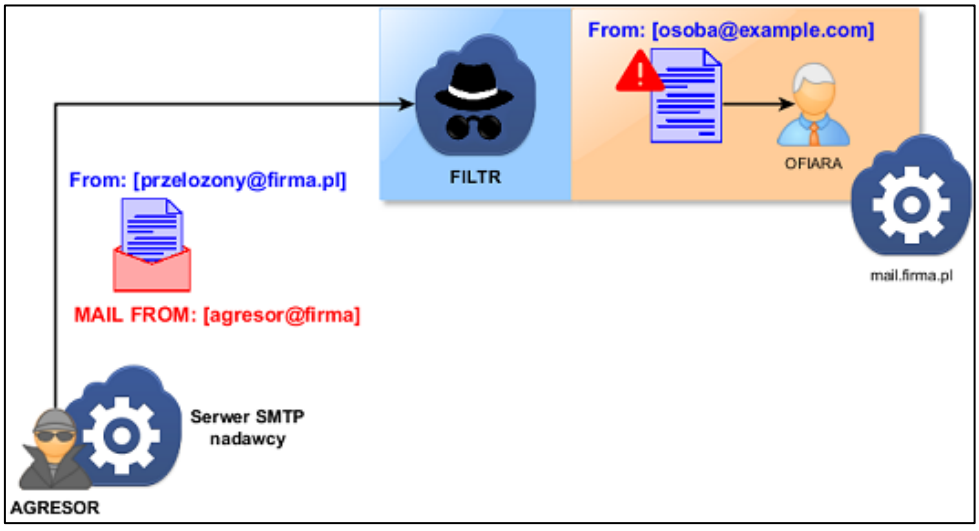
AntiSpoof SMTP
–rozwiązanie do ochrony poczty elektronicznej przed atakami typu Spoofing oraz niechcianą pocztą

AntiSpoof SMTP jest rozwiązaniem dedykowanym do ochrony systemów poczty elektronicznej przed atakami typu *Spoofing* i SPAM, nawet w przypadku, gdy atak jest wykonywany w sposób niewykraczający poza normy działania protokołu SMTP (RFC 5321 i powiązane). System dokładnie analizuje i przetwarza informacje opisujące wiadomości poczty elektronicznej, w szczególności w zakresie opisu nadawcy wiadomości. ***AntiSpoof SMTP*** uwzględnia możliwość otrzymywania przez użytkowników tzw. „kopii ukrytych" oraz wiadomości z *przekazujących serwerów SMTP* (tzw. *forwarders*). Zastosowany w nim zaawansowany mechanizm przetwarzania pól `MAIL FROM` oraz `From` uwzględnia możliwość występowania w nich dodatkowych ciągów znaków (np. opis nadawcy), znaków białych, niedrukowalnych (np. załączonych w celu zmylenia mechanizmu filtrującego), czy też małych i wielkich liter. Dokładniejszy opis istoty nadużyć, z którymi można się spotkać w ramach Spoofingu SMTP został opisany na stronie www.milstar.pl/smtospoof.html.

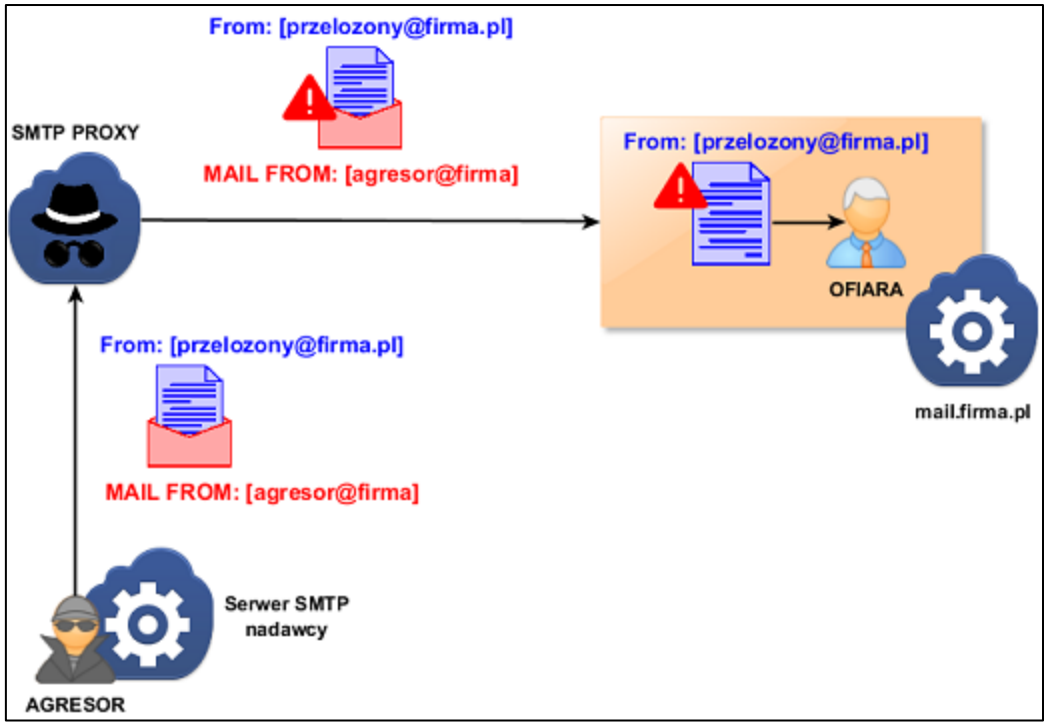
Wdrożenie rozwiązania *AntiSpoof SMTP* może zostać przeprowadzone na dwa różne sposoby, umożliwiając dostosowanie do architektury już istniejącego systemu teleinformatycznego.

