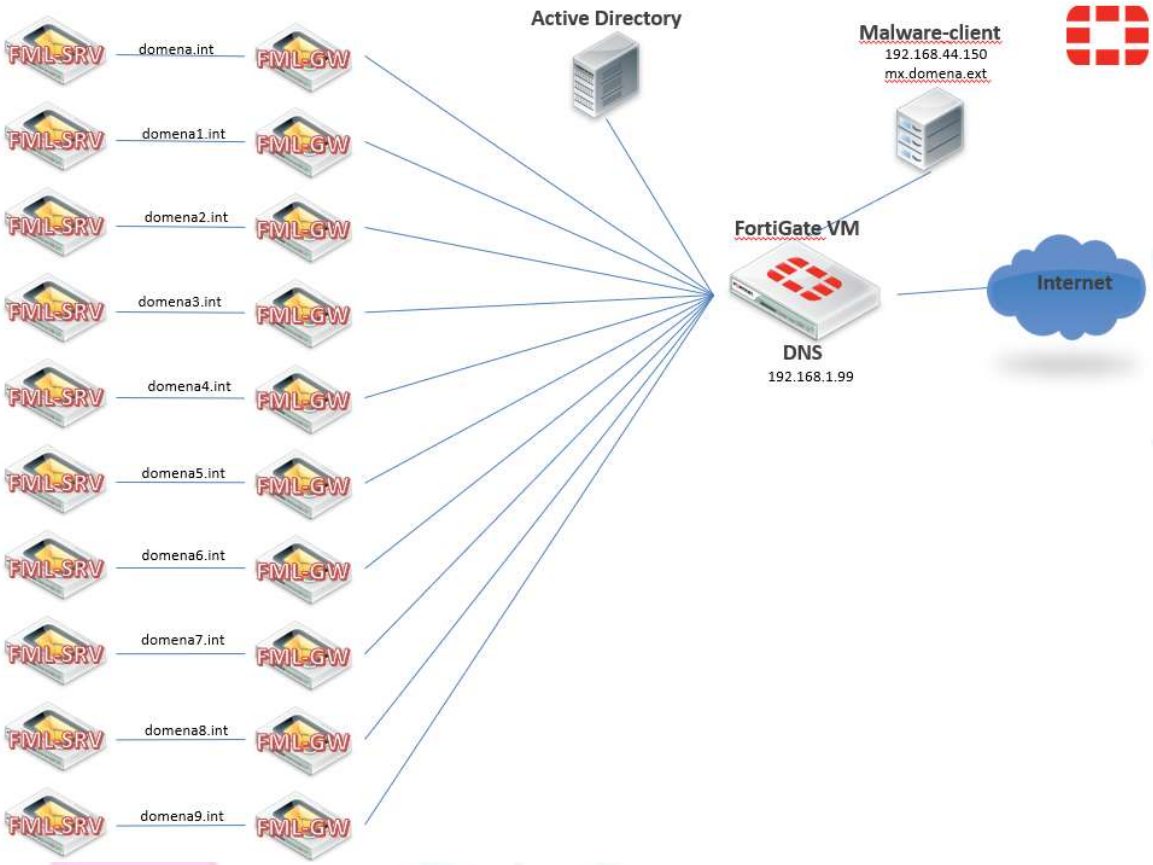
FortiMail Szkolenie

Wersja 7.6.

Maciej Gradzik

Spis treści

Topologia Środowiska



Podstawowe pojęcia:

- **MUA - Mail User Agent**. Komunikuje się z predefiniowanym serwerem obsługującym jego domenę używając ESMTP (najczęściej uwierzytelnionego i szyfrowanego) do wysyłki poczty i POP lub IMAP (zawsze uwierzytelnionego, często szyfrowanego) do jej odbioru.
- **MTA - Mail Transfer Agent.** Dystrybuuje pocztę do innych MTA znajdowanych dzięki rekordom MX w DNS. Komunikacja ta jest generalnie nieuwierzytelniona i nieszyfrowana.
- **MX - Mail Exchanger**. Dodatkowy rekord w DNS wskazujący system lub systemy odpowiedzialne za dystrybucję poczty dla danej domeny
- **Open Relay - MTA**, który akceptuje w nieuwierzytelniony sposób pocztę dla nieswojej domeny

Zasada działania DNS

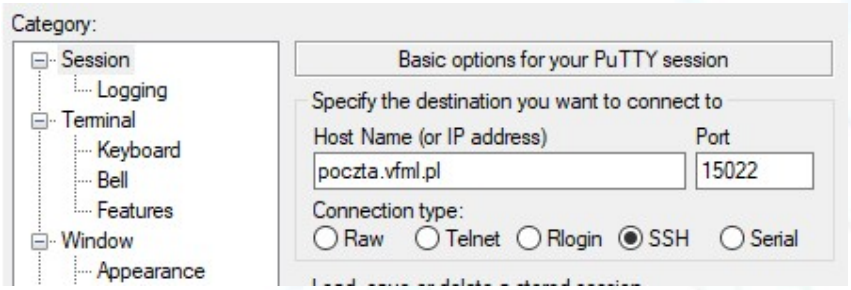
Rekordy Mail Exchange (MX) kierują pocztę e-mail na serwery w danej domenie. Dla domeny można zdefiniować wiele rekordów MX, każdy z różnym priorytetem, przy czym najniższa cyfra oznacza najwyższy priorytet. Jeśli nie można dostarczyć poczty za pomocą rekordu o najwyższym priorytecie, jest używany rekord o drugim priorytecie i tak dalej.

Aby skonfigurować pocztę należy najpierw zmodyfikować rekordy MX, tak by wskazywały serwery pocztowe.

Funkcja routingu poczty w naszej sieci wykonywana jest przy użyciu rekordów DNS skonfigurowanych na serwerze DNS (FortiGate) dostępnym na hoście pod adresem: 192.168.1.99. (topologia sieci).

1. Z hosta „malware-client" logujemy się poprzez SSH

   Użytkownik: malware-client
   hasło: fortinet



2. za pomocą *nslookup* możemy wyświetlić rekordy MX skojarzone z domeną domena.int:

```
nslookup -type=mx domenaXX.int
```

Powinniśmy otrzymać poniższy wynik:

```
malware-client@malware-client:~$ nslookup -type=mx domenal.int
Server:         127.0.1.1
Address:        127.0.1.1#53

domenal.int     mail exchanger = 10 mx.domenal.int.
```

W wyniku widzimy, że istnieją rekord MX związane z domeną *domenaX.int*:
mx.domenaX.int preference 10

FQDN dla FortiMail'a w trybie bramy to *mx.domena.int*. Oznacza to, że każdy e-mail dla domeny *domena.int* zostanie najpierw przekazany do FortiMail w trybie Gateway. Z punktu widzenia routingu poczty, gdy rekord MX zostanie zwrócony, DNS serwer sprawdzi wpis A i zostanie skojarzony z tym hostem.

3. Sprawdzimy czy host *mx.domena.in*t wskazuje na prawidłowy adres. Można to zweryfikować za pomocą nslookup:

```
nslookup -type=a mx.domenaXX.int
```

Powinniśmy otrzymać poniższy wynik:

```
malware-client@malware-client:~$ nslookup -type=a mx.domenal.int
Server:         127.0.1.1
Address:        127.0.1.1#53

Name:   mx.domenal.int
Address: 192.168.1.11
```

Używając powyższych czynności sprawdzamy rekordy DNS MX dla domeny *domena.ext*. Na przykład:

```
nslookup -type=mx domena.ext
```

I. Konfiguracja chronionej domeny:

Pojedynczy serwer pocztowy

1. Logujemy się do GUI FortiMail'a w trybie gateway:

   URL: *https://poczta.vfml.pl:XX443/admin/* **TABELA !!!**

2. Przechodzimy do *System* > *Mail Settings* w zakładce *Mail Server Settings*, konfigurujemy:

Host name: mx

Local domain name: *domenaX.int*

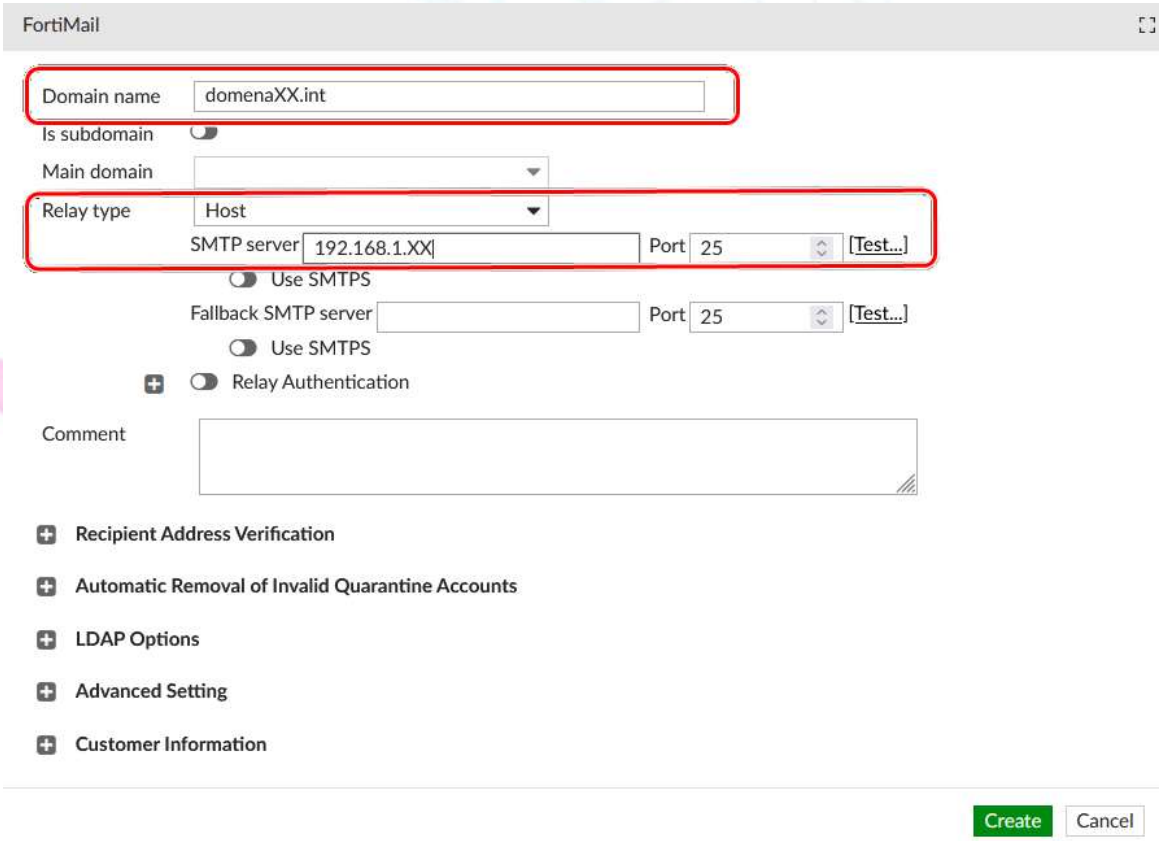
Pozostałe opcje zostawiamy z domyślnymi ustawieniami, zatwierdzamy *Apply*.

