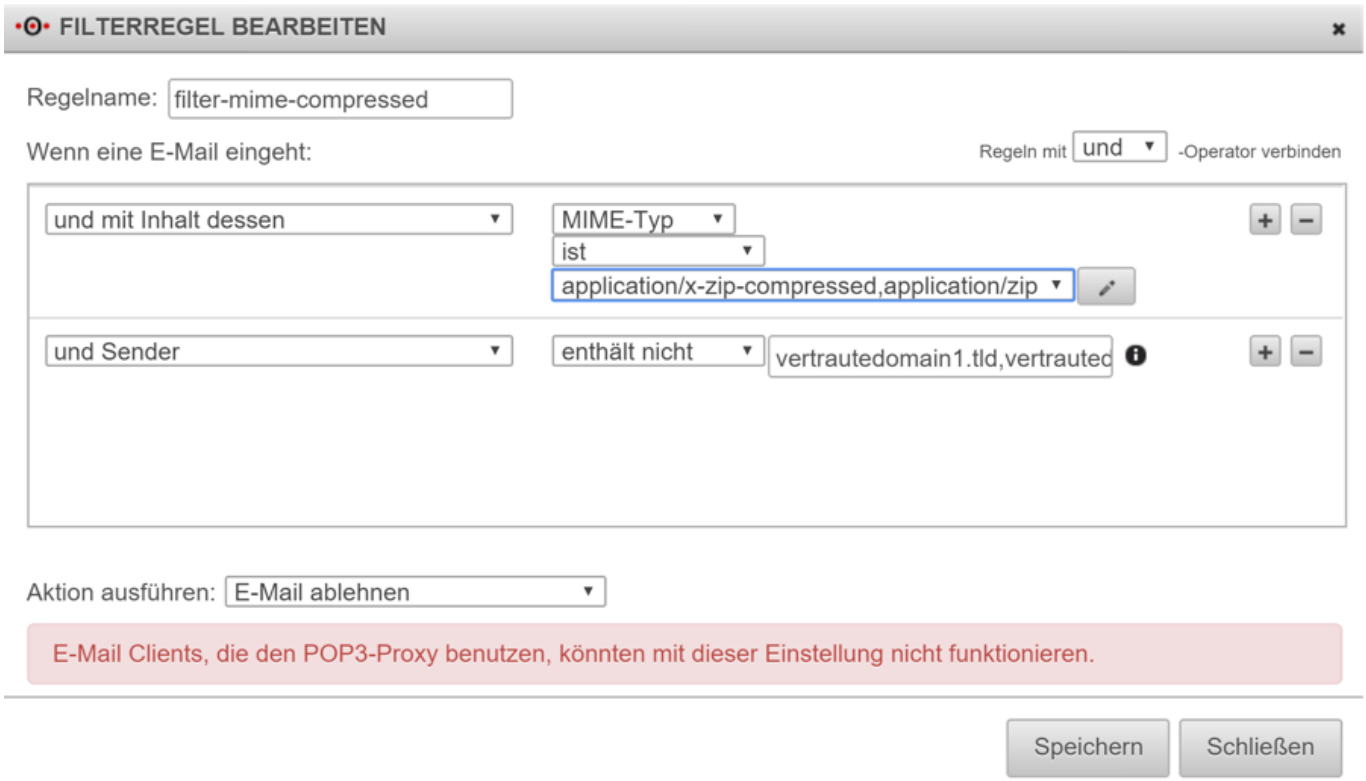


**ZIP und Co. blocken**
Hier finden Sie das korrespondierende Beispiel, um komprimierte Dateien zu blocken.

**Ablehnen von komprimierten Dateien auf Basis des MIME-Type**
Legen Sie auch hier einen neuen Filter an. Bei MIME-Type klicken Sie auf das Stift Symbol und geben folgende Liste ein:

```
application/x-zip-compressed,application/zip
```