Nasze rozwiązanie może pracować jako dodatkowy moduł serwera SMTP tzw. *milter* (rysunek 1). Dzięki takiemu podejściu nie jest wymagane dodawanie jakichkolwiek urządzeń, czy maszyn wirtualnych w infrastrukturze, gdzie jest wdrażany. W tym przypadku *AntiSpoof SMTP* zostanie osadzony na maszynie obsługującej pocztę elektroniczną i rozpocznie współpracę z serwerem SMTP filtrując przychodzące wiadomości pod kątem występowania w nich znamion ataków typu *Spoofing* lub SPAM.



Rys. 1. Wdrożenie *AntiSpoof SMTP* jako modułu serwera SMTP

Alternatywą jest wdrożenie naszego produktu jako pośredniczącego serwera filtrującego *AntiSpoof SMTP – Proxy* zlokalizowanego przed właściwym serwerem SMTP dostarczającym wiadomości e-mail do użytkowników (rysunek 2). Dzięki takiemu podejściu odciążany jest serwer SMTP, ponieważ filtrowaniem poczty elektronicznej zajmowała się będzie odrębna maszyna, posiadająca własne zasoby sprzętowe. Istnieje też możliwość uruchomienia *AntiSpoof SMTP – Proxy* jako oddzielnego procesu na tej samej stacji, na której pracuje właściwy serwer SMTP, co z kolei eliminuje konieczność wprowadzania do systemu teleinformatycznego dodatkowych składników (sprzętowych). Możliwe jest również uruchomienie serwera pośredniczącego (z oprogramowaniem ***AntiSpoof SMTP***), jako wirtualnej maszyny w dowolnej lokalizacji fizycznej, jak i logicznej.



Rys. 2. Wdrożenie *AntiSpoof SMTP - Proxy* jako osobny węzeł sieci

Rozwiązanie *AntiSpoof SMTP* wyróżnia odpowiednie połączenie mechanizmów wykorzystywanych przy filtrowaniu wiadomości, dzięki czemu zapewnia zaawansowaną ochronę przed atakami typu *Spoofing*. Nasze rozwiązanie można w pełni dostosować do potrzeb Zamawiającego poprzez uruchomienie wszystkich, bądź tylko wybranych mechanizmów filtrowania.

Podstawowy wykorzystywany mechanizm wykorzystuje weryfikację zgodności reguł SPF (*Sender Policy Framework*) dla nadawcy wiadomości do wysyłania wiadomości w imieniu określonej domeny. *AntiSpoof SMTP* umożliwia weryfikację na dwóch poziomach, tj. w polu `MAIL FROM` podawanym podczas przesyłania wiadomości między serwerami SMTP oraz w polu `From` zawartym w tzw. *kopercie*. **Zatem nasze rozwiązanie umożliwia wykonanie dodatkowego sprawdzenia mechanizmem SPF na podstawie wyniku działania mechanizmu SPF**

zapisanego w nagłówku wiadomości przez bramkę SMTP (lub serwer brzegowy SMTP). Opcja ta jest użyteczna, gdy *AntiSpoof SMTP* nie funkcjonuje, jako brzegowy serwer SMTP.

Wykorzystywanie sygnatur **DKIM** (*Domain Keys Identified Mail*) umożliwia filtrowanie wiadomości na podstawie weryfikacji, czy została ona wysłana z uprawnionego do tego serwera SMTP. Rozwiązanie to wymaga odpowiedniego skonfigurowania po stronie nadawcy mechanizmu DKIM. Dodatkowo istnieje możliwość wykorzystania infrastruktury klucza publicznego do podpisywania wiadomości, co jest zapewnione przez mechanizm **S/MIME** *(Secure/Multipurpose Internet Mail Extensions)*. Rozwiązanie to **umożliwia weryfikację, czy wiadomość faktycznie została wysłana przez uprawnionego do tego nadawcę i czy nie została w trakcie dostarczania zmodyfikowana**. Do poprawnej współpracy również wymagana jest odpowiednia konfiguracja serwera po stronie nadawcy.

