Jak działa poczta

Droga wiadomości, SPF, DKIM i DMARC.

- Jak działa poczta: MTA, MDA, MUA, SMTP, kolejka

Jak działa poczta: MTA, MDA, MUA, SMTP, kolejka

Poziom: podstawy **Dotyczy: dowolny serwer pocztowy (Postfix, MailCow, Zimbra)**

Czas: ~20 min

Zanim zaczniemy konfigurować którykolwiek serwer pocztowy, ustalamy wspólny słownik — kto jest kim na drodze wiadomości i co faktycznie sprawdzają SPF, DKIM i DMARC.

Skróty użyte na tej stronie (17)

Skrót	Co znaczy
DKIM	DomainKeys Identified Mail: cyfrowy podpis wiadomości e-mail
DMARC	Domain-based Message Authentication, Reporting and Conformance: reguła domeny mówiąca, co robić z mailem, który nie przeszedł SPF i DKIM
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
IMAP	Internet Message Access Protocol: protokół, którym klient pocztowy pobiera wiadomości z serwera, zostawiając je tam zamiast kasować
IP	Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)
MDA	Mail Delivery Agent: program wkładający pocztę do skrzynki
MTA	Mail Transfer Agent: serwer przekazujący pocztę dalej, np. Postfix
MTA-STS	Mail Transfer Agent Strict Transport Security: zasada opublikowana przez domenę, że poczta do niej ma być wysyłana wyłącznie szyfrowanym połączeniem z serwerem o ustalonej nazwie
MUA	Mail User Agent: program pocztowy użytkownika, np. Outlook
MX	Mail Exchanger: rekord DNS wskazujący serwer poczty domeny
POP3	starszy protokół pobierania poczty na dysk lokalny, w odróżnieniu od IMAP
PTR	rekord DNS odwrotny: zamienia adres IP na nazwę
RFC	Request for Comments: oficjalny dokument opisujący standard internetowy, na przykład sposób działania danego protokołu; w ITIL także Request for Change, czyli wniosek o zmianę
SMTP	Simple Mail Transfer Protocol: protokół wysyłania poczty
SPF	Sender Policy Framework: rekord DNS mówiący, które serwery mogą wysyłać pocztę domeny

Skrót	Co znaczy
TLS-RPT	SMTP TLS Reporting: rekord _smtp._tls z adresem, na który serwery nadawców wysyłają raz na dobę raport o udanych i nieudanych szyfrowanych połączeniach z naszymi serwerami poczty (RFC 8460)
TXT	typ rekordu DNS przechowującego dowolny tekst, wykorzystywany między innymi do publikowania reguł SPF, DKIM i DMARC

Z życia wzięte

□□ Z ŻYCIA WZIĘTE

Pan Wojtek podczas audytu pyta, dlaczego wiadomość z fałszywym adresem `prezes@zielona.example` w polu „Od" przeszła bez ostrzeżenia do skrzynki księgowej. Zespół sprawdza rekordy DNS i widzi poprawny SPF, ale brak jakiegokolwiek DMARC dla domeny. SPF sam w sobie nie broni pola widocznego w kliencie pocztowym, więc dopiero dodanie DMARC z polityką `quarantine` zaczyna faktycznie łapać takie próby.

Droga jednej wiadomości

Pojęcie: MUA (Mail User Agent). Program, którym użytkownik pisze i czyta pocztę — klient pocztowy typu Outlook, Thunderbird, albo aplikacja webmail. MUA nie dostarcza wiadomości samodzielnie, tylko przekazuje ją dalej protokołem SMTP do serwera.

Pojęcie: MTA (Mail Transfer Agent). Serwer odpowiedzialny za przekazywanie wiadomości między serwerami pocztowymi po protokole SMTP — to jest rola, którą pełnią Postfix, opisany na stronie Postfix: konfiguracja, oraz komponent MTA wewnątrz MailCow i Zimbry. MTA odbiera wiadomość od nadawcy (albo od innego MTA) i albo dostarcza ją lokalnie, albo przekazuje dalej w stronę serwera docelowego, ustalanego na podstawie rekordu MX domeny odbiorcy.