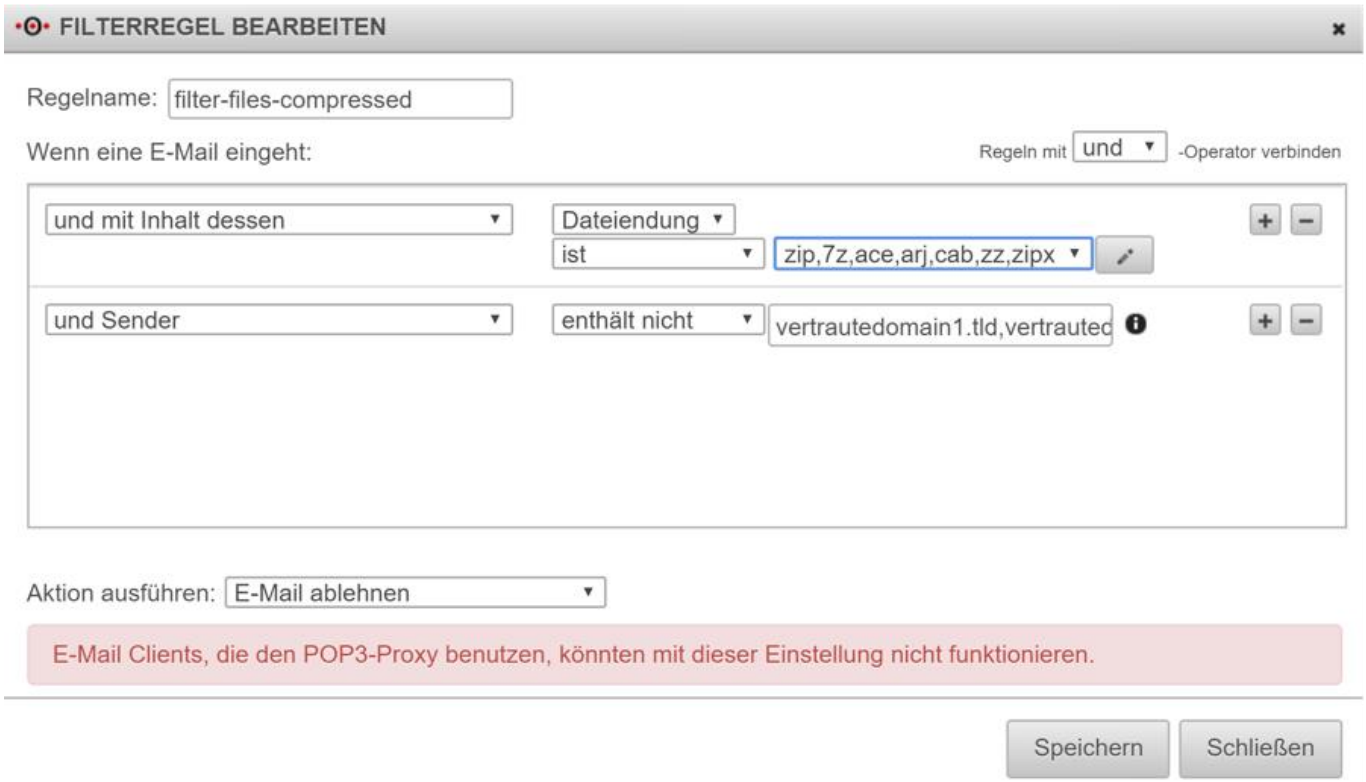
Wenn Sie von definierten Domains doch E-Mails mit dem aufgelisteten MIME-Type empfangen wollen, dann müssen Sie dies wie unten angezeigt einstellen. Hier können Sie mehrere Domains angeben - diese müssen mit einem Komma voneinander getrennt werden.



**Und hier noch die Sperrung von komprimierten Dateien auf Basis der Endung**
Bitte geben Sie bei Dateiendung die folgende Liste ein:

```
zip, 7z, ace, arj, cab, zz, zipx
```

Wenn Sie von definierten Domains doch E-Mails mit dem aufgelisteten Dateierweiterungen empfangen wollen, dann müssen Sie dies wie unten angezeigt einstellen. Hier können Sie mehrere Domains angeben - diese müssen mit einem Komma voneinander getrennt werden.