Ogromne możliwości daje zaimplementowana w *AntiSpoof SMTP* obsługa wyrażeń regularnych zgodnych ze standardem PCRE. Poprzez zdefiniowanie odpowiednich zbiorów wyrażeń regularnych możliwe jest wychwycenie niechcianej poczty (*SPAMu*). **Nasze rozwiązanie dopuszcza oznaczenie wiadomości jako SPAM w następujących przypadkach:**

- dopasowanie wiadomości do wyrażenia ze zbioru, np. gdy zawiera słowo „loan”,
- brak dopasowania wiadomości do wyrażenia ze zbioru, np. gdy nie zawiera słowa „From:”,
- dopasowanie wiadomości do określonej liczby wyrażeń w danym zbiorze, np. gdy wiadomość zawiera słowa „genuine”, „loan” i „offer” (tzw. *filtry przesiewowe*).

Wyrażenia regularne można dodawać do *AntiSpoof SMTP* pojedynczo lub załadować przygotowaną wcześniej bazę z pliku CSV.

Nasze rozwiązanie umożliwia automatyczne blokowanie wiadomości zaklasyfikowanych jako *Spoofing* lub SPAM. **Istnieje także funkcja, która umożliwia wysłanie do informacyjnych adresów e-mail kopii takiej wiadomości przed jej zablokowaniem** dzięki czemu Administratorzy będą mogli się jej dokładnie przyjrzeć i poddać ją gruntownej analizie w późniejszym czasie. Ponadto istnieje możliwość wysyłania do informacyjnych adresów e-mail listy kont nieistniejących na serwerze docelowym dzięki czemu można usunąć z wykorzystywanych przez Państwa list *mailingowych* nieaktywne adresy.

AntiSpoof SMTP **umożliwia także tworzenie list zaufanych serwerów SMTP**, dla których filtrowanie wiadomości nie będzie realizowane. Istnieje także możliwość określenia konkretnych skrzynek pocztowych, tylko dla których ma być realizowane filtrowanie wiadomości, bądź tylko dla których filtrowanie ma nie być realizowane.

Poza mechanizmami filtrowania poczty elektronicznej *AntiSpoof SMTP* posiada wiele innych przydatnych funkcji. Jedną z istotniejszych jest **możliwość wymuszenia wyświetlania informacji o nadawcy wiadomości**, co spowoduje wymuszenie na aplikacjach klienckich wyświetlania użytkownikom informacji o adresie e-mail nadawcy wiadomości (w nawiasach kwadratowych) – przykład został przedstawiony na rysunku 3.

Rys. 3. Wyświetlanie adresu e-mail nadawcy

Większość klientów poczty elektronicznej domyślnie nie udostępnia użytkownikom takiej informacji, co może prowadzić do wykonania względem nich jednego z wariantów ataku typu *Spoofing*. Warto również zaznaczyć, że sposób realizacji przedmiotowej funkcji przez aplikację *AntiSpoof SMTP* jest niezależny od klienta poczty elektronicznej, dzięki czemu **informacja o adresie e-mail nadawcy zostanie wyświetlona nawet w przypadku, gdy oprogramowanie użytkownika standardowo w ogóle nie zapewnia opisanej możliwości.**

Nasze rozwiązanie umożliwia także oznaczanie podejrzanych wiadomości za pomocą ciągów znaków (np. *** SPAM ***) informujących użytkownika o wykrytych nieprawidłowościach. **Wiadomości będą oznaczane na podstawie każdego z aktywnych filtrów**.

Oprogramowanie *AntiSpoof SMTP* może być skonfigurowane do **wykorzystywania certyfikatu w formacie PEM** co spowoduje, że będzie się nim legitymowało przy odbieraniu/wysyłaniu wiadomości poczty elektronicznej. Omawiana funkcja znajduje zastosowanie głównie w przypadku, gdy nasza aplikacja działa, jako brzegowy serwer SMTP.

Rezultaty swojej pracy nasz produkt może zapisywać w formacie rozszerzonego dziennika zdarzeń, gdzie rejestrowany będzie pełny przebieg komunikacji SMTP dla przetwarzanych wiadomości. Dodatkową opcją jest **możliwość wykorzystywania systemowego dziennika zdarzeń (procesu *syslog*)**, zamiast wbudowanego mechanizmu.

Efektywność filtrowania wiadomości jest uzależniona jedynie od wydajności platformy sprzętowej, na której rozwiązanie zostanie osadzone. *AntiSpoof SMTP* może zostać rozbudowany o dodatkowe moduły/filtry wykorzystujące znane mechanizmy (np. filtr *Bayesa*, mechanizm DMARC, etc.), rozwiązania autorskie oraz o filtry (bazujące np. na wyrażeniach regularnych) dostosowane do charakterystyki rzeczywistego ruchu SMTP specyficznego dla środowiska Państwa firmy. ***AntiSpoof SMTP*** **cechuje się wysoką niezawodnością i stabilnością działania.**