SPAM Abwehr - Blacklists und Whitelists

In der letztem Ausgabe haben wir uns mit den allgemeinen Einstelloptionen beschäftigt, die uns in Domino zur Vermeidung des Missbrauchs der Domino SMTP Dienste für Spam Weiterleitungen geboten werden. Neben den Basiseinstellungen bietet Domino noch weiterführende Möglichkeiten, mit denen sie ihren Domino Server und das Netzwerk gegen SPAM schützen können.

Ein weiterer, wichtiger Bereich, wenn es um die Vermeidung von SPAM Mails geht, sind die so genannten Blacklists. Bei einer Blacklist handelt es sich um ein Verzeichnis solcher Adressen, von denen keine Mails empfangen werden sollen. Neben öffentlichen Blacklists (auch als „SPAM Reports bezeichnet), deren Inhalt aufgrund von allgemeinen Verstößen oder Meldungen zentral von darauf spezialisierten Unternehmen gepflegt wird, können wir uns auch eigene Blacklists erstellen, mit denen wir definieren können, von welchen Mail-Absendern wir keine Mails empfangen wollen (bzw. an die wir keine Mails zustellen möchten). Dies hört sich zunächst recht gut an – birgt aber auch einige Nachteile: Zum einen hat es in der Vergangenheit auch solche Fälle gegeben, in denen „unschuldige“ Mailversender in eine solche Blacklist aufgenommen wurden (zum Beispiel, weil sie die in diesem Artikel vorgeschlagenen Präventionseinstellungen nicht vorgenommen hatten und als Spam Verteiler missbraucht wurden). Zum anderen verwenden pfiffige Mailversender, also die Erfinder der SPAMs ständig wechselnde Mailadressen, so dass häufig Zweifel an der Aktualität der Blacklists deren Nutzen ein wenig schmälern. Nur ein Beispiel: In der Vergangenheit hat es auch schon einmal einen Fall gegeben, bei dem die Absenderadresse „@t-online“ als Spam-Verteiler erkannt und dementsprechend in einer weit verbreiteten, öffentlichen Blacklist aufgenommen wurde – die Folge können sie sich sicher vorstellen: kein Mailversand mehr an irgendeinen Benutzer, der diese Domäne verwendet hat.

Diese Beispiele sind kein striktes Votum gegen den Einsatz von Blacklists, ich möchte allerdings die Gelegenheit nutzen und eine weit verbreitete Meinung widerlegen, die besagt, dass Blacklists „DIE“ Lösung sind, wenn es um SPAM Vermeidung geht.

