**Tổng quát:**

Postscreen là một công cụ bổ sung để chống Spam cho Mail Zimbra. Nó cung cấp các tính năng để bảo vệ hệ thống mail khỏi tình trạng bị quá tải. Một quy trình postscreen có thể xử lý nhiều kết nối SMTP, và quyết định máy trạm nào có thể giao tiếp và gửi thư tới máy chủ Post-fix SMTP. Bằng việc để các trạm chống spam ở xa, các quy trình tại máy chủ SMTP của postscreen sẽ đảm bảo khả năng đáp ứng bất cứ lúc nào, từ đó có thể trì hoãn thời gian tạo ra điều kiện quá trải của máy chủ.

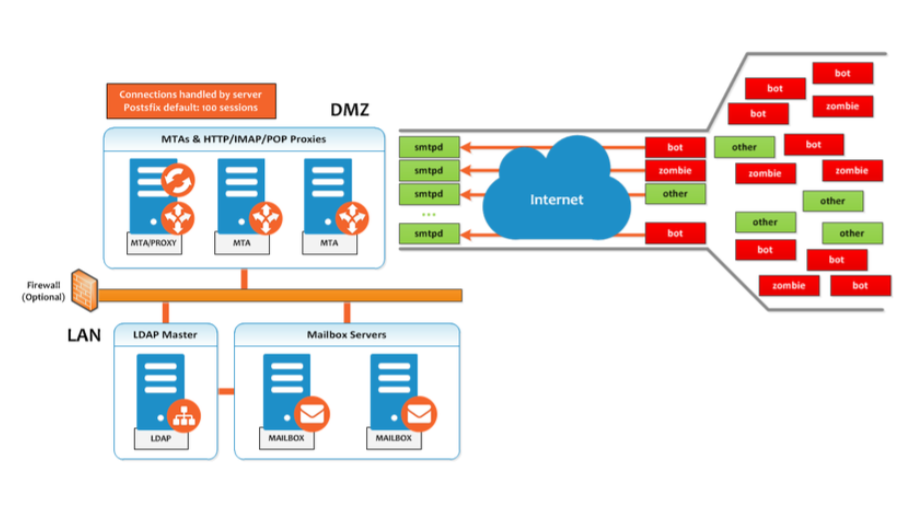
Zimbra Collaboration Postscreen không nên được sử dụng trên các cổng SMTP - cái mà nhận thư từ những khách hang sử dụng cuối ( MUA ) . Trong mô hình triển khai, postscreen xử lý dịch vụ MX ( Mail Exchange) trên cổng 25 bằng giao thức TCP, trong khi MUA clients lại gửi mail qua cổng 587 bằng giao thức TCP và yêu cầu quá trình xác thực. Ngoài ra, một trang web có thể thiệt lập một máy chủ chuyên dụng qua cổng 25, không phải là postscreen hay MX, nó sẽ cung cấp các dịch vụ gửi thư và xác thực cho máy khách.

Zimbra Collaboration Postscreen duy trì một danh sách trắng tạm thời cho các khách hàng đã vượt qua một số bài kiểm tra. Khi một địa chỉ IP của máy khách SMTP được liệt kê, thì postscreen sẽ tắt kết nối ngay lập tức tới một quá trình máy chủ Postfix SMTP. Điều này giảm thiểu thời gian cho thư hợp lệ.

Trong một thiết lập sản xuất điển hình, postscreen được cấu hình để loại bỏ thư từ các máy khách không thành công một hoặc nhiều lần kiểm duyệt. Zimbra Collaboration Postscreen sẽ loại bỏ thư cùng với các thông tin đi kèm như địa chỉ khách hàng, helo, người gửi và người nhận thông tin.

Zimbra Collaboration Postscreen không phải là một proxy SMTP.Mục đích chính của nó là để giữ các máy trạm spam tránh xa khỏi máy chủ Postfix SMTP, đồng thời giảm thiểu chi phí cũng như thời gian cho lưu lượng truy cập hợp lệ.