Pojęcie: MDA (Mail Delivery Agent). Komponent, który bierze wiadomość dostarczoną przez MTA do lokalnej domeny i zapisuje ją do faktycznej skrzynki odbiorcy — w formacie takim jak Maildir albo mbox, skąd MUA odczytuje ją przez protokół IMAP albo POP3. MTA i MDA bywają częścią tego samego pakietu (Postfix ma wbudowany prosty MDA) albo

osobnymi programami połączonymi ze sobą (np. Dovecot jako MDA obok Postfixa jako MTA).

Pełna droga wiadomości wysłanej z klienta pocztowego do skrzynki odbiorcy w innej domenie wygląda więc tak: MUA nadawcy → MTA nadawcy → (SMTP przez internet) → MTA odbiorcy → MDA odbiorcy → skrzynka → MUA odbiorcy (przez IMAP/POP3).



MUA nadawcy przekazuje wiadomość swojemu MTA, ten po SMTP przekazuje ją MTA odbiorcy, a MDA zapisuje ją do skrzynki, skąd MUA odbiorcy czyta ją przez IMAP lub POP3 (kliknięcie otwiera pełny rozmiar)

Czym jest kolejka

Pojęcie: kolejka. Miejsce, w którym MTA tymczasowo przechowuje wiadomości między odebraniem ich od nadawcy a skutecznym dostarczeniem dalej — wiadomość nie jest przekazywana natychmiast i bezpośrednio z gniazda nadawcy do gniazda odbiorcy, tylko najpierw zapisywana na dysku, a dopiero potem MTA próbuje ją dostarczyć, ewentualnie ponawiając próby, jeśli serwer docelowy jest chwilowo niedostępny. Kolejka jest tym, co pozwala poczcie działać mimo tymczasowych awarii sieci czy przeciążenia serwera odbiorcy — mechanizm ten opisujemy szczegółowo na przykładzie Postfixa na stronie Kolejka Postfiksa: podgląd, wymuszenie, czyszczenie.

Protokół SMTP i porty

Pojęcie: SMTP (Simple Mail Transfer Protocol). Protokół tekstowy, którym jeden MTA przekazuje wiadomość do drugiego, oraz którym MUA wysyła nową wiadomość do swojego serwera. Ten sam protokół obsługuje trzy różne porty, w zależności od tego, kto z kim rozmawia i czy połączenie jest od razu szyfrowane.

Port	Nazwa	Zastosowanie

25/tcp	SMTP	komunikacja między serwerami MTA (relay) — tym portem jeden serwer pocztowy przekazuje wiadomość do drugiego po drodze do odbiorcy
465/tcp	SMTPS	wysyłka od klienta (MUA) do serwera z szyfrowaniem TLS nawiązywanym od razu przy połączeniu (implicit TLS)
587/tcp	Submission	wysyłka od klienta (MUA) do serwera, połączenie zaczyna się jako zwykłe, nieszyfrowane, a szyfrowanie włącza się komendą `STARTTLS` w trakcie sesji

Uważaj: port 25 jest tym, który blokuje większość dostawców internetu dla zwykłych łączy domowych i wiele serwerów aplikacyjnych w chmurze domyślnie — to jest powód, dla którego serwer aplikacyjny wysyłający pocztę przez zewnętrzny przekaźnik łączy się z nim zwykle na porcie 587 albo 465, a nie na 25, co opisujemy szerzej na stronie Postfix: konfiguracja.

Koperta a nagłówki

> **Pojęcie: koperta SMTP (envelope).** Adresy nadawcy i odbiorcy przekazywane w samym protokole SMTP komendami `MAIL FROM` i `RCPT TO`, używane przez serwery do faktycznego routingu wiadomości — to jest adres, na który serwer próbuje dostarczyć wiadomość i na który wraca powiadomienie o błędzie dostarczenia, jeśli coś pójdzie nie tak.