Zusätzlich wird empfohlen, SPAM und Viren-E-Mails abzulehnen.
E-Mails der Kategorie „Probably Spam" sollten in die Quarantäne verschoben oder abgelehnt werden.

***Empfehlung für Mail-Connector***
Wenn Sie den Mail-Connector verwenden, ist E-Mail ablehnen für gefilterte Dokumente nicht die richtige Wahl. Hier sollten Sie ggf. Quarantäne verwenden.

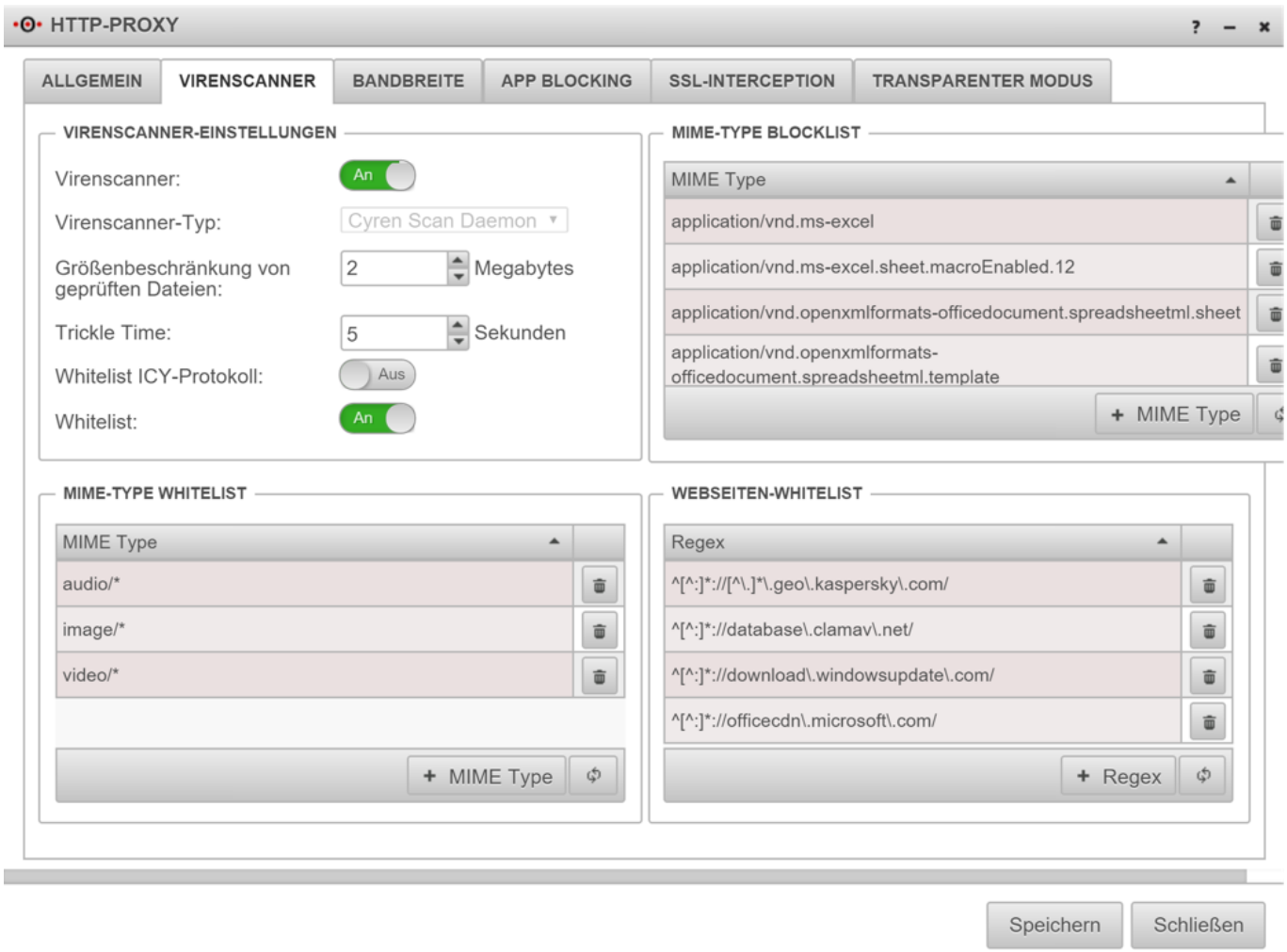
***Empfehlung für POP3-Proxy***
Die Möglichkeiten des Eingriffs beim POP3-Proxy sind begrenzt. E-Mails können nur vom Inhalt befreit oder im Betreff markiert werden. Für die gefilterten Dateitypen, MIME-Types und für Viren wird die Methode „Zutreffenden Inhalt filtern" empfohlen. Für SPAM die Methode „E-Mail im Betreff markieren mit".

