

MPP (Message Processing Platform) Enhanced Edition jest kompleksowym systemem bezpieczeństwa dla serwera poczty elektronicznej. Zapewnia pełną ochronę poczty przed wirusami, phishingiem i spamem, daje możliwość archiwizacji poczty przychodzącej i wychodzącej, filtrowania zawartości poczty oraz chroni serwer przed niektórymi atakami DoS. MPP dostępny jest w postaci oprogramowania na serwer lub bramkę pocztową lub też w postaci urządzenia podłączanego bezpośrednio do chronionej sieci.

Modułowa budowa systemu MPP Enhanced Edition sprawia, że może on zostać bardzo łatwo dopasowany do potrzeb użytkowników. Podstawę stanowi moduł zarządzający MPP, w którym administrator definiuje całość polityki bezpieczeństwa dla poczty w firmie. Moduł ten zapewnia także pełną kontrolę nad funkcjami archiwizacji oraz filtrowania treści. Do modułu głównego MPP dołączane są dodatkowe skanery antywirusowe i antyspamowe. W zależności od zdefiniowanych polityk, różne grupy użytkowników mogą korzystać z różnych skanerów lub też z kilku skanerów jednocześnie.

Konsola zarządzająca

Graficzna konsola zarządzająca systemem MPP Enhanced Edition dostępna jest poprzez przeglądarkę internetową i pozwala ona na pełną konfigurację wszystkich parametrów systemu, w tym na zdefiniowanie polityk.

Definiowanie polityk

Konfiguracja systemu MPP Enhanced Edition odbywa się poprzez definiowanie tzw. polityk, czyli reguł postępowania. Polityki mogą być definiowane oddzielnie dla poszczególnych użytkowników, grup użytkowników, adresów pocztowych, domen lub kierunków przepływu poczty (przychodząca/wychodząca). Definiując politykę administrator określa czy dana wiadomość ma być kontrolowana na obecność wirusów lub innych wrogich programów, czy ma być sprawdzana przez filtr antyspamowy, czy ma być sprawdzana pod kątem zawartości niepożądanych treści i czy ma podlegać archiwizacji. W polityce zawarte są także szczegółowe informacje o akcjach, jakie mają zostać podjęte przez system w przypadku wykrycia wirusa, zakwalifikowania wiadomości jako spam lub w przypadku stwierdzenia w wiadomości niepożądanych treści. Elastyczność w zakresie definiowania polityk daje

administratorowi bardzo dużą swobodę i pozwala na idealne dopasowanie systemu do standardów bezpieczeństwa obowiązujących w danej firmie.

Skanery antywirusowe

MPP Enhanced Edition pozwala na kontrolę przychodzących i wychodzących wiadomości pod kątem obecności wirusów oraz innych wrogich programów. Standardowo MPP posiada wbudowany skaner antywirusowy ClamAV. Istnieje możliwość podłączenia dodatkowych skanerów antywirusowych: NOD32, Kaspersky, Sophos. W zależności od ustawień określonych w politykach, różne wiadomości mogą być sprawdzane różnymi skanerami. Możliwe jest również skonfigurowanie polityki w taki sposób, aby jedna wiadomość była sprawdzana więcej niż jednym skanerem antywirusowym.

Skanery antyspamowe

System MPP Enhanced Edition jest zintegrowany z podstawowym skanerem antyspamowym SpamAssassin. Podobnie jak w przypadku skanerów antywirusowych, istnieje możliwość podłączenia innych skanerów antyspamowych: Cloudmark Authority lub Mailshell, które pozwalają na niemal stuprocentowe odfiltrowanie spamu. W zależności od ustawień określonych w politykach, różne wiadomości mogą być skanowane różnymi filtrami antyspamowymi. Możliwe jest także skanowanie jednej wiadomości kolejno kilkoma filtrami antyspamowymi. Każdy z filtrów pracujących w systemie MPP może być niezależnie ustawiony na inną czułość, co pozwala na bardzo precyzyjne ich dostrojenie. Dodatkowo istnieje możliwość ustawienia białej i czarnej listy.

MPP zawiera zintegrowany *Postfix Policy Server*. Dzięki temu może odrzucić niepożądane maile zanim trafią one na serwer. Decyzje o dostępie przekazane są

**kompletny system
bezpieczeństwa dla
bramki lub serwera
pocztowego**

**zarządzanie przez
www w trybie
graficznym**

**pełna ochrona
antywirusowa**

**pełna ochrona
antyspamowa**

**filtrowanie treści
wiadomości**

archiwizacja poczty

**wymienne skanery
antywirusowe i
antyspamowe**

**definiowanie
polityk wg
użytkownika,
grupy, adresu,
domeny lub
kierunku
przesyłania**

przez serwer Postfix na serwer polityk podczas sesji SMTP. MPP może podejmować decyzje czy odrzucić wiadomość zanim trafi ona na serwer poczty czy pozwolić na przekazanie i przeskanowanie wiadomości przez system MPP. Już podczas sesji SMTP pewne cechy mogą wskazywać na to, że dana wiadomość jest spamem. W przypadku innych serwerów poczty sesja SMTP odbywa się pomiędzy serwerami i dopiero po otrzymaniu wiadomości przez serwer odbywa się skanowanie poprzez system MPP.