> **Pojęcie: nagłówki wiadomości (headers).** Pola `From:`, `To:`, `Subject:` widoczne w treści samej wiadomości, wyświetlane użytkownikowi przez klienta pocztowego. Koperta i nagłówki nie muszą się pokrywać — to normalny mechanizm używany np. przy wysyłce w imieniu wielu adresów (`Send As` opisany na stronie MailCow), ale jest też mechanizmem nadużywanym w phishingu, gdzie nagłówek `From:` pokazuje zaufany adres, a koperta wskazuje zupełnie inny serwer nadawcy.

SPF, DKIM, DMARC

> **Pojęcie: SPF (Sender Policy Framework).** Rekord DNS typu TXT publikowany przez właściciela domeny, wymieniający, które serwery mają prawo wysyłać pocztę w imieniu tej domeny — serwer odbiorcy sprawdza adres IP, z którego faktycznie przyszło połączenie

SMTP, i porównuje go z listą w rekordzie SPF domeny z koperty (`MAIL FROM`). SPF sprawdza więc tylko, czy nadawca połączył się z dozwolonego adresu — nic nie mówi o integralności treści wiadomości.

Przykład rekordu SPF:

```
v=spf1 ip4:203.0.113.10 include:_spf.zielona.example -all
```

Pojęcie: DKIM (DomainKeys Identified Mail). Mechanizm podpisu kryptograficznego dodawanego do nagłówków wiadomości przez serwer wysyłający, weryfikowanego przez klucz publiczny opublikowany w rekordzie DNS TXT domeny nadawcy. W przeciwieństwie do SPF, DKIM sprawdza integralność samej treści — jeśli wiadomość zostanie zmieniona po drodze (nawet przez pośredniczący serwer), podpis przestaje się zgadzać.

Pojęcie: DMARC (Domain-based Message Authentication, Reporting and Conformance). Rekord DNS TXT mówiący odbiorcy, co zrobić z wiadomością, która nie przejdzie SPF ani DKIM (albo przejdzie, ale niezgodnie z domeną z nagłówka `From:`) — możliwe polityki to `none` (nic nie rób, tylko raportuj), `quarantine` (do spamu) i `reject` (odrzuć). DMARC dodatkowo wiąże wynik SPF/DKIM z domeną widoczną w nagłówku `From:`, czego żaden z tych dwóch mechanizmów osobno nie robi — to jest mechanizm, który realnie broni przed podszywaniem się pod domenę w polu widocznym dla użytkownika.

DMARC opisuje dziś RFC 9989 z maja 2026 roku, który zastąpił RFC 7489: rekord nadal zaczyna się od `v=DMARC1`, ale znacznik `pct` przeszedł do historii, a doszły `np` i `t`. Rekordy dla Zielonej i systemów wysyłających w jej imieniu są na stronie SPF, DKIM i DMARC: trzy podejścia do poczty i systemy wysyłające w imieniu domeny, droga od `p=none` do `p=reject` na stronie Droga DMARC od p=none do p=reject z raportami parsedmarc na docker01, a szyfrowanie między serwerami (MTA-STS, TLS-RPT) na stronie MTA-STS i TLS-RPT: szyfrowanie poczty między serwerami, a BIMI informacyjnie.

Mechanizm	Co sprawdza	Gdzie żyje
SPF	czy adres IP nadawcy jest na liście dozwolonych dla domeny koperty	rekord DNS TXT
DKIM	czy treść wiadomości nie została zmieniona po podpisaniu	rekord DNS TXT (klucz publiczny) + nagłówek `DKIM-Signature`
DMARC	co zrobić, gdy SPF/DKIM zawiodą, i czy wynik zgadza się z domeną z `From:`	rekord DNS TXT

Rekordy MX i PTR

> **Pojęcie: rekord MX (Mail Exchanger).** Rekord DNS domeny odbiorcy, wskazujący nazwę serwera (albo kilku serwerów z priorytetami), do którego inne MTA mają wysyłać pocztę dla tej domeny — to właśnie ten rekord sprawdza MTA nadawcy, żeby w ogóle wiedzieć, dokąd się połączyć.