Na chwilę obecną nie zostały jeszcze skonfigurowane chronione domeny. Oznacza to, że ze cały ruch pocztowy uważany jest za wychodzący (*outgoing).*

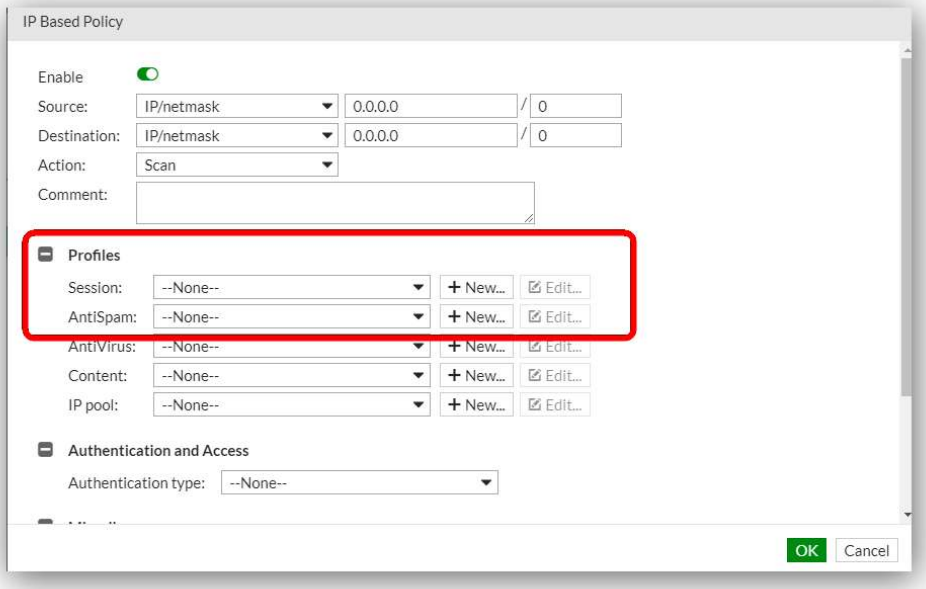
3. Następnie przechodzimy do *Domain&User* > *Domain* i wybieramy *New* w celu skonfigurowania chronionej domeny:

```
Domain name: domenaX.int
Relay Type:      Host
SMTP Server:     192.168.1.XXX TABELA !!!
```

Pozostałe opcje zostawiamy z domyślnymi ustawieniami.



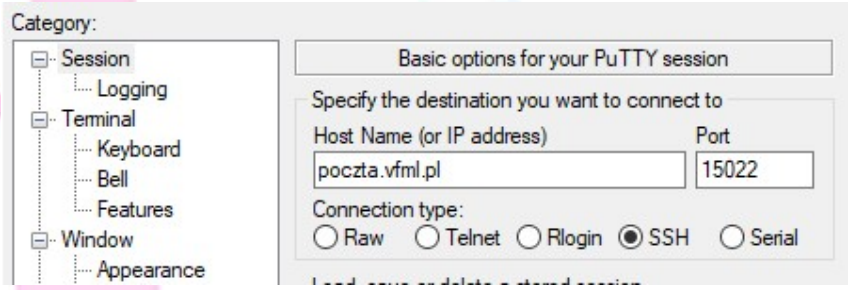
4. Przechodzimy do *Policy >IP Policy*. W domyślnej regule IP Policy odznaczamy profil sesyjny *Inbound_Session. **UWAGA:** Inbound_Session* wyłączamy również na naszym serwerze URL: https://poczta.vfml.pl:XX443/admin/ TABELA!!!



5. Aby sprawdzić, czy FortiMail jest gotów do zaakceptowania e-maili dla domeny domenaX.int, za pomocą telnet sprawdzamy komunikacje:

6. Logujemy się z „malware-client" poprzez SSH

Użytkownik: malware-client
hasło: fortinet

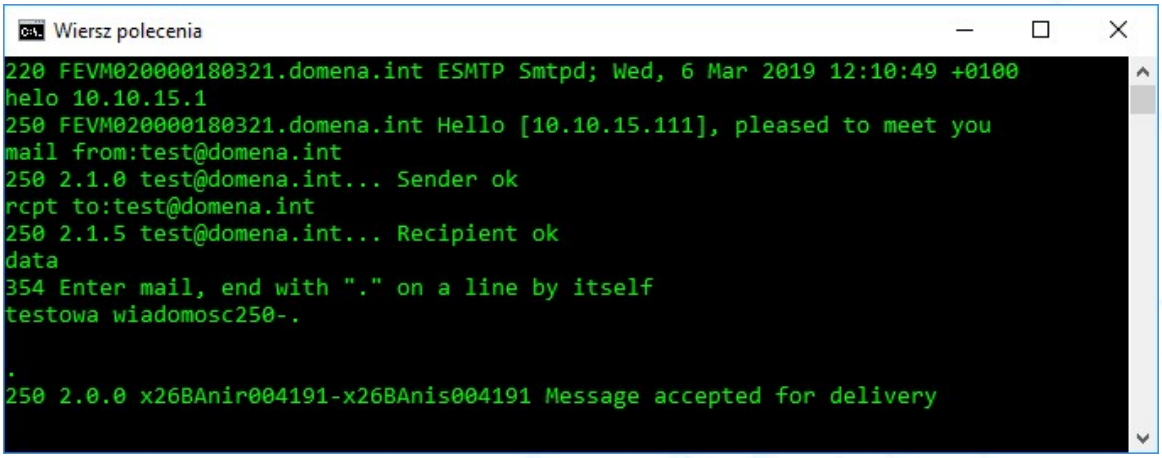


7. Uruchamiamy linie komend:

```
telnet mx.domenaXX.int 25
```

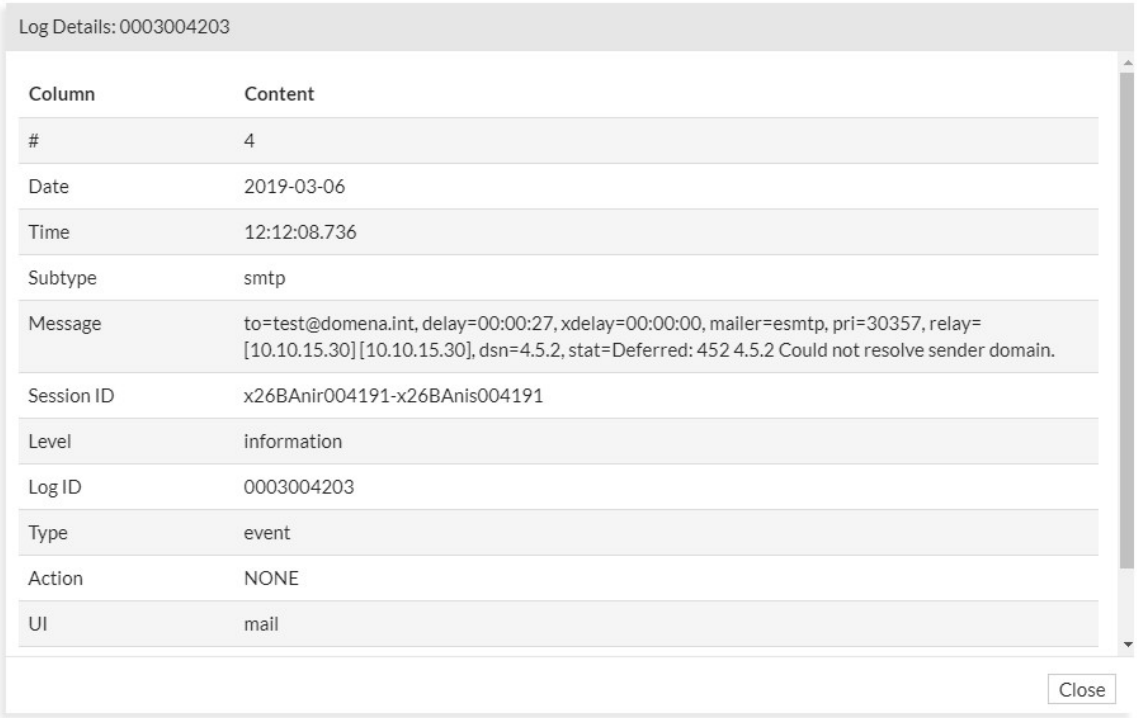
Następnie wysyłamy wiadomość wpisując kolejno:

```
helo 192.168.1.99
mail from:test@domenaXX.int
rcpt to:test@domenaXX.int
data
Testowa wiadomosc
.
```



Wiadomość powinna zostać zaakceptowana przez FortiMail. Ciąg znaków w postaci: x26BAnir004191-x26BAnis004191, to unikalny identyfikator sesji (ID session) wartość ta opisuje sposób przetwarzania wiadomości e-mail przez urządzenie. (kopiujemy wartość)

8. Logując się do FortiMail I przechodząc do *Monitor > Log > Mail Event*.
9. Klikamy *Search* I w polu *Session-ID* wklejamy skopiowany unikalny identyfikator sesji .
10. Z listy wyświetlonych logów znajdujemy log zaczynający się od *to=test@domena.int* i dwukrotnie w niego klikamy w celu wyświetlenia szczegółowych informacji.