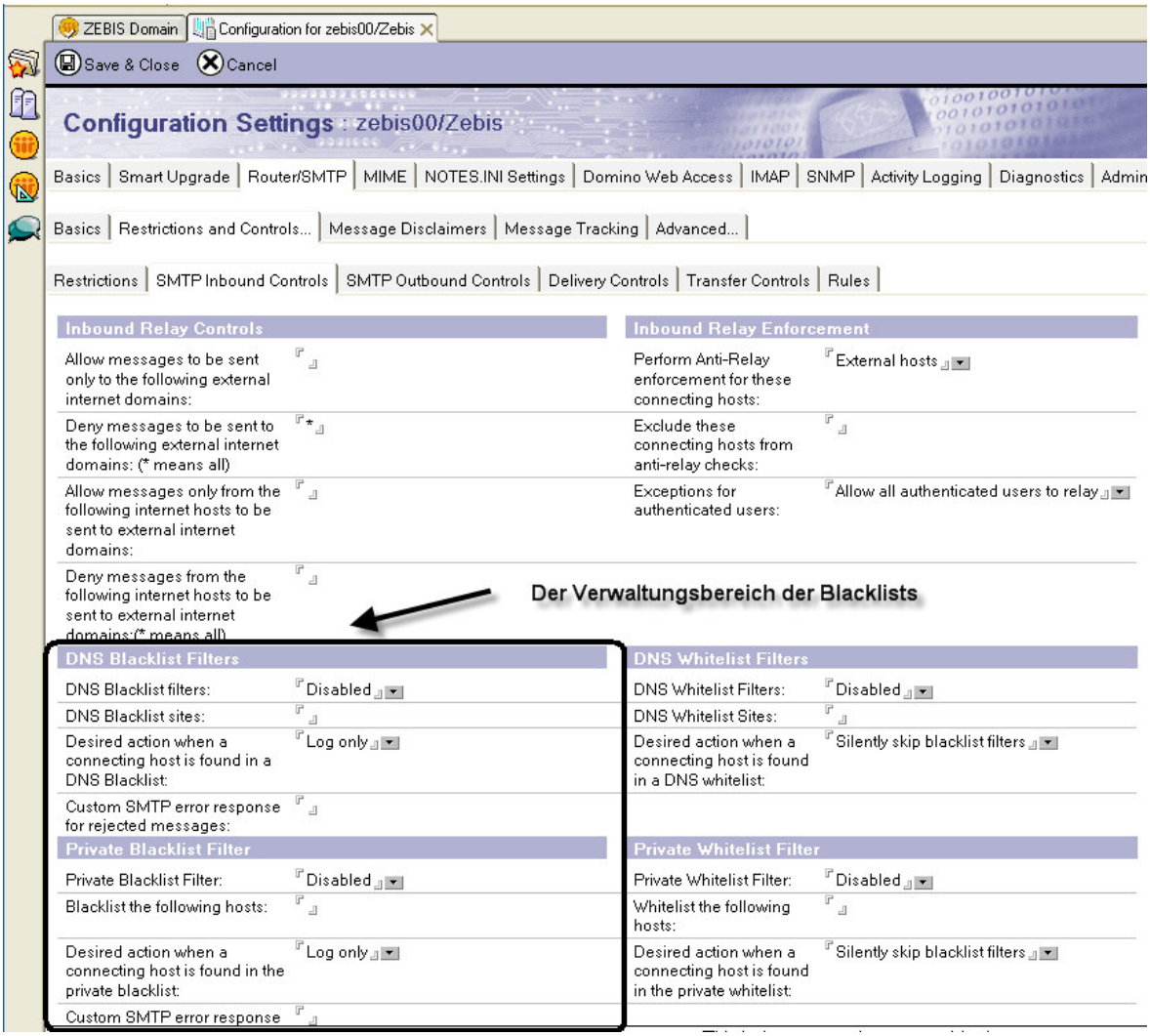
Die Kombination der verschiedenen Möglichkeiten ist es, was einen weitestgehenden Schutz gegen SPAMs bedeutet. Deshalb möchte ich in diesem Abschnitt auch die Unterstützung von Blacklists in Domino ansprechen und erläutern.

In Domino steht, ebenfalls wieder in dem Konfigurationsbereich „Mailing“ des Domino Servers, ein Bereich zur Definition der Blacklists zur Verfügung. Dort können wir DNS Blacklistfilter definieren, mit deren Hilfe jede eingehende SMTP Verbindung auf Einträge untersucht wird, die als SPAM-verdächtig gelten. Wird ein Eintrag einer solchen Blacklist bei der eigenen Mailverwaltung erkannt, dann wird automatisch eine Meldung an den Domino Administrator generiert, die einen Hinweis auf die Mail und den mutmaßlichen SPAM Verteiler enthält. Dies ist die Standardeinstellung, die es dem Administrator dann ermöglicht, nachträgliche Aktionen zu definieren. Mehr Sinn macht es – zumindest, wenn es nachweislich wirklich um SPAMs geht – wenn diese erst gar nicht weiter verarbeitet werden. Dazu sind zusätzliche Einstellungen in Domino erforderlich.

Hier ist eines zu erwähnen: Bei einer großen Anzahl Mails, die mit dem Domino Server verarbeitet werden, ist zu berücksichtigen, dass bei der Verwendung von externen Blacklists(also Blacklists, die sich auf einem Server im Internet befinden – ein Beispiel dazu finden sie unter *www.surbl.org*), unter Umständen Beeinträchtigungen in der Geschwindigkeit zu erwarten sind. Aus Performancegründen ist es außerdem ratsam, die Anzahl der in der Blacklist enthaltenen Einträge zu begrenzen, da jeder einzelne Eintrag verarbeitet wird – zumindest so lange, bis eine Übereinstimmung gefunden wurde. Um die Prüfungen nicht unnötig auszuweiten, werden nur solche Einträge verarbeitet, die auch in dem Bereich „SMTP inbound relay“ angegeben wurden.