Przykład:

```
zielona.example.    3600    IN    MX    10 poczta.zielona.example.
```

> **Pojęcie: rekord PTR (reverse DNS).** Rekord odwrotny, przypisujący nazwę domenową do adresu IP — w przeciwieństwie do zwykłego rekordu A (nazwa → IP), PTR działa w drugą stronę (IP → nazwa) i jest utrzymywany przez właściciela zakresu adresów IP, nie przez właściciela domeny. Wiele serwerów pocztowych na świecie odrzuca albo mocno punktuje ujemnie połączenia z adresów IP bez poprawnie skonfigurowanego PTR, traktując jego brak jako sygnał serwera niewłaściwie skonfigurowanego albo pochodzącego z puli adresów dynamicznych typowych dla spamerów.

Częste błędy

Traktowanie SPF jako wystarczającego zabezpieczenia. SPF sam w sobie nie chroni przed podszywaniem się pod adres widoczny w kliencie pocztowym (nagłówek `From:`) — chroni tylko adres z koperty, który użytkownik zwykle w ogóle nie widzi. Pełna ochrona wymaga DMARC wiążącego oba mechanizmy z widoczną domeną nadawcy.

Brak rekordu PTR dla serwera wysyłającego. Wiadomości wysyłane z serwera bez poprawnego PTR trafiają do spamu albo są odrzucane przez sporą część odbiorców, mimo poprawnie skonfigurowanego SPF i DKIM — PTR ustawia dostawca łącza albo hostingu, nie da się go dodać samodzielnie w DNS własnej domeny.

□□ Ćwiczenia

Ćwiczenie 1 — sprawdzenie rekordów własnej domeny

```
dig +short TXT zielona.example | grep spf
dig +short MX zielona.example
dig +short -x 203.0.113.10
```

Sprawdzamy kolejno rekord SPF, rekord MX i rekord PTR dla wybranego adresu IP wysyłającego pocztę.

Odpowiedź

Pierwsza komenda pokazuje politykę SPF domeny, druga serwer(y) przyjmujące pocztę dla tej domeny, trzecia nazwę domenową przypisaną do adresu IP — brak wyniku w trzeciej komendzie oznacza brak skonfigurowanego PTR dla tego adresu.

Pytania kontrolne

1. Dlaczego wiadomość może przejść SPF, a mimo to zostać odrzucona przez DMARC?

Odpowiedź

SPF sprawdza domenę z koperty (`MAIL FROM`), a DMARC dodatkowo wymaga, żeby domena, która przeszła SPF (lub DKIM), zgadzała się z domeną widoczną w nagłówku `From:` — jeśli te dwie domeny się różnią, DMARC uznaje to za niezgodność, nawet gdy SPF samo w sobie przeszło pozytywnie.

Powiązane: SPF, DKIM i DMARC: trzy podejścia do poczty i systemy wysyłające w imieniu domeny · Droga DMARC od p=none do p=reject z raportami parsedmarc na docker01 · MTA-STS i TLS-RPT: szyfrowanie poczty między serwerami, a BIMI informacyjnie · Postfix: konfiguracja · Kolejka Postfiksa: podgląd, wymuszenie, czyszczenie · Diagnostyka dostarczania

Źródła: RFC 5321 (SMTP) · RFC 7208 (SPF) · RFC 6376 (DKIM) · RFC 9989 (DMARC, maj 2026, zastąpił RFC 7489; zmiany opisuje strona o SPF, DKIM i DMARC w książce o domenie)