Pole ***relay*** informuje gdzie wiadomość została przekazana

Pole ***stat*** informuje o statusie wiadomości oraz zawiera identyfikator sesji od MTA gdzie wiadomość została dostarczona.

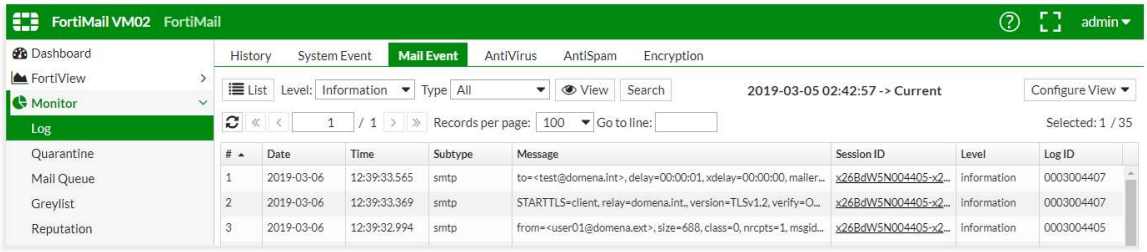
11. Aby odtworzyć wysyłanie wiadomości e-mail z zewnętrznej domeny *domena.ext* do domena.int, uruchamiamy wirtualną maszynę malware-client z zainstalowanym SquirrelMail (zewnętrzny MTA), poprzez adres URL możemy zalogować się do webmaila:

http://poczta.vfml.pl:16022/squirrelmail/src/login.php

Logujemy się za pomocą użytkownika ***userXX*** z hasłem ***fortinet***

12. Używając SquirrelMail wysyłamy wiadomość do: *test@domenaXX.int*. (Treść wiadomości dowolna)

Wiadomość powinna zostać dostarczona co można zaobserwować w logach.



II. Obsługa SMTP przez FortiMail

FortiMail jako MTA dla poczty przychodzącej i wychodzącej

SMTP to względnie prosty, tekstowy protokół, w którym określa się przynajmniej jednego odbiorcę wiadomości (w większości przypadków weryfikowane jest jego istnienie), a następnie przekazuje treść wiadomości. Demon SMTP działa najczęściej na porcie 25. Łatwo przetestować serwer SMTP przy użyciu programu telnet.

Chociaż będziemy używać różnych narzędzi podczas testów zawsze można (i jest to zalecane dla co najmniej jednego z testów) użyć usługi telnet do ustanowienia sesji SMTP. Przykłady sesji SMTP znajdziemy w linkach poniżej:

Przykłady sesji SMTP w linku poniżej:

https://pl.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

Bez względu, w jakim trybie pracuje FortiMail analiza poczty opiera się na domyślnych zasadach:

- dla domen chronionych domyślnym działaniem jest RELAY
- dla domen niezabezpieczonych domyślną akcją jest REJECT

W naszym teście skorzystamy z bardzo pomocnego narzędzia do testowania SMTP jakim jest SWAKS. Więcej szczegółów w linku poniżej:

http://www.jetmore.org/john/code/swaks/

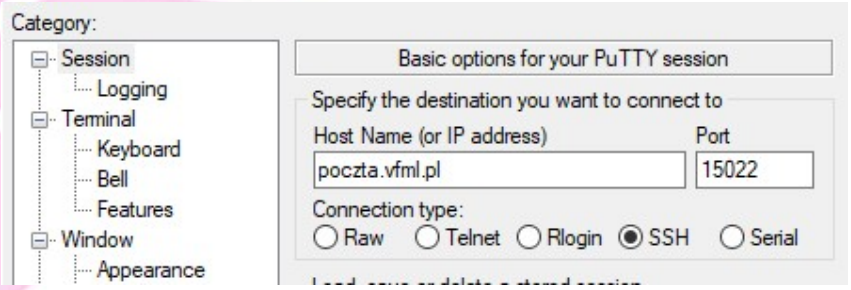
Wspomniany SWAKS jest dostępny poprzez SSH na maszynie „malware-client" pod adresem:

poczta.vfml.pl:15022

1. Logujemy się z „malware-client" poprzez SSH

Użytkownik: malware-client
hasło: fortinet

2. Uruchamiamy linie komend:



3. Wykonujemy kilka testów zgodnie z poniższymi opisami, które zobrazują domyślne zachowania FortiMaila w trybie Gateway: **(Sprawdz w tabeli lokalny adres IP !!!)**

```
· int-->int
swaks -f test@domenaXX.int -t test@domenaXX.int -s 192.168.1.XXX

· int-->ext
swaks -f test@domenaXX.int -t userXX@domena.ext -s 192.168.1.XXX

· ext-->int
swaks -f test@domena.ext -t test@domenaXX.int -s 192.168.1.XXX

· ext-->ext
swaks -f userXX@domena.ext -t userXX@domena.ext -s 192.168.1.XXX
```

oraz w trybie serwer:

```
· int-->int
swaks -f test@domenaXX.int -t test@domenaXX.int -s 192.168.1.XXX

· int-->ext
swaks -f test@domenaXX.int -t userXX@domena.ext -s 192.168.1.XXX

· ext-->int
swaks -f test@domena.ext -t test@domenaXX.int -s 192.168.1.XXX

· ext-->ext
swaks -f userXX@domena.ext -t userXX@domena.ext -s 192.168.1.XXX
```

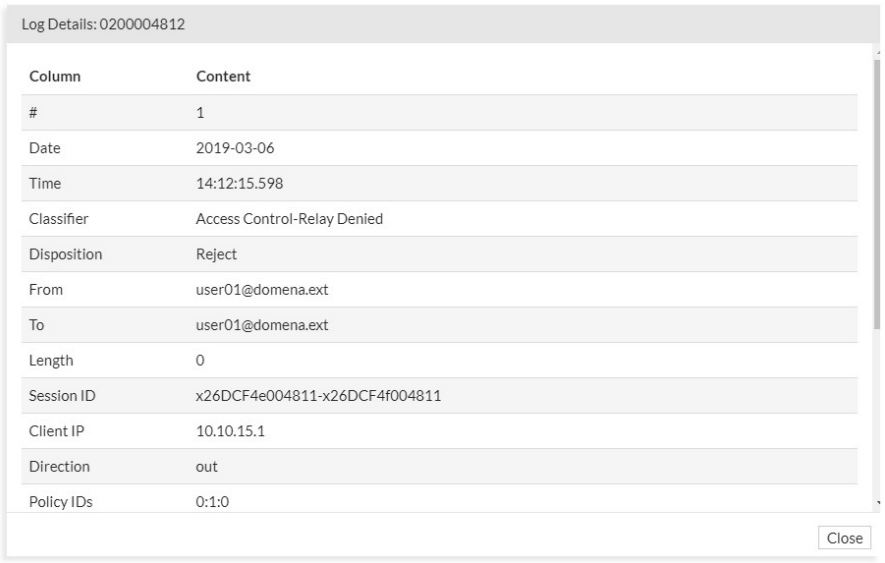
4. Obserwujemy każdą sesje, która została wygenerowana przez skrypt.

- Czy wszystkie wiadomości mogły zostać dostarczone?
- Jaka informacja została zwrócona przez sesję SMTP?
- Jaki był powód niedostarczenia wiadomości?

5. Logujemy się do GUI na FortiMail w jednym z poniższych trybów:

- Serwer: URL: *https://poczta.vfml.pl:XX443/admin/* **TABELA !!!**
- Gateway: URL: *https://poczta.vfml.pl:XX443/admin/* **TABELA !!!**
- Przechodzimy do *Monitor > Log* zakładka *History*.

W logach znajdziemy szczegółowe informacje o powodzie doręczenia lub nie doręczenia wiadomości. Poniżej przykład:



Weryfikacja adresów recipiet

Sprawdzenie adresu odbiorcy zapewnia, że FortiMail odrzuca wiadomości z nieprawidłowymi adresatami i nie skanuje ich ani nie wysyła ich na chroniony serwer pocztowy. Ta weryfikacja może zmniejszyć obciążenie FortiMail, gdy spamer próbuje wysłać wiadomości do każdego możliwego adresata na serwerze poczty e-mail.

Jeśli chcemy używać weryfikacji adresu odbiorcy, musimy zweryfikować adresy odbiorców wiadomości e-mail, korzystając z serwera poczty poprzez SMTP lub poprzez serwera LDAP.

Zwykle można użyć serwera poczty elektronicznej do przeprowadzania weryfikacji adresu.