Schauen wir uns zunächst den generellen Bereich in Domino für die Definition der Blacklists an. Dazu benötigen wir den Domino Administrator und eine Verbindung zu dem zu verwaltenden Domino Server. Die Blacklist Verwaltung finden wir in dem Bereich „Messaging“ und dort unter „

SMTP/Restrictions and Controls../SMTP Inbound Controls“. Schauen sie sich dazu auch die folgende Abbildung an.



01 Blacklist Verwaltung des Domino Servers

Diese Abbildung stammt aus der Version von Domino 7 und ist im Vergleich zu einer Version 6 leicht modifiziert. Wie sie erkennen können, sind die Angaben in Bezug auf die Blacklists in zwei Bereiche unterteilt: den DNS Blacklist Filter Bereich, mit dem wir im Wesentlichen die Angaben der öffentlichen Blacklists verwalten, und der Bereich der privaten Blacklists.

Beachten sie auch den Bereich der Whiteliste, der sich rechts in der Anzeige befindet. Die Whitelists haben in der letzten Zeit stark an Bedeutung gewonnen – ich werde später auf diese noch eingehen.

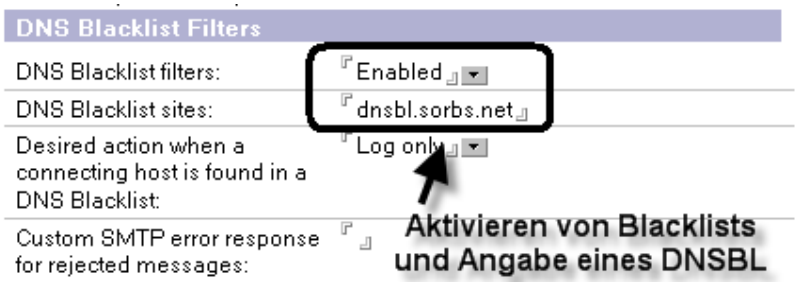
Bevor wir mit der Definition der Blacklists beginnen können, muss ein Konfigurationsdokument existieren. Sollte dieses noch nicht vorhanden sein, dann kann es in dem Bereich „Messaging“ und dort unter „ SMTP/Restrictions and Controls../SMTP Inbound Controls“ angelegt werden. Führen sie dort die gewünschten Einstellungen durch und speichern sie diese. Damit wird das Konfigurationsdokument generiert.

☝ Anmerkung

Sobald Änderungen an den SMTP Einstellungen durchgeführt wurden, muss der SMTP Dienst beendet und anschließend neu gestartet werden, damit sich die Änderungen auch auswirken!

Schauen wir uns jetzt den Bereich „DNS Blacklist Filters“ an. Dort können wir zunächst die Blacklist Unterstützung für Domino aktivieren, indem wir in den Auswahlbereich klicken und den Eintrag „enabled“ selektieren.

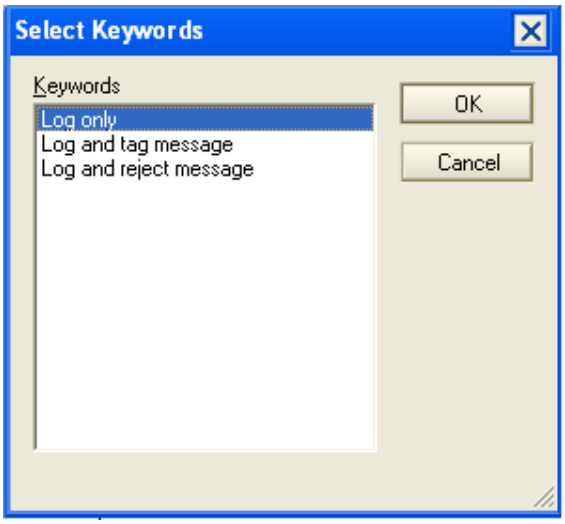
Wenn die Verwendung der Blacklists aktiviert wurde, sollte auch in dem Feld „DNS Blacklist Sites“ mindestens ein Eintrag enthalten sein. Wie bereits erwähnt, finden sie solche Blacklists im Internet. Dabei stehen sowohl kostenfreie, als auch kostenpflichtige Blacklist Verzeichnisse zur Verfügung. Sollten sie einmal auf die Abkürzung „DNSBL“ stoßen: dabei handelt es sich um eine allgemein gebräuchliche Abkürzung für DNS Blacklists.