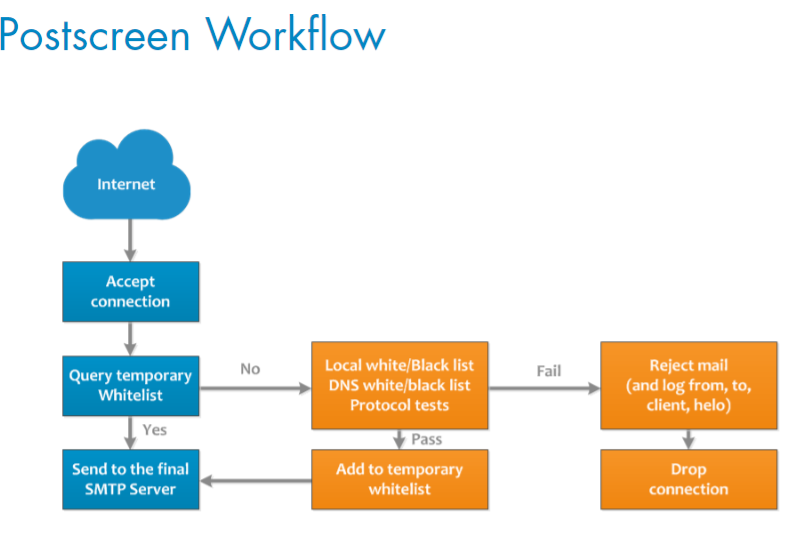
1. **Kịch bản không sử dụng Postscreen**: Tất cả các khách hang sử dụng mail zimbra sẽ giao tiếp trực tiếp với các hiểm họa luôn rình rập từ các tổ chức nguy hiểm cũng như sẽ bị thiệt hại bởi cả những mối đe dọa thông thường.



Như ta thấy trong hình, các kết nối an toàn với đường truyền tốt “other” phải chờ cho tới khi những kết nối xấu hoặc ảo “bot”, “zombie” hoàn thành xong việc giao tiếp của chúng, cái mà đôi khi có thể tạo nên các lỗi về thời gian phản hồi quá lâu hoặc hết hạn trên postfix cho các kết nối tốt. ( vd : Khi có các kết nối đến như có người gọi điện đến cho mình, nhưng lúc nghe thì bên họ không trả lời, những lần như vậy gọi là spam, trong 1 ngày không thể mất thời gian vào những cuộc gọi mất thời gian như vậy thì sẽ k đủ thời gian hoặc không thể nghe những cuộc gọi quan trọng)



1. **Kịch bản sử dụng postscreen:**

****

**Hoạt động :**

Khi các kết nối từ mạng ngoài truy cập vào hệ thống mail, nó sẽ tạm thời được đưa vào trong danh sách trắng- danh sách an toàn.

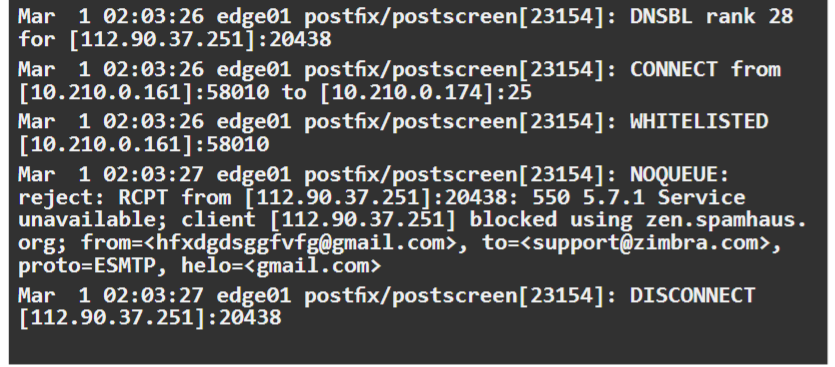
(“<http://www.postfix.org/POSTSCREEN_README.html>” )

+ Nếu nó hợp lệ sẽ được gửi thẳng tới máy chủ SMTP để tiến hành nhận thư.