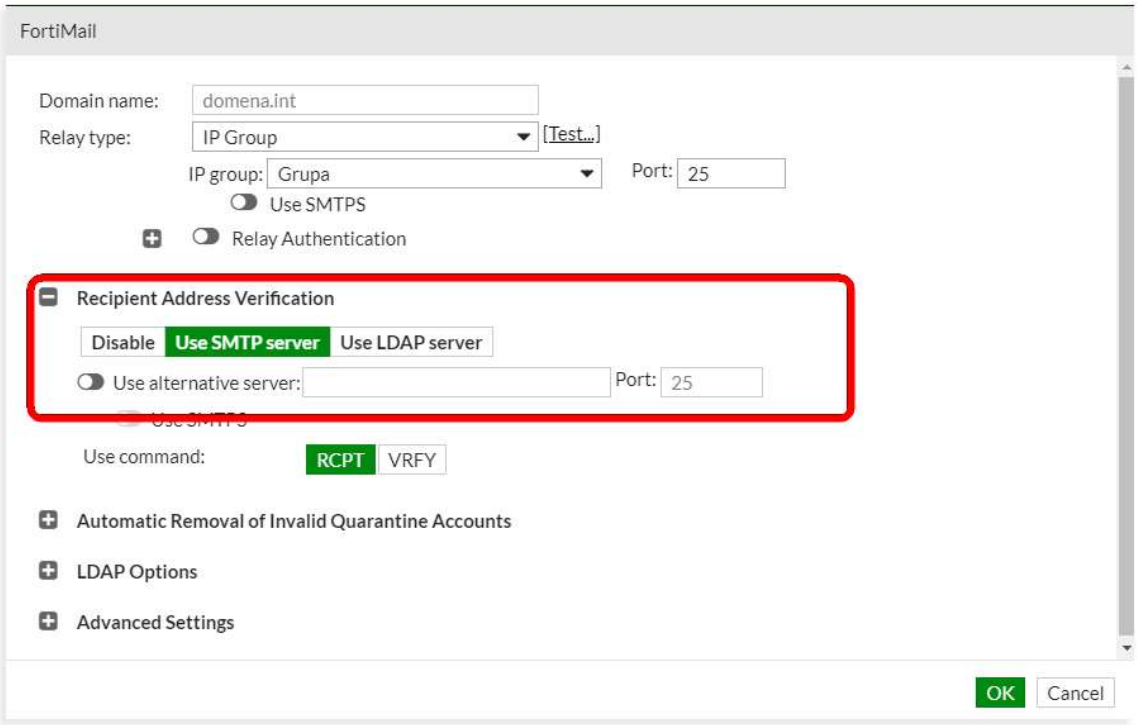
Weryfikacja adresów recipiet nie działa dla urządzenia w trybie serwera.

1. Logujemy się do GUI na FortiMail w trybie Gateway : URL: https://poczta.vfml.pl:XX443/admin/ **TABELA !!!**

2. przechodzimy do *Domain&User > Domain*

3. Wybieramy chronioną domenę *domena.int* a następnie *Edit*

4. Rozwijamy Recipient Address Verification, zaznaczamy opcję Use SMTP server, jak poniżej:



5. Za pomocą zewnętrznej domeny *domena.ext* wysyłamy wiadomość do użytkownika, który istnieje test@domena.int oraz do użytkownika, który nie został zdefiniowany np. test1@domenaXX.int, uruchamiamy wirtualną maszynę malware-client z zainstalowanym SquirrelMail (zewnętrzny MTA), poprzez adres URL możemy zalogować się do webmaila:

http://poczta.vfml.pl:16022/squirrelmail/src/login.php

Logujemy się za pomocą użytkownika ***userXX*** oraz hasłem ***fortinet***

6. Weryfikujemy zachowanie.

FortiMail jako proxy dla sesji uwierzytelnionych

Rozszerzeniem protokołu SMTP o mechanizmy uwierzytelniania to protokół SMTP-AUTH. Można wyróżnić dwie podstawowe metody autoryzacji sesji:

- metodą AUTH PLAIN
- metodą AUTH LOGIN

Każda z nich do komunikacji pomiędzy serwerem a klientem stosuje kodowanie Base64, które samo w sobie nie zapewnia bezpieczeństwa danych.

Aby skorzystać z autoryzacji, klient powinien zamiast standardowego powitania **HELO** użyć **EHLO**, które umożliwi wykorzystanie rozszerzonego zestawu poleceń SMTP. W odpowiedzi serwer SMTP powinien zwrócić w powitaniu ciąg znaków "AUTH", a po nim dostępne metody uwierzytelniania.

Tak jak w powyższym przykładzie pomocny będzie SWAKS warto żeby chociaż jeden test przeprowadzić używając telnet. W poniższych linkach szczegółowe informacje na temat rozszerzenia SMTP-AUTH oraz narzędzie do zakodowania i odkodowania Base64

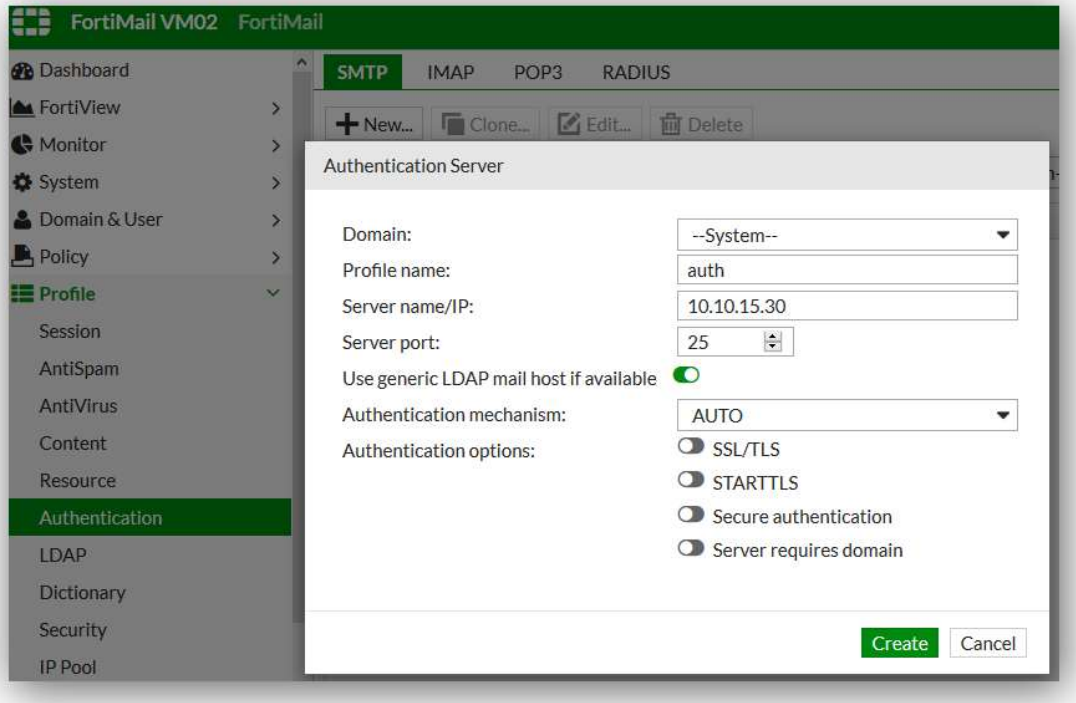
https://pl.wikipedia.org/wiki/SMTP-AUTH
https://www.base64encode.org/

1. Logujemy się do GUI na FortiMail w trybie Gateway:

   URL: *https://poczta.vfml.pl:XX443/admin/* **TABELA !!!**

2. Przechodzimy do *Profile* → *Authentication* zakładka *SMTP* wybieramy *New*
3. Konfigurujemy nowy profil zgodnie z poniższym:

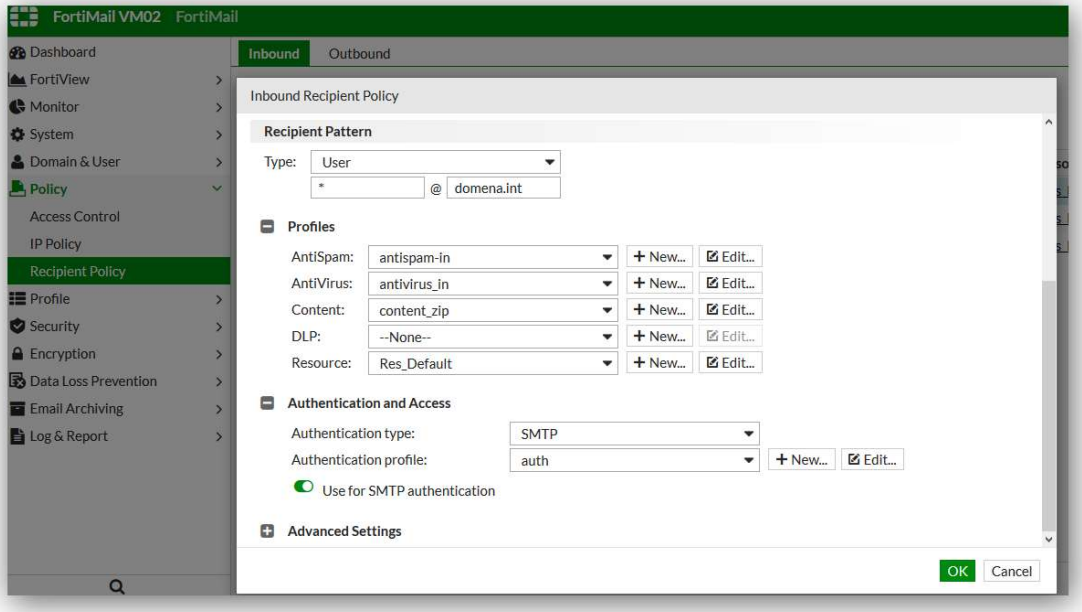
   Profile name: auth
   Server name/IP: **TABELA lokalny adres IP FML-SRV !!!**



Zatwierdzamy, *Create*

4. Następnie przechodzimy do *Policy* → *Recipient Policy* i edytujemy nasza regułę.
5. W polityce przechodzimy do sekcji *Authentication and Access* i ustawiamy:

   Authentication type: SMTP
   Authentication Profile: auth
   Use for SMTP authentication: włączamy

