

## FortiMail

Unikatowe zabezpieczenie poczty elektronicznej przeznaczone dla dostawców usług internetowych (ISP)

### Wyzwanie biznesowe

Aby zagwarantować najwyższy poziom usług oraz zapewnić łączność elektroniczną bez spamu, dostawcy usług internetowych (ISP) są zmuszeni do kontrolowania wychodzącego ruchu sieciowego aż do poziomu subskrybentów. Niezależnie od typu stosowanej sieci (komórkowa 3G, ADSL, modem kablowy, itd.), dostawcy muszą być w stanie identyfikować złośliwe treści lub złośliwych użytkowników.

### Czarne listy dostawców usług internetowych: kwestia podstawowa

Aby zapobiegać rozpowszechnianiu spamu, wyspecjalizowane organizacje opracowują i publikują listę adresów IP, z których jest rozsyłany spam.

Lista ta (zwana w skrócie DNSBL) jest powszechnie stosowana przez agenty pocztowe (MTA) oraz bramki antyspamowe do filtrowania przychodzącego spamu. Zasadniczą kwestią dla dostawców usług internetowych jest to, aby nie ograniczając się tylko do tej listy, zapewnić łączność między subskrybentami i siecią Internet - bez spamu.

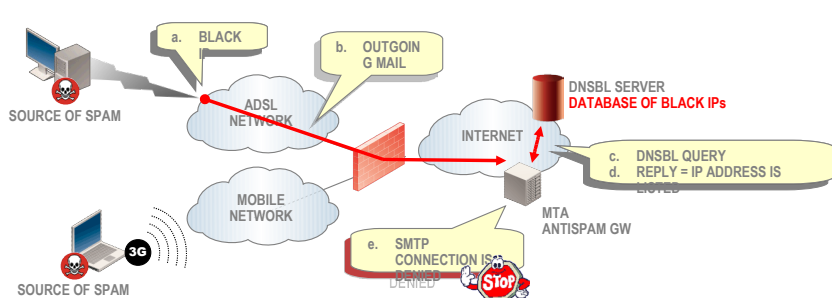
### Unikanie czarnej listy DNSBL jest koniecznością

#### Dzieje się tak z dwóch głównych powodów:

1. Usługa na poziomie klienta:
  - W przypadku wielu adresów IP subskrybentów ukrytych za pojedynczym, publicznym adresem IP: jeżeli jeden zainfekowany komputer rozsyła spam i jego adres IP trafia na czarną listę, żaden subskrybent nie będzie mógł wysłać wiadomości;
  - Jeśli na czarnej liście odnotowany jest zakres adresów sieciowych dostawcy usług internetowych: wszyscy subskrybenci będą mieli zablokowaną możliwość wysyłania wiadomości lub zablokowany dostęp do innych usług oferowanych przez dostawcę usług internetowych;
  - W przypadku ponownego przypisania nielegalnego adresu IP do nowego subskrybenta, nie będzie on mógł wysłać żadnych wiadomości nawet wtedy, gdy jego komputer nie jest zainfekowany złośliwym oprogramowaniem.

#### 2. Zarządzanie i koszty

Proces usunięcia firmy i użytkownika z baz danych DNSBL jest często trudny i kosztowny, a przecież wszystko zaczyna się od nowa za każdym razem, gdy adres IP trafia na czarną listę.



## Rozwiązanie: moduł zwalczający spam w poczcie wychodzącej

Dostawcy usług internetowych muszą filtrować wiadomości wychodzące, bez wpływu na jakość działania poczty elektronicznej.

### Dłatego rozwiązanie antyspamowe powinno:

- Działać jako niewidoczny serwer pośredniczący (proxy): subskrybenci powinni być w stanie przysłać wiadomości bezpośrednio do sieci Internet przy pomocy istniejących ustawień, zamiast korzystać z przekaźnika poczty oferowanego przez dostawcę usług internetowych;
- Być niewidoczne w kopercie i nagłówkach SMTP: kontrola antyspamowa jest niewidoczna dla użytkownika końcowego. Ponadto, rozwiązanie zwalczające spam nie powinno kolejkować wiadomości w celu równoważenia potencjalnej niedostępności internetowego agenta MTA;
- Być niewidoczne w warstwie IP: podczas przesyłania wiadomości do sieci Internet, źródłowy adres IP użytkownika nie powinien ulec zmianie. Jeżeli źródłowy adres IP pochodzący z różnych filtrowanych sesji pocztowych jest zastępowany przez unikatowy adres IP, mógłby on zostać zablokowany z powodu generowania zbyt dużego ruchu sieciowego;
- Oferować dedykowane filtry antyspamowe: filtr tradycyjny oparty na ocenie publicznych adresów IP nie sprawdza się w przypadku dostawców usług internetowych, ponieważ spam powinien być blokowany przed identyfikacją adresu IP jako adresu rozsyłającego spam;
- Śledzić działanie modułu antyspamowego poczty wychodzącej na poziomie subskrybenta: aby uniknąć stosowania czarnej listy i wprowadzić pełne monitorowanie reputacji subskrybentów, a także stały podgląd czynności wykonywanych w sieci oraz użytkowników dokonujących nielegalnych działań.