02 DNSBL Angabe

Nach dem Aktivieren und der Angabe mindestens eines DNSBL können wir festlegen, wie im Falle eines Aufspürens einer mutmaßlichen SPAM Adresse weiter verfahren werden soll. Per Standardeinstellung ist lediglich die Protokollierung dieses Ereignisses eingestellt. Zu wenig sicherlich, wenn es um die Vermeidung der SPAM Verarbeitung geht – aber sicherlich auch erst einmal hilfreich, um feststellen zu können, ob man selbst ein SPAM Problem hat.

Klicken wir jetzt auf den Erweiterungspfeil in dem Feld „Desired Action“ (gewünschte Aktion), um eine Auflistung aller möglichen Aktionen zu erhalten.



03 mögliche Auswahlen bei der Erkennung von SPAMs

Neben der reinen Protokollierung können wir noch weitere Einstellungen vornehmen:

- Protokollieren und Nachricht markieren (Log and tag message)
  - Jede Mail, deren Host in einer Blacklist enthalten ist, wird um das Feld $DNSBLSites erweitert. Diese Mail wird also nicht nur protokolliert, sondern um einen Hinweis, dass es sich um eine SPAM handelt, erweitert. Diese Nachricht wird von Domino entgegen genommen.

- Protokollieren und Nachricht zurückweisen (Log and reject message)
  - Stellt Domino fest, dass der Host dieser Mail in einer Blacklist enthalten ist, dann wird diese Mail abgelehnt, ein Protokolleintrag erstellt und an den Administrator gesendet.

Bei der Protokollierung einer SPAM Nachricht verwendet Domino per Standard einen vordefinierten Text, der auf den SPAM Eintrag hinweist. Diese bei dem Erkennen einer SPAM erstellte Nachricht kann auch mit einem eigen definierten Text versehen werden, den sie in dem Feld „Custom SMTP error response...“ (Benutzerdefinierte Antwort auf SMTP Fehler...) angeben können.

In der SPAM Nachricht können auch Variablen eingebunden werden, die zum Beispiel Aufschluss über den versendenden Host geben. Solche Variablen sind mit dem Platzhalter „%“ zu definieren. Das folgende Beispiel zeigt, wie man eine solche Nachricht um die Blacklist Informationen erweitern kann.

ACHTUNG ! Der Hosteintrag %s der Mail ist in der DNS Blackliste %s enthalten!

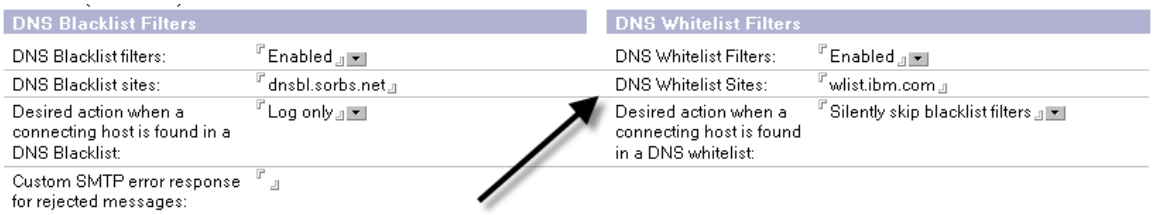
Die Platzhalter werden bei dem Erkennen eines SPAM Eintrags in einer Blackliste entsprechend umgesetzt, so das eine Meldung dann so aussehen kann:

ACHTUNG ! Der Hosteintrag www.wwinzig.de *der Mail ist in der DNS Blackliste testdnsbl.mail.org enthalten!*

Mit diesen wenigen, aber nichts desto trotz effizienten Einstellungen, kann ein bedeutender Teil der täglichen SPAM Flut vermieden werden. Wie bereits erwähnt, ist nur ein Lösungsansatz, wie in diesem Fall die Blacklistverwendung, meist nicht ausreichend. Ideal ist die Kombination mit weiteren Funktionen, die für eine SPAM Abwehr sowohl in Domino direkt, als auch in Form von Zusatzprodukten zur Verfügung stehen.

Wichtig ist auch hier, dass sich mögliche Veränderungen erst nach einem Neustart des SMTP-Dienstes auswirken.

IBM hat in den beiden Versionen 6 und 7 von Domino den Anforderungen durch die immer weiter steigende SPAM Flut Rechnung getragen, und mit der Version 6 neue Blacklist Filter, und seit der Version 7 auch die Unterstützung privater Blacklists und auch Whitelists realisiert – letztere genau wie auch die Blacklists im öffentlichen DNS- und auch im privaten Bereich.

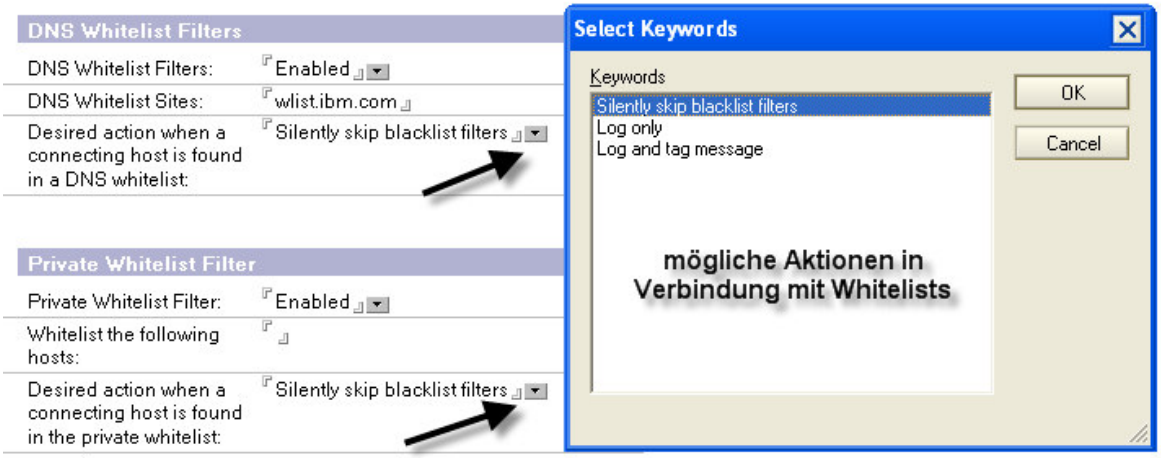


04 Definition der Whitelists

Im Gegensatz zu den Blacklists, mit denen wir festlegen, welche Domänen als nicht vertrauenswürdig einzustufen sind, definieren wir mit Whitelists solche Domänen, die als sicher einzustufen sind. Wenn Whitelists in Domino angegeben werden, dann hat das zur Folge, dass Mails, die von den in einer solchen Whitelist enthaltenen Domänen stammen, zunächst einmal als „erwünschte“ Mails angesehen und auch so behandelt werden (sicher sollten auch in einem solchen Fall Virenprüfungen etc. zusätzlich neben den Whitelists eingesetzt werden!).

In dem Feld „DNS Whitelist Filters“ können wir, ähnlich wie bei der Angabe der Blacklists, die IP Adresse der Domäne angeben, die in diesem Bereich aufgenommen werden soll. Alternativ dazu können wir hier den Hostnamen verwenden. Auch hier steht wieder das Asterixzeichen (*) zur Auswahl aller Einträge zur Verfügung. Letzteres sollte jedoch nur in Ausnahmefällen eingesetzt werden, denn es öffnet wieder Tür und Tor!