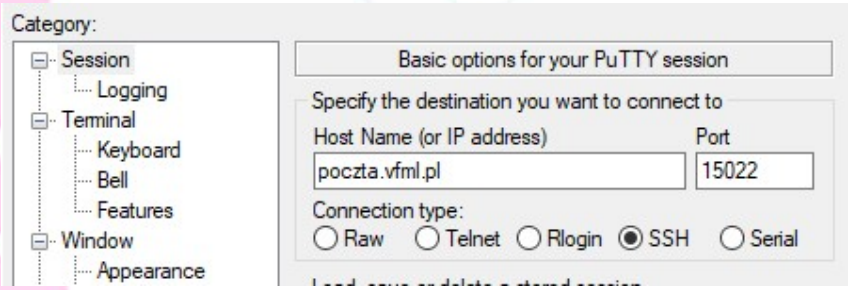


6. Zatwierdzamy, *OK*

7. Logujemy się z „malware-client” poprzez SSH

Użytkownik: malware-client
hasło: fortinet

8. Uruchamiamy linie komend:



9. Wykonujemy kilka testów zgodnie z poniższymi opisami, które zobrazują domyślne zachowania FortiMaila w trybie gateway

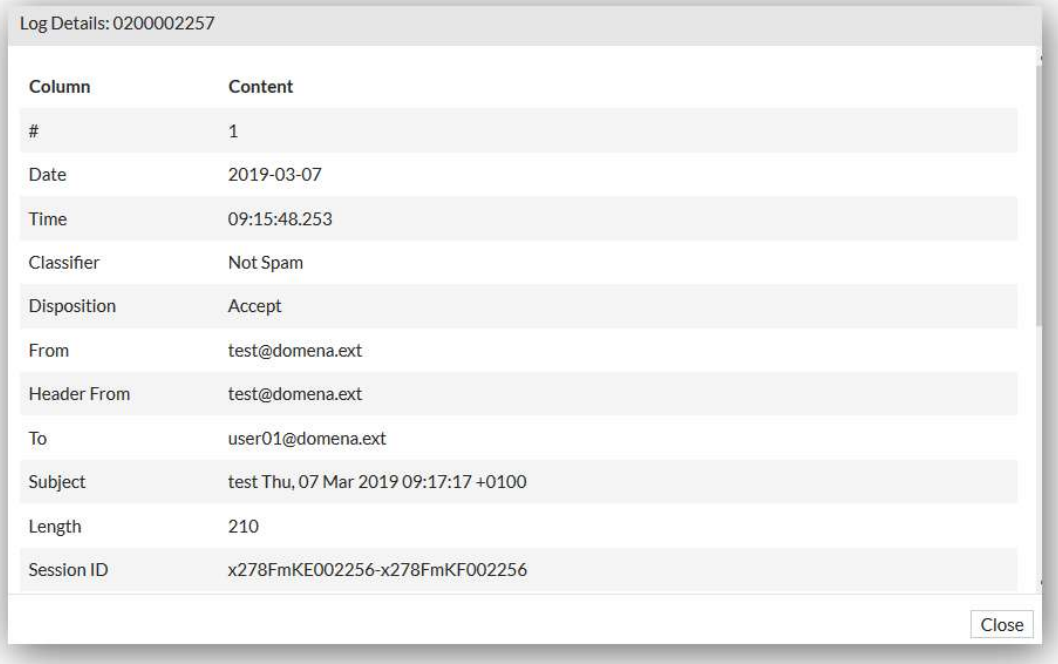
· int-->int
swaks -f test@domenaXX.int --auth-user=test --auth-password=test -t test@domenaXX.int -s 192.168.1.XXX
· int-->ext
swaks -f test@domenaXX.int --auth-user=test --auth-password=test -t userXX@domena.ext -s 192.168.1..XXX
· ext-->int
swaks -f test@domena.ext --auth-user=test --auth-password=test -t test@domenaXX.int -s 192.168.1.XXX
· ext-->ext
swaks -f test@domena.ext --auth-user=test --auth-password=test -t userXX@domena.ext -s 192.168.1.XXX
Oraz w trybie serwer
· int-->int
swaks -f test@domenaXX.int --auth-user=test --auth-password=test -t test@domenaXX.int -s 192.168.1.XXX
· int-->ext
swaks -f test@domenaXX.int --auth-user=test --auth-password=test -t userXX@domena.ext -s 192.168.1..XXX
· ext-->int
swaks -f test@domena.ext --auth-user=test --auth-password=test -t test@domenaXX.int -s 192.168.1.XXX
· ext-->ext
swaks -f test@domena.ext --auth-user=test --auth-password=test -t userXX@domena.ext -s 192.168.1.XXX

10. Logujemy się do GUI na FortiMail w jednym z poniższych trybów:

- Serwer: URL: *https://poczta.vfml.pl:XX443/admin/* **TABELA !!!**
- Gateway: URL: *https://poczta.vfml.pl:XX443/admin/* **TABELA !!!**

11. Przechodzimy do Monitor > Log zakładka History.

12. W logach znajdziemy szczegółowe informacje o powodzie doręczenia wiadomości. Poniżej przykład:



Jak widzimy FortiMail z obecnymi ustawieniami dla uwierzytelnionych sesji umożliwia przekazywanie ich dalej, czyli stanowi open relay

III. Konfiguracja i omówienie reguł Access Control

Polityki Access Control pozwalają kontrolować sposób przenoszenia wiadomości e-mail do i z, za pośrednictwem FortiMail. Korzystając z reguł kontroli dostępu, FortiMail może analizować wiadomości e-mail i podejmować działania w oparciu o wynik. Wiadomości można sprawdzać według adresu nadawcy, adresu odbiorcy oraz adresu IP lub nazwy hosta systemu dostarczającego wiadomość e-mail.

Każda reguła kontroli dostępu określa działanie, jakie należy podjąć w celu dopasowania wiadomości.

Biorąc pod uwagę powyższe testy z poprzedniego ćwiczenia urządzenie umożliwia przesyłanie poczty zgodnie z poniższa tabelą:

	Kierunek komunikacji	**Uwierzytelnianie**	**Akcja**
1.	int → int	off	relay
2.	int → int	on	relay
3.	int → ext	off	relay denied
4.	int → ext	on	relay
5.	ext → int	off	relay
6.	ext → int	on	relay
7.	ext → ext	off	relay denied
8.	ext → ext	on	relay

Niezbędne polityki do poprawnej obsługi ruchu

Analizując powyższe, można łatwo zauważyć, że nie potrzebujemy aż ośmiu reguł a można je łatwo zastąpić zaledwie trzema:

- reguły 1, 2, 3, 4 mogą zostać uproszczone do jednej która wymusza uwierzytelnianie w komunikacji int ---> * (gdziekolwiek) a pozostałe odrzuca,
- reguły 5 i 6 mogą pozostać domyślne,
- W przypadku reguł 7 i 8 wymagane jest odrzucenie przekazywania wiadomości (nawet dla uwierzytelnionych użytkowników)

Zalecane reguły kontroli dostępu powinny wyglądać jak w tabeli poniżej:

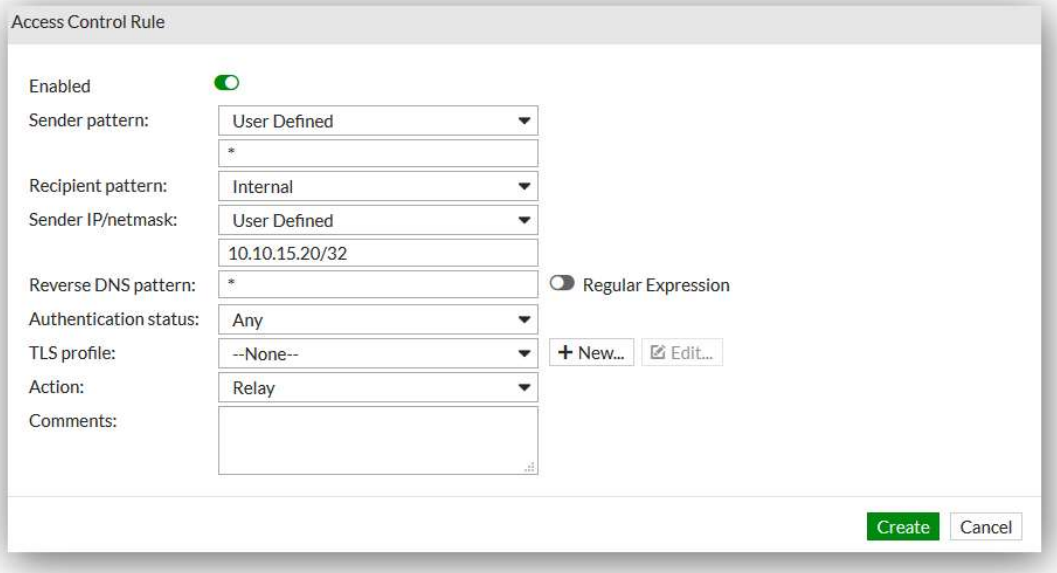
	Kierunek komunikacji	**Uwierzytelnianie**	**Akcja**
1, 2, 3, 4.	int → *	off	reject
5, 6.	int →*	on	relay
7, 8	ext → ext	on	reject

Plus dodatkowa reguła na ruch z naszego mx (brama FML) - Niezależnie od statusu AUTH (po prostu ufamy naszym własnym zasobom)

1. Logujemy się do GUI FortiMail'a w trybie **serwera**: URL: *https://poczta.vfml.pl:XX443/admin/* **TABELA !!!**
2. Przechodzimy do *Policy > Access Control* i w zakładce *Receiving*, wybieramy *New*: Konfigurujemy regułę zgodnie z poniższym:

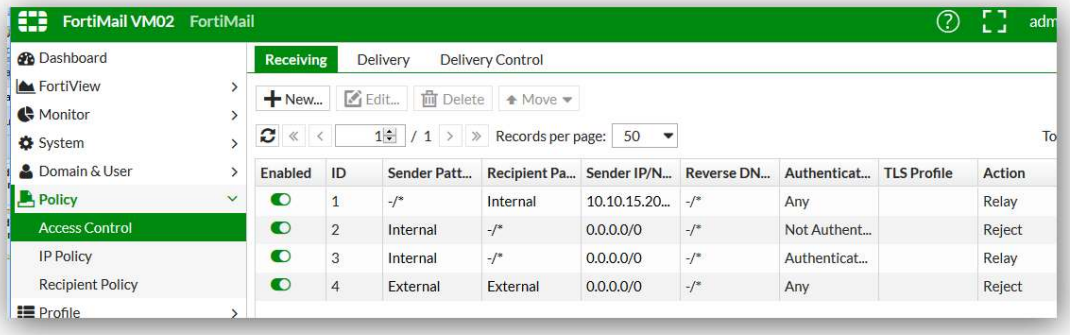
Enabled:	zaznaczamy
Sender pattern	User Defined / *

Recipient pattern:	Internal
Sender IP/netmask:	User Defined / **loalny adres IP FML-GW** !!
Authentication status	Any
Action	Relay



Zatwierdzamy klikając *Create*

3. Podobnie kreujemy pozostałe reguły zgodnie z powyższą tabelą.
4. W rezultacie powinniśmy otrzymać tak wyglądające reguły:



5. Ponownie korzystając ze SWAKS przeprowadzamy testy wcześniejsze testy tym razem ze stworzonymi regułami.
6. Jakie jest zachowanie FortiMaila?