***Schneller über die CLI***
Schneller können Sie die hier aufgeführten Filterregeln über die CLI einfüge. Dafür haben wir Ihnen unter folgendem Link die notwendigen Kommandos zusammengestellt.
http://wiki.securepoint.de/index.php/FAQ/UTM1000001

## HTTP-proxy

Je nach Verbreitungsart eines Schädlings, kann es zusätzlich notwendig sein, definierte Dateien auch beim Surfen im Internet heraus zu filtern. Dafür ist es natürlich notwendig, dass alle PCs im Netzwerk den Proxyserver für HTTP und HTTPs verwenden.

Entsprechende MIME-Types können Sie hier filtern über:
„Anwendungen" -> „HTTP-Proxy" -> „Virenscanner" -> „MIME-Type Blocklist"
Hier muss für jeden MIME-Type ein einzelner Eintrag erfolgen.




***Zusätzliche Hinweise zu Drive-by-Downloads – generelle Empfehlungen***
Es sollte sichergestellt werden, dass der Client den Proxy der Firewall benutzt und auf der Securepoint NextGen UTM-Firewall der Virenschutz aktiviert ist. Bekannter Schadcode wird hier erkannt und beim Download gelöscht.

Als zweites ist es wichtig, dass die Clientsysteme (Betriebssystem inkl. aller installierter Software) immer aktuell gepatcht sind. Denn oft werden bei solchen Drive-by-Downloads Sicherheitslücken des Clients ausgenutzt. Ein aktueller Virenschutz darf natürlich auf dem Client auch nicht fehlen.

Danach wird es je nach Umgebung beim Kunden spezifisch: Entweder man verwendet in allen Browsern Adblocker/Tracking-Blocker und/oder deaktiviert Javascript gleich komplett. Das bedeutet

im ersten Schritt natürlich einen erhöhten administrativen Aufwand, um bestimmte Seiten dann wieder zu whitelisten, aber ist angesichts der aktuellen Bedrohungslage doch zu empfehlen. Zusätzlich können auch über manuelle Anpassungen in der Konfiguration des HTTP-Proxys auf der Firewall nur noch bestimmte User-Agents zugelassen werden. So kann das nachladen von Schadcode ggf. verhindert werden, da hier der Standard Browser des Betriebssystems verwendet wird, die User aber immer Chrome, Firefox und Co. verwenden. Wenn man jetzt nur noch diese Useragents zulässt, ist die Schadsoftware nicht in der Lage weitere unheilbringende Software nachzuladen.

**Bitte beachten Sie:**
Diese Anleitung hat keinen Anspruch auf Vollständigkeit in Bezug auf Schadcode und aktuelle Bedrohungen. Diese Anleitung berücksichtigt keine Besonderheiten Ihrer Konfigurationen - diese müssen Sie entsprechend selber anwenden. Im Zweifel steht Ihnen unser Support gerne zur Verfügung.