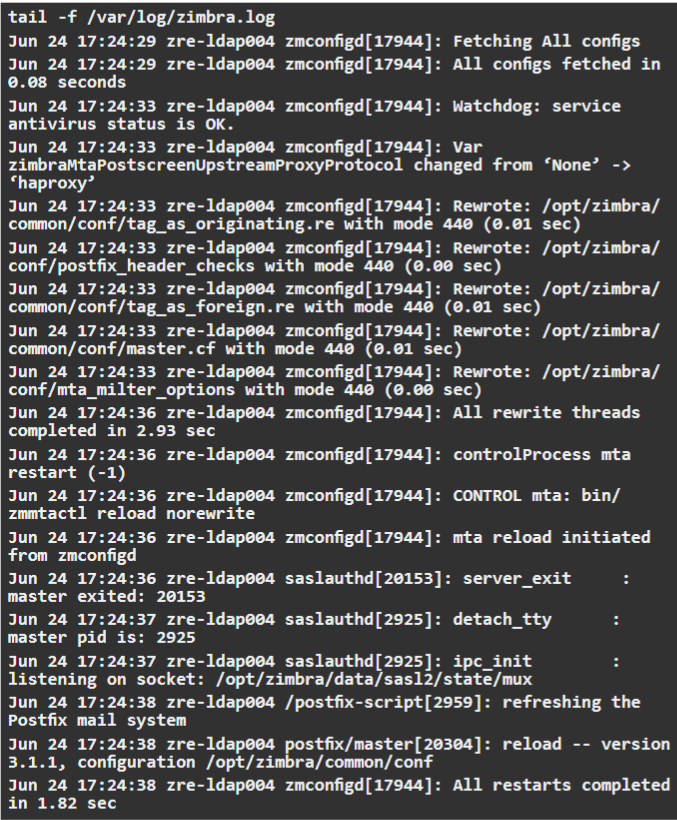
+ Nếu trường hợp kết nối không đáp ứng được các yêu cầu trong danh sách truy vấn tạm thời (Query temporary whitelist) , chúng sẽ phải qua các quá trình kiểm tra giao thức nội vùng hoặc các máy chủ DNS bằng danh sách chặn của máy chủ DNS và các bộ lọc . Nếu kết nối đó được xác định là Spam thì nó sẽ bị từ chối và loại bỏ . Trong trường hợp còn lại , nếu qua được các qá trình kiểm duyệt, nó sẽ được them vào danh sách trắng tạm thời và được chuyển tới máy chủ SMTP cuối để tiến hành gửi thư.

* Ignore- Bỏ qua (mặc định) - Bỏ qua kết quả này. Cho phép các bài kiểm tra khác hoàn thành. Lặp lại thử nghiệm này vào lần tiếp theo khách hàng kết nối. Tùy chọn này hữu ích cho việc thử nghiệm và thu thập số liệu thống kê mà không chặn thư.
* Enforce- Thi hành - Cho phép các bài kiểm tra khác hoàn thành. Từ chối các nỗ lực gửi thư với 550 SMTP và đăng nhập thông tin helo / sender / recipient. Lặp lại quá trình này vào lần tiếp theo khách hàng kết nối.
* Drop- ngắt kết nối – Ngắt kết nối ngay lập tức với một phản hồi SMTP 521. Lặp lại kiểm tra này vào lần kết nối khách hàng tiếp theo.
* **Bật chế độ Postscreen:** Những bản Zimbra trước 8.7 sẽ phải cài thêm hoặc khởi chạy nó bằng lệnh tuy nhiên từ Zimbra 8.7 trở đi nó sẽ tự động khởi chạy khi cài Zimbra và có thể dùng luôn.
* **Quá trình kiểm thử Postscreen:**
* Bạn có thể cài đặt DNSBLs (Domain Name System Blacklists hoặc DNS Blacklists, là danh sách chặn thư rác cho phép quản trị viên trang web chặn tin nhắn từ các hệ thống cụ thể có lịch sử gửi spam “ <http://www.dnsbl.info/>” ) nhưng nên để nó ở chế độ ignore để kiểm thử sự thưc thi của postscreen.
* Postscreen sẽ ghi lại những gì nó đã làm. Khi bạn hài lòng rằng việc thực hiện của bạn là chính xác, bạn có thể đặt các giá trị sao cho phù hợp.

Dưới đây là ví dụ về việc lưu lại lỗi 550 trừ postscreen:



Xác minh quá trình thay đổi đang diễn ra:



Xác minh các thay đổi bằng việc chạy cá dòng lệnh sau:

