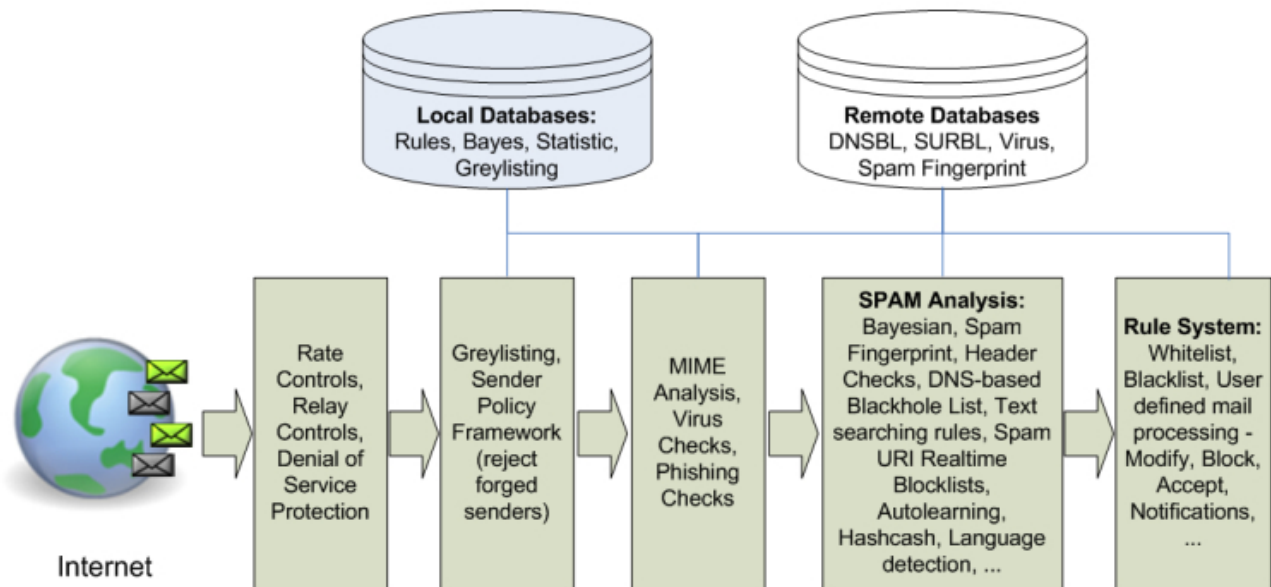


Spam Filter Methoden



Greylisting

Ein Server der Greylisting verwendet, verarbeitet bei jeder E-Mail die drei folgenden Informationen :

- Die IP Adresse des SMTP Clients
- Die Envelope Sender- Adresse
- Die Envelope Recipient- Adresse

Zuerst wird die IP Adresse des SMTP Clients mit den Einträgen in der internen Server-Whitelist verglichen. Wenn keine der 3 Adressen bekannt ist, wird die E-Mail mit der unbekanntem IP Adresse eine Weile greygelistet (Die Dauer des Greylisting kommt auf die Server Konfiguration an); d.h. die E-Mail wird mit einer temporären Fehlermeldung zurückgewiesen. Dabei wird folgendes angenommen: Temporäre Fehler sind bei der Zustellung von E-Mails in der RFC Spezifikation inkludiert. Ein rechtmäßiger Mailserver wird nach einiger Zeit versuchen, die E-Mail erneut zuzustellen. Da dem System die Adresse schon bekannt ist, wird die E-Mail schlussendlich zugestellt.

Der Erfolg von Greylisting ergibt sich aus folgender Tatsache: Tools, die Spammern verwenden um Massenemails zu versenden, können nicht mit temporären Fehlern umgehen.

Greylisting kann unerwünschten E-Mail Verkehr um bis zu 90 % senken. Durch das Greylisting werden keine "Non Delivery Reports" mehr an Spammer geschickt.

Sender Police Framework (SPF)

Domains verwenden public records (DNS) um Anfragen für verschiedene Services (WWW, E-Mail, usw.) zu jenen Servern zu leiten, die diese Services anbieten. Alle Domains geben ihre MX- Einträge bekannt, um der Welt zu sagen welcher Server E-Mails für diese Domain empfängt.

SPF verwendet so genannte „umgekehrte“ MX Einträge, um der Welt mitzuteilen welcher Server E-Mails für diese Domain sendet. Wird eine E-Mail empfangen, kann der Empfänger diese „verkehrten“ MX Einträge verwenden, um sicherzugehen, dass diese E-Mail auch vom richtigen Sender kommt.

Bayesian Filter

Der Bayesian Filter ist ein statistischer Filter, der mit bedingten Wahrscheinlichkeiten operiert. Auf Grund bestimmter Wörter, wie z.b. Viagra, wird geschlossen, dass es sich bei einem vorliegenden E-Mail um Spam handelt.

Blacklist

Blacklist ist ein Zugangs- Kontrollmechanismus. Allen - außer jenen, die einen Eintrag in der Blacklist haben - ist es erlaubt, ein E-Mail an das Proxmox Mail Gateway zu senden.

Whitelist

Jeder eingetragene Sender auf der Whitelist kann E-Mails an das Proxmox Mail Gateway senden ohne dass seine E-Mails auf Spam überprüft werden.

DNS-based Blackhole List

In diesen Listen werden IP-Adressen von Computern gespeichert, die schon in der Vergangenheit Spam gesendet haben. Diese Listen werden beim Eingang einer E-Mail von der Spam-Erkennungs Software (z. b. Spamassassin) ausgewertet und bei positiver Bewertung wird die Annahme der E-Mail verweigert.

Distributed Checksum Clearinghouse (DCC)

E-Mail Clients oder SMTP Server sammeln Prüfsummen von E-Mails und leiten sie an einen DCC Server weiter. Der DCC Server stellt anhand der eindeutigen Prüfsumme fest, wie oft diese E-Mail empfangen wurde. Ist dieser Wert sehr hoch, wird die E-Mail als Spam identifiziert und kann nun von den DCC Clients registriert oder gelöscht werden oder die Annahme kann verweigert werden.

Erweiterte E-Mail Header Analyse und Text- Suchregeln

E-Mail Header sind im Normalfall nicht sichtbar, beinhalten aber jene Informationen, die nötig sind, um E-Mails korrekt zuzustellen. Das System überprüft die E-Mail Header auf Inkonsistenz - ein Hinweis auf Spam.

Es gibt circa 600 Text- Suchregeln die typische Phrasen von Spam Mails aufdecken.

Spam URI's Realtime Blocklists (SURBL)

SURBL's entdecken Spam anhand von Uniform Resource Identifier (normalerweise Webseiten) im message body. Derart identifizierte Spam E-Mails können nun vom Empfänger blockiert werden.

Selbst lernend

Das System sammelt statistische Informationen über Spam Mails. Diese Informationen werden von selbst lernenden Algorithmen verarbeitet. Dadurch wird das System mit der Zeit noch effektiver.

Hashcash

Jede E-Mail wird vom Absender mit einem header versehen, der belegt, dass das "virtuelle Porto" in Form von ein wenig Rechenzeit bezahlt ist.

Da die meisten Spammer wenig Zeit verwenden um möglichst viele E-Mails abzusenden, kann der Empfänger mittels Hashcash dies mit vergleichsweise wenig Aufwand verifizieren.