## Unikatowe zabezpieczenie poczty elektronicznej przeznaczone dla dostawców usług internetowych (ISP)

FortiMail jest urządzeniem antyspamowym, zaprojektowanym specjalnie do tego celu. Spełnia ono wymagania określone przez dostawców usług internetowych odnośnie bezpieczeństwa wiadomości poczty elektronicznej, dzięki opcji pełnej niewidoczności serwera pośredniczącego, monitorowaniu antyspamowemu poczty wychodzącej oraz możliwościom dotyczącym skanowania wiadomości. FortiMail oferuje również moduł antyspamowy sprawdzający pocztę przychodzącą, przeznaczony do ochrony wewnętrznych skrzynek pocztowych dostawcy usług internetowych.

Niewidoczność dla protokołów	<ul style="list-style-type: none"><li>• Unikatowy i prawnie zastrzeżony, niewidoczny serwer pośredniczący (proxy);</li><li>• FortiMail nie zakłóca działania protokołu SMTP;</li><li>• Wyniki pracy urządzenia FortiMail nie pojawiają się w kopercie i nagłówkach SMTP .</li></ul>
Niewidoczność dla sieci Dedykowane techniki antyspamowe	<ul style="list-style-type: none"><li>• FortiMail ukrywa swoją obecność w warstwie IP i nie wpływa na źródłowe i docelowe adresy IP.</li><li>• FortiMail oferuje techniki specjalne, przy pomocy których blokuje spam przed powiązaniem go z konkretnym adresem IP.</li></ul>
Monitorowanie / raportowanie / blokowanie identyfikatorów subskrybentów (w czasie rzeczywistym)	<ul style="list-style-type: none"><li>• Unikatowość urządzenia FortiMail polega na możliwości śledzenia, pobierania i przetwarzania wiadomości na podstawie ich identyfikatorów, zamiast dynamicznych adresów IP;</li><li>• FortiMail dynamicznie oblicza reputację identyfikatorów subskrybentów, rejestruje dane statystyczne i automatycznie ostrzega lub blokuje podejrzane identyfikatory.</li></ul>
Moduł zwalczający spam w poczcie przychodzącej	<ul style="list-style-type: none"><li>• FortiMail oferuje ochronę przed spamem i wirusami, dzięki czemu subskrybenci 3G/ADSL mają czyste skrzynki pocztowe. Wiadomości przychodzące są filtrowane przed wystaniem ich do serwerów wewnętrznych dostawców usług internetowych (ISP).</li></ul>
Tryb serwera pocztowego	<ul style="list-style-type: none"><li>• W trybie tym urządzenie FortiMail oferuje konta pocztowe z usługą usuwania spamu i wirusów we wszystkich skrzynkach pocztowych.</li></ul>
Trasowanie oparte na strategii	<ul style="list-style-type: none"><li>• Aby zapewnić optymalne wykorzystanie zasobów, urządzenie FortiMail otrzymuje do skanowania wyłącznie wiadomości poczty elektronicznej (bez treści sieciowych, ftp, pop3, itd.).</li></ul>
Trasowanie MMS (dla operatorów komórkowych)	<ul style="list-style-type: none"><li>• Aby zapewnić większe bezpieczeństwo, FortiMail przekazuje wiadomości MM3/MM4, skanując pocztę przychodzącą i wychodzącą zanim dojdzie do Centrum MMS.</li></ul>
Platforma dedykowana	<ul style="list-style-type: none"><li>• FortiMail jest technologią opracowaną w całości przez firmę Fortinet i nie zawiera żadnych mechanizmów antyspamowych i antywirusowych wykonanych przez firmy trzecie. Charakteryzuje się wysokim poziomem optymalizacji kodu oraz doskonałą integracją zadań z zakresu ochrony.</li></ul>
Inne właściwości	<ul style="list-style-type: none"><li>• Centralne rejestrowanie / raportowanie / kwarantanna;</li><li>• Opcja konfiguracji grupy;</li><li>• Usługi subskrypcyjne FortiGuard® aktualizujące moduły: antywirusowy, antyspamowy i zwalczający oprogramowanie szpiegowskie;</li><li>• Cena urządzenia jest taka sama, niezależnie od ilości użytkowników i skrzynek pocztowych.</li></ul>

**FORTINET - Oddział w Polsce:**  
ul. Złota 59  
Złote Tarasy - LUMEN II, 6 piętro  
00-102 Warszawa  
www.fortinet.pl

**Autoryzowany Dystrybutor:**  
Veracomp SA  
ul. Zawia 61, 30-390 Kraków  
www.veracomp.pl/fortinet

Wszelkie znaki towarowe i nazwy zawarte w niniejszej publikacji zostały użyte za zgodą ich właścicieli i stanowią przedmiot ich praw ochronnych. Używanie, kopiowanie, opracowywanie i jakiegokolwiek postępowanie się tymi znakami bez uprzedniej zgody właścicieli praw ochronnych jest zabronione.