Filtrowanie treści

Moduł filtrowania treści pozwala na kontrolę poczty przychodzącej i wychodzącej pod kątem zawartości określonych słów czy wyrażań lub też pod kątem zawartości określonych załączników. Pozwala zatrzymać wiadomości mogące zawierać informacje, które nie powinny wyjść poza firmę np. informacje poufne.

Treść wiadomości, jej temat i nagłówek mogą być filtrowane pod kątem zawartości określonych słów lub wyrażań, które definiowane są w politykach przez administratora w postaci wyrażań regularnych. Co ważne, system rozpoznaje także polskie znaki (standard UTF-8). Załączniki wiadomości mogą być filtrowane pod kątem określonej nazwy, rozszerzenia lub zawartej treści.

Dodatkowo system pozwala na zdefiniowanie tzw. list dostępu określających reguły wysyłania i odbierania wiadomości. Listy dostępu dają możliwość szczegółowego określenia, na jakie adresy dana osoba może wysyłać pocztę lub z jakich może ją otrzymywać.

W przypadku wykrycia wiadomości, która zawiera niepożądaną treść lub załącznik, system podejmuje akcję zgodną ze zdefiniowaną polityką bezpieczeństwa.

System pozwala na odłączenie od przychodzącej wiadomości jej załącznika, umieszczenie go na serwerze FTP lub HTTP, a następnie dołączenie do maila jedynie linka do miejsca, w którym został zapisany załącznik (funkcja *body stripping*).

Pozwala to na zmniejszenie rozmiarów skrzynek pocztowych, a także daje firmie lepszą kontrolę nad poufnymi dokumentami.

Archiwizacja wiadomości

System MPP Enhanced Edition umożliwia archiwizację przychodzących oraz wychodzących wiadomości. Archiwum może być utworzone w formacie MySQL, Maildir lub w postaci zwykłego pliku. W zależności od potrzeb możliwe jest archiwizowanie wiadomości od wybranych użytkowników, grup użytkowników, z wybranych domen lub w zależności od kierunku przepływu poczty (przychodząca/wychodząca). Archiwizacji mogą podlegać wszystkie wiadomości lub tylko te, które uznano za pożądane (nie zawierają wirusów i nie są spamem).

Kwarantanna

Kwarantanna jest miejscem przechowywania wiadomości, które zostały zatrzymane z powodu wykrycia wirusa, niepożądanego treści lub też sklasyfikowania wiadomości jako spam. W systemie MPP Enhanced Edition każdy użytkownik może mieć własny katalog kwarantanny, do którego może mieć pełny dostęp (w zależności od polityki zdefiniowanej przez administratora).

Moduł qReview

Moduł qReview (płatny dodatkowo) pozwala na zarządzanie katalogiem kwarantanny. Dostępny jest poprzez przeglądarkę internetową i pozwala na łatwe przeglądanie, sortowanie i wyszukiwanie wiadomości znajdujących się w kwarantannie. qReview umożliwia także uwalnianie wiadomości z kwarantanny, wysyłanie ich pod wskazany adres lub też ich kasowanie. Moduł ten pozwala także na tworzenie indywidualnych białych i czarnych list przez użytkowników. qReview może być poszerzony o funkcję zarządzania katalogiem archiwum (MPP-AR), która pozwala na łatwe przeglądanie i wyszukiwanie wiadomości znajdujących się w archiwum. Wiadomości mogą być wyszukiwane według ciągu znaków w treści lub temacie wiadomości, adresu nadawcy, określonej daty lub przedziału czasowego.

Wymagania:

Linux (i386, PPC, glibc 2.3 lub nowszy)
FreeBSD 6 lub nowszy
Solaris 8/9 (Sparc)
Mac OS X 10.3 lub nowszy (PPC, i386)

Wspierane serwery pocztowe:

Sendmail
Qmail
Postfix
SurgeMail
CommuniGate Pro
Exim
Sun Java Systems
Messaging Server

Wspierane skanery:

Anty-spamowe:
SpamAssassin, Cloudmark, Mailshell
Antywirusowe:
ClamAV, NOD32, Kaspersky, Sophos.