Auch bei dem Einsatz von Whitelists sind wieder verschiedene Aktionen erforderlich, die in Verbindung mit den Ergebnissen einer Whitelist Analyse ausgeführt werden können. Dabei kann, wie auch bei den Blacklists in Bezug auf die Aktionen zwischen den privaten Whitelists und den öffentlichen Whitelists unterschieden werden.



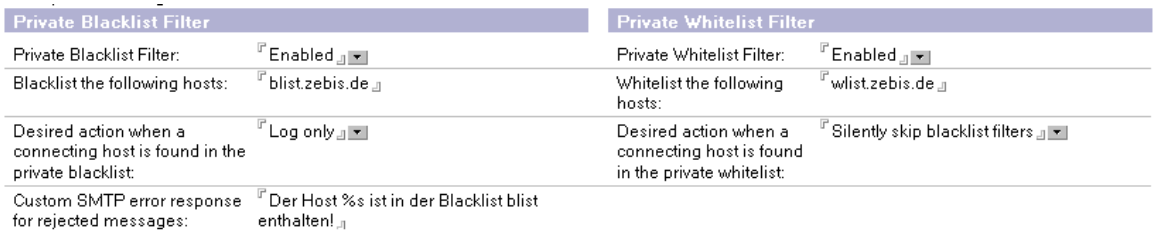
05 Aktionen in Verbindung mit Whitelists

Die Bedeutungen der verschiedenen Aktionen sind denen in der Blacklist ähnlich. Auch hier kann ein Zusatz zu den korrespondierenden Whitelist Mails in Form des Zusatzes $DNSWLSite verwendet werden. Damit lassen sich zum Beispiel weitere Analysen in Bezug auf die Whitelists durchführen.

Natürlich können wir sowohl Whitelists, als auch Blacklists parallel auf einem Domino Server verwenden.

Schauen wir uns dazu ein kleines Beispiel an, das die Verarbeitung der Mails veranschaulicht:

Nehmen wir einmal an, wie haben eine private Blacklist definiert. Die Angaben dazu sehen sie auch in der folgenden Abbildung:



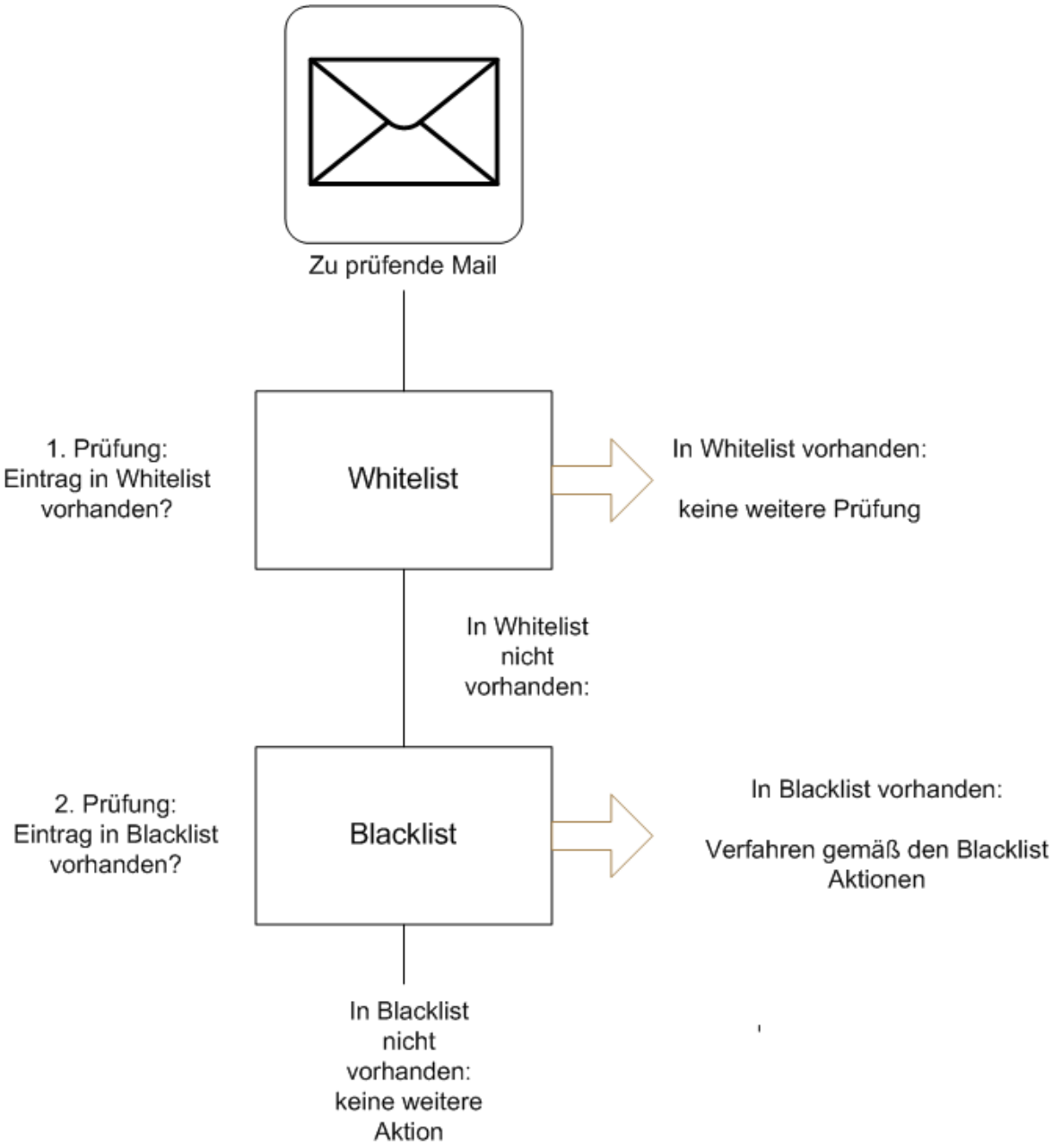
Private Blacklist Filter		Private Whitelist Filter	
Private Blacklist Filter:	Enabled	Private Whitelist Filter:	Enabled
Blacklist the following hosts:	blist.zebis.de	Whitelist the following hosts:	wlist.zebis.de
Desired action when a connecting host is found in the private blacklist:	Log only	Desired action when a connecting host is found in the private whitelist:	Silently skip blacklist filters
Custom SMTP error response for rejected messages:	Der Host %s ist in der Blacklist blist enthalten!		

06 Blacklist und Whitelist

Zusätzlich zu dieser Blacklist wurde eine private Whitelist definiert. Auch deren Einstellungen sind in der vorhergehenden Abbildung zu sehen.

Wir der Host einer zu verarbeitenden Mail nicht in der Whitelist gefunden (die zuerst verarbeitet wird), dann haben wir in unserem Beispiel mit dem Eintrag „Silently skip blacklist filters“ festgelegt, dass keine Protokollierung stattfinden soll, sondern die Mail bzw. der Host dieser Mail in einem Blacklist Eintrag überprüft wird.

Ist der Mailhost in einer Blacklist enthalten, dann werden die dort definierten Aktionen ausgeführt – also entweder wird diese Mail protokolliert und empfangen, protokolliert und abgewiesen oder protokolliert und markiert.



07 Ablauf der gemeinsamen Whitelist und Blacklist Verwendung

Ähnlich wie auch bei der Verwendung der Blacklists, so können auch bei den Whitelists Statistiken darüber geführt werden, welche Aktionen mit Whitelists verarbeitet wurden und welche Ergebnisse diese zur Folge hatten. Dazu steht ein Parameter SMTPExpandDNSWLStats=value zur Verfügung. Ist dieser aktiviert (value = 1) dann erstellt der SMTP Dienst pro Host einen Eintrag, der die Anzahl der Whitelist Zugriffe zu diesem Host aufnimmt.

Wie sie sehen, stellen sowohl die Blacklists als auch die Whitelists viele Möglichkeiten in Bezug auf die Belastungen durch SPAM dar.