……

Dla przypomnienia reguła 4 zabezpiecza nas przed open relayem

Teraz przejdziemy do konfigurowania FortiMaila w trybie Gateway. Zabezpieczenie przed open relay przeniesiemy na FortiMail będącego bramą dla FortiMaila Serwer.

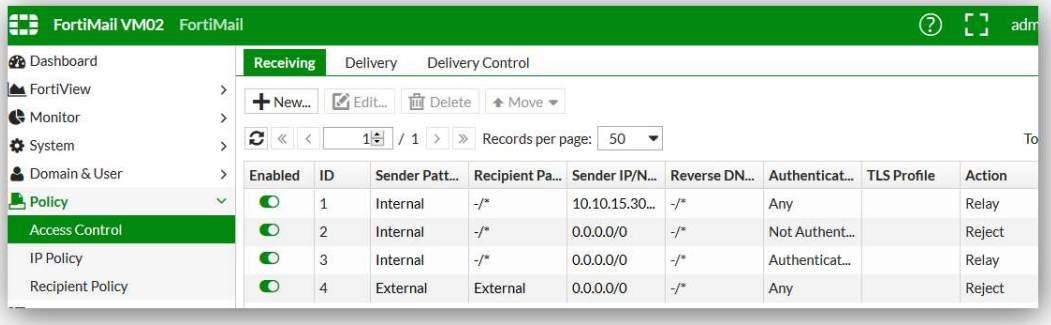
7. Wyłączamy przed chwilą utworzoną na serwerze regułę External →External.

8. Logujemy się do GUI FortiMail'a w trybie gateway: URL: *https://poczta.vfml.pl:XX443/admin/* **TABELA !!!**

9. Przechodzimy do *Policy* > *Access Control* i kreujemy reguły zgodnie z poniższym przykładem:

lp	Sender pattern	Recipient pattern:	Sender IP/netmask:	Authentication status	Action
1	Internal	User Defined / *	User Defined / **Lokalny adres IP FML_SRV !!!**	Any	Relay
2	Internal	User Defined / *	User Defined / 0.0.0.0/0	Not authenticated	Reject
3	Internal	User Defined / *	User Defined / 0.0.0.0/0	Authenticated	Relay
4	External	External	User Defined / 0.0.0.0/0	Any	Reject

Powinniśmy otrzymać efekt jak na rysunku poniżej:



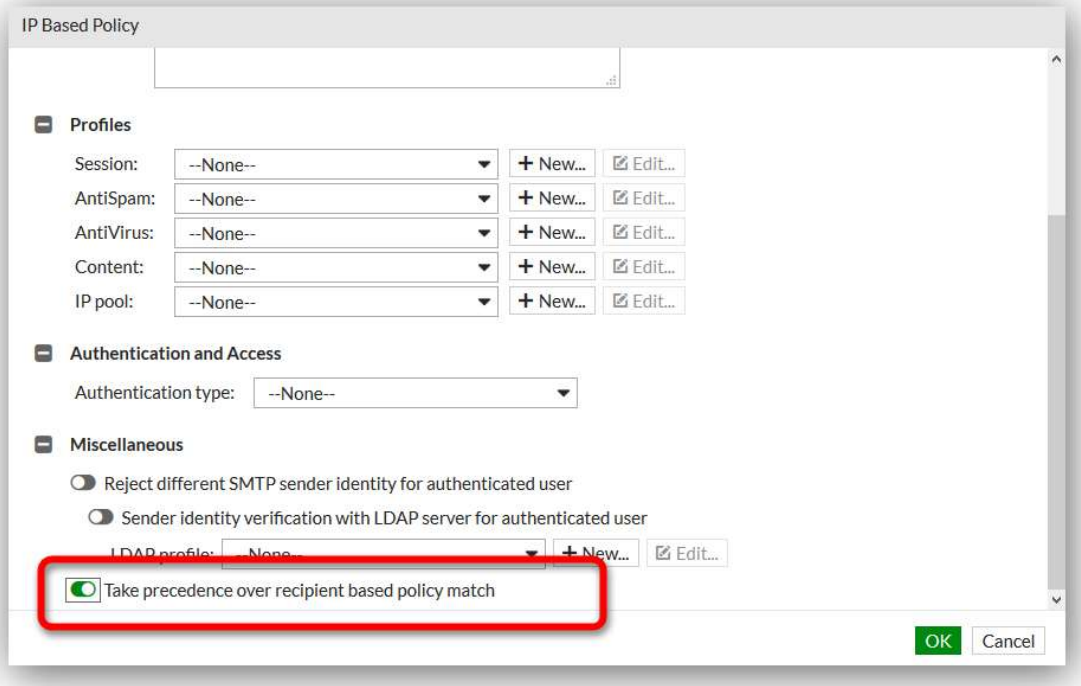
IV. Omówienie zasad działania reguł (IP Policies, Recipient Policies)

Polityki typu *IP Policies* umożliwiają tworzenie reguł uwzględniając profile do połączeń SMTP na podstawie adresów IP klientów SMTP i / lub serwerów.

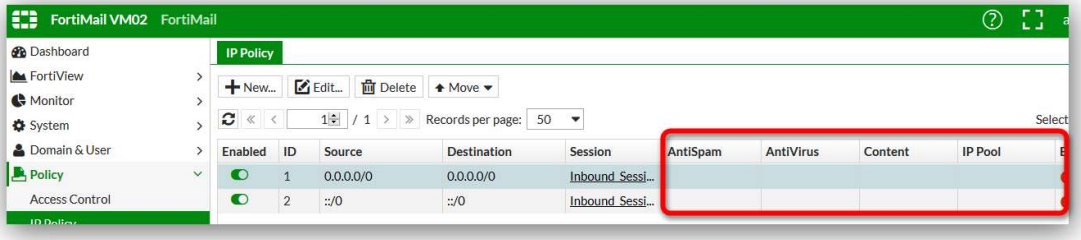
Ze względu na charakter połączenia SMTP, klient SMTP niekoniecznie musi znajdować się na komputerze użytkownika poczty e-mail. Klientem SMTP jest inicjator połączenia; Może to być na przykład MTA lub MUA, który próbuje dostarczyć pocztę elektroniczną. Natomiast serwerem SMTP jest zawsze serwer, który odbiera połączenie, może to być serwer pocztowy lub urządzenie które tą pocztę przekazuje (Gateway).

Polityki typu *Recipient Policy* umożliwiają tworzenie reguł opartych na odbiorcach chronionej domeny zarówno dla poczty przychodzącej jak i wychodzącej. Reguły *Recipient* mają pierwszeństwo przed politykami *IP Policy* jeśli chodzi o stosowanie profili ochronnych.

Wyjątkiem są polityki IP które mają włączona funkcję "*Take precedence over recipient based policy match*". Zgodnie z poniższym screen'em.

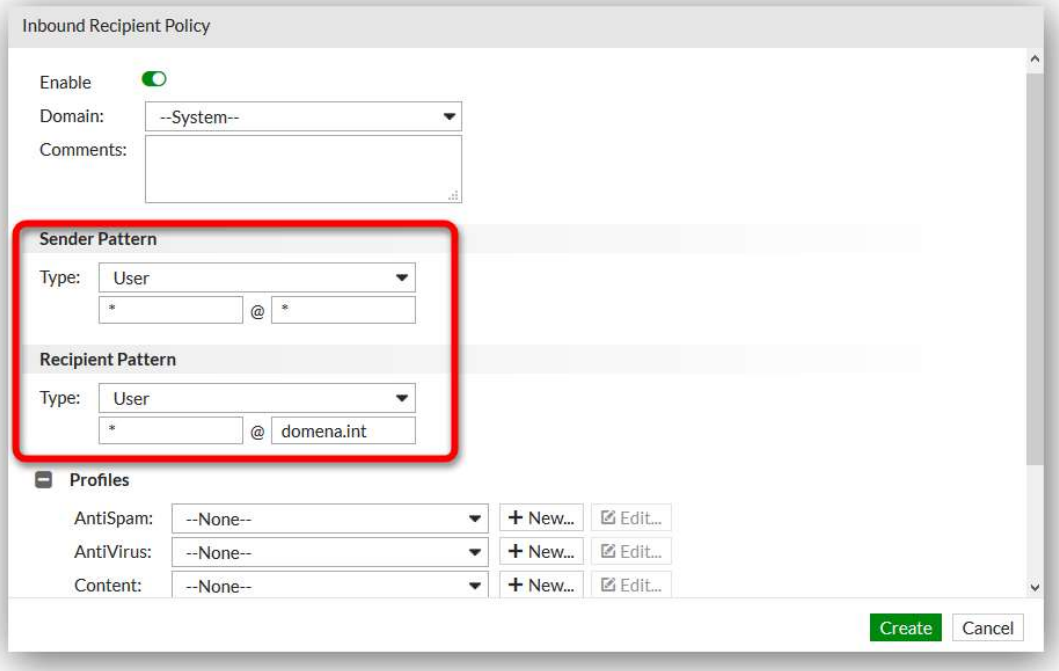


W naszych testach odpowiedzialność za ochronę serwera pocztowego przerzucimy na FortiMail w trybie Gateway w tym celu należy zweryfikować czy na FortiMailu w trybie serwera mamy wyłączone profile ochronne w politykach IP Policies:



1. Logujemy się do GUI FortiMail'a w trybie gateway: https://mx.domena.int/admin.
2. Przechodzimy do *Policy* > *Recipient Policy* wybieramy *New*
3. Konfigurujemy politykę zgodnie z poniższymi ustawieniami:

   Sender pattern: User *@*
   Recipient pattern: User *@domenaX.int



4. Zatwierdzamy poprzez *Create*
5. W kolejnych krokach właśnie do tej polityki będziemy stosować profile ochronne.

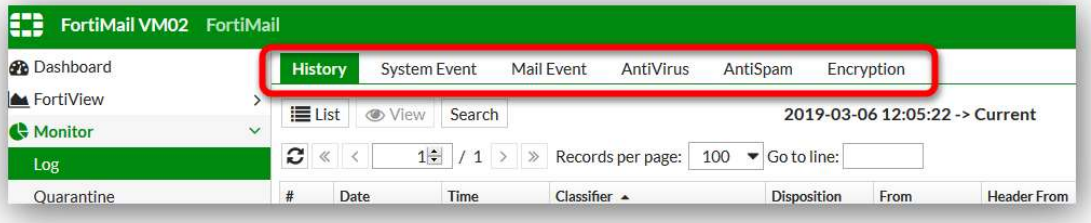
V. Analiza logów

Logując się na urządzenie w każdym trybie pracy mamy dostęp do logów. Domyślnie urządzenie przechowuje logi lokalnie, mogą one również zostać wyeksportowane na zewnętrzne zasoby, o czym będziemy mówić później. Logi na urządzeniu są składowane zgodnie z ustawieniami szczegóły możemy uzyskać logując się do urządzenia poprzez SSH:

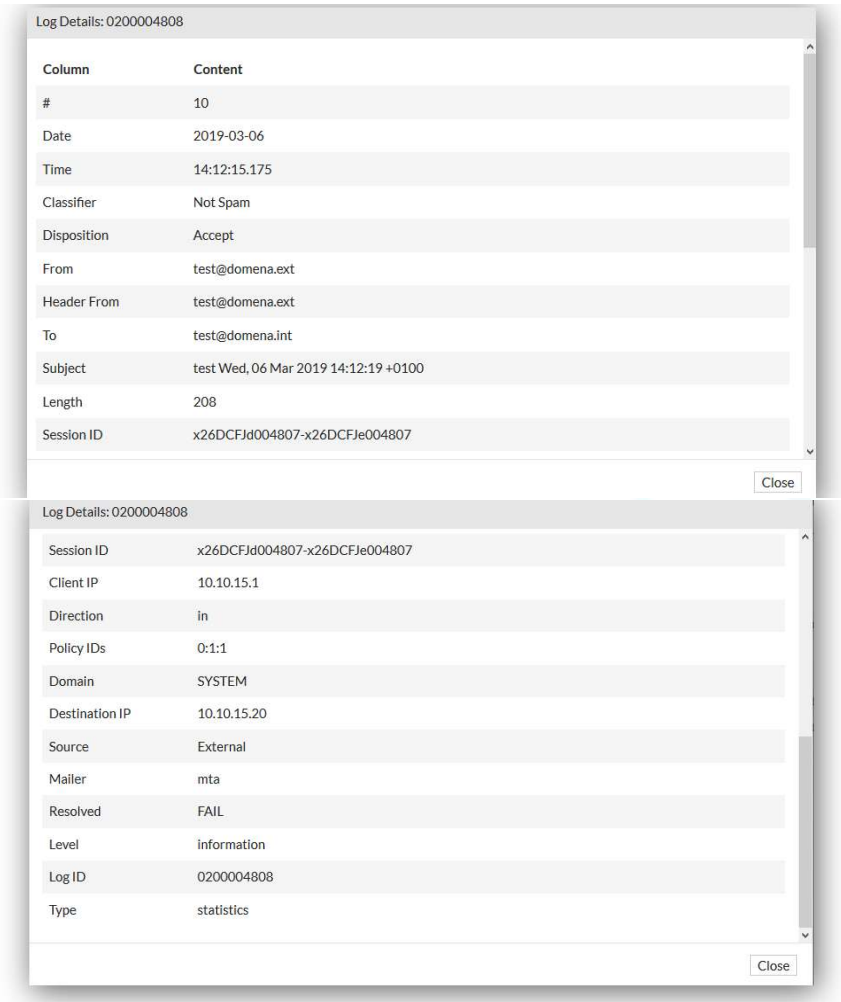
```
# config log setting local
(local) # show full-configuration
config log setting local
  set status enable
  set rotation-size 20
  set rotation-period 10
  set retention-period 0
  set rotation-hour 0
  set disk-full overwrite
  set loglevel information
  set event-log-category webmail smtp
  set event-log-status enable
  set sysevent-log-category configuration admin system ha update
  set system-event-log-status enable
  set antivirus-log-status enable
  set antispam-log-status enable
  set history-log-status enable
  set encryption-log-status enable
end
```

Przechodząc do *Monitor > Log* logi zostały podzielone na sekcje typu

- ***History*:** dziennik wysyłanych i niedostarczonych wiadomości e-mail SMTP.
- **System *Event***: dziennik czynności administratora i zdarzeń systemowych.
- ***Mail Event:*** zdarzenia związane z dostarczaniem poczty e-mail
- ***AntiVirus*:** rejestr poczty wykrytej jako zarażona wirusem.
- ***AntiSpam*:** rejestr wykrytych wiadomości jako spam.
- ***Encryption***: dziennik szyfrowania IBE

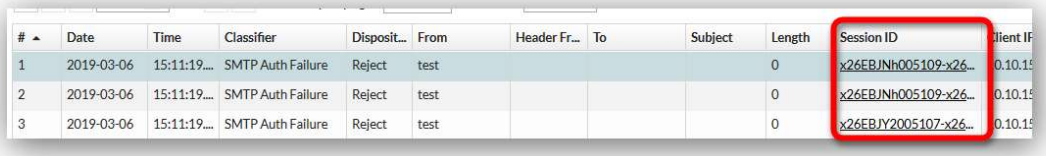


Przechodząc do logów *History* mamy informacje o połączeniach SMTP. Dwukrotnie klikając w dany log uzyskamy szczegółowe informacje na temat konkretnej sesji. Przykładowo:

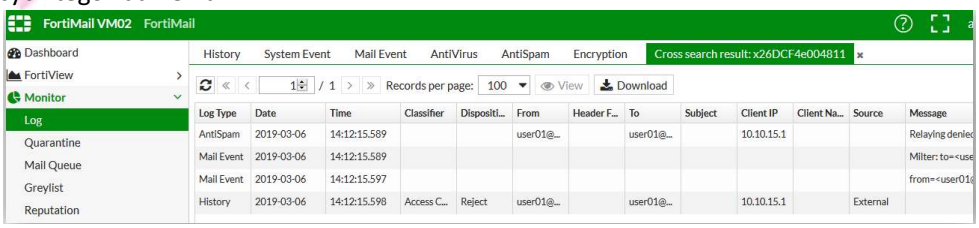


W logu mamy podstawowe informacje o dostarczeniu lub nie doręczeniu wiadomości, mamy informacje o adresach e-mail oraz IP nadawcy oraz odbiorcy. Jaki filtr sprawił, że dana wiadomość nie została dostarczona oraz które reguły zadziałały w danej sesji. Tak jak widzimy *Policy IDs* oznacza, że ta sesja wpadła w polityke domyślna Acces Control 0, następnie w politykę IP Policy 1, a następnie w politykę Recipient Policy 1.

W każdym logu mamy również informacje o Session ID z załączonym linkiem



Klikając w link uzyskamy szczegółowe informacje o sesji oraz o powiązaniach do innych logów dotyczących tego zdarzenia:



VI. Troubleshooting

Do rozwiązywania problemów z urządzeniem oczywiście podstawowymi informacjami będą zebrane logi.

Podczas procesu rozwiązywania problemów można zaoszczędzić czas i wysiłek, sprawdzając, czy inni użytkownicy FortiMail doświadczali podobnego problemu wcześniej. Poniżej kilka zasobów internetowych firmy Fortinet, które dostarczają cennych informacji na temat problemów technicznych z FortiMail.

- **Fortinet Document Library** znajdująca się pod adresem
  https://docs.fortinet.com/product/fortimail/6.0
  Na uwagę zasługują przede wszystkim:
  - FortiMail Admin Guides
  - Release Notes
- **Baza wiedzy** znajdująca się pod adresem
  https://kb.fortinet.com/kb/microsites/microsite.do
- **Forum techniczne** znajdujące się pod adresem
  https://forum.fortinet.com/

VII. Omówienie i konfiguracja profilu sesji

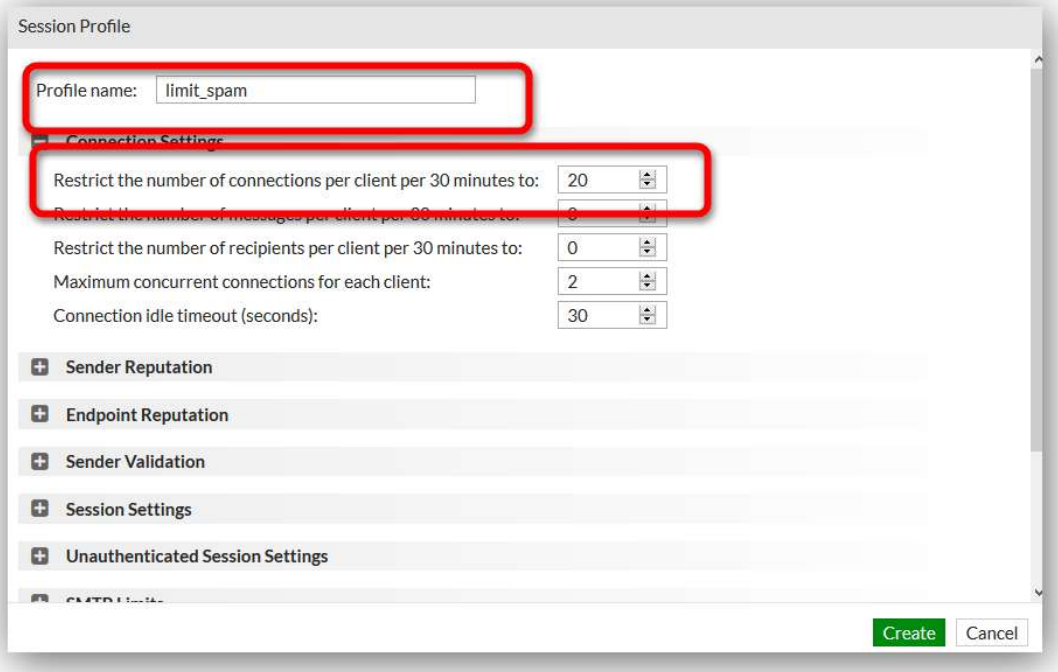
Profile sesyjne kontrolują ruch poczty elektronicznej na poziomie protokołu SMTP oraz działają poprzez analizowanie sesji SMTP, a nie jak w przypadku profili antyspamowych poprzez analizę nagłówka, treści lub załącznika.

Profil sesji jest wykorzystywany w politykach IP Policy na FortiMail w celu ograniczania ilości połączeń z naszym urządzeniem. W ćwiczeniu wykorzystamy serwer spamujący żeby sprawdzić jak FortiMail zachowuje się z różnymi opcjami.

1. Logujemy się do GUI na FortiMail w trybie Gateway (URL: *https://poczta.vfml.pl:XX443/admin/* **TABELA !!!**), przechodzimy do *Profile* > *Session*

2. Wybieramy *New* i konfigurujemy profil zgodnie z poniższymi ustawieniami:

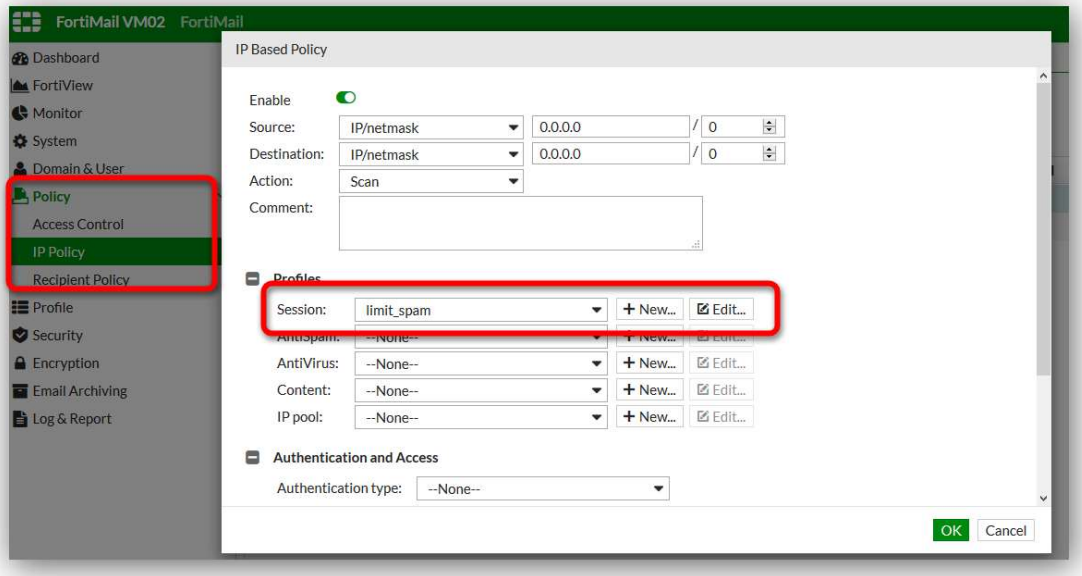
Profile name: limit_spam
Connection Settings: Restrict the number of connections per client per 30 minutes to: 20
Pozostałe parametry zostawiamy z ustawieniami domyślnymi, zatwierdzamy *Create*.



Obecne ustawienia oznaczają, że gdy od tego samego adresu IP zostanie osiągniętych 20 połączeń na 30 minut, FortiMail na kolejne próby połączenia odpowie *"Temporary Fail"*

3. Przechodzimy do *Policy* > *IP Policy* i edytujemy domyślna regułę ID 1 dla adresów 0.0.0.0/0.0.0.0).

Poniżej *Profiles*, wybieramy *limit_spam* dla profile *Session* pozostałe opcje bez zmian, zapisujemy poprzez *OK*.



4. W środowisku testowym skorzystamy z wirtualnej maszyny „malware-client" do wygenerowania i wysłania testowych wiadomości spamowych do skrzynki odbiorczej test@domena.int. Do generowania spamu korzystamy ze skryptu o nazwie *spamengine.pl*. Szczegóły dotyczące używania tego skryptu zostaną przedstawione w kolejnych krokach.

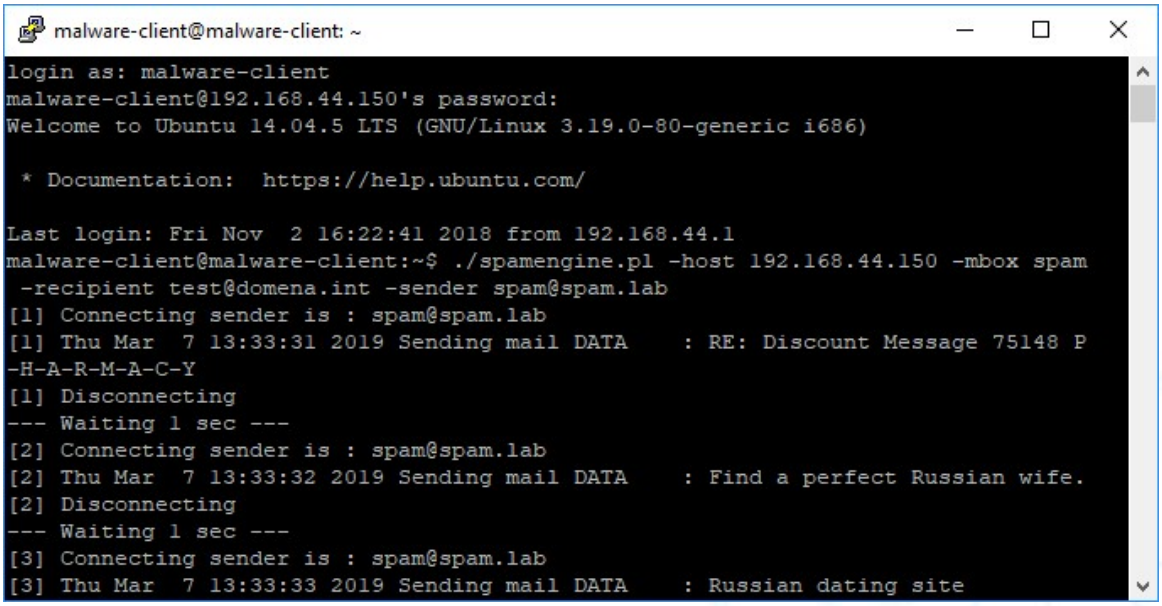
5. Korzystając z *putty.exe*, łączymy się za pomocą SSH z serwerem spamującym: *poczta.vfml.pl:15022*

6. Logujemy się użytkownikiem: *malware-client* oraz hasłem: *fortinet*

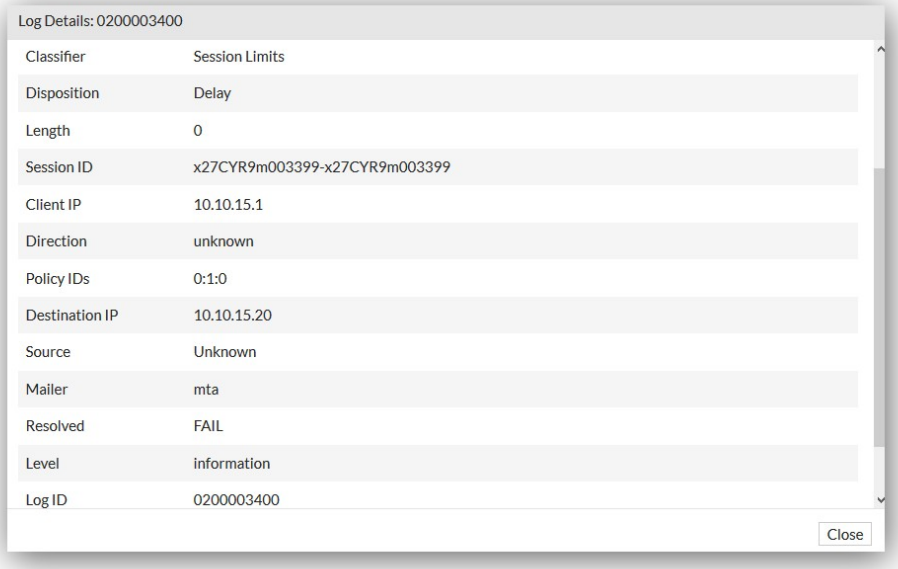
7. Uruchamiamy skrypt:

```
./spamengine.pl -host 192.168.44.150 -mbox spam -recipient test@domenaXX.int -sender spam@spam.lab
```

Ten test spowoduje wygenerowanie wystarczającej liczby wiadomości e-mail, aby osiągnąć limit sesji skonfigurowany powyżej w profilu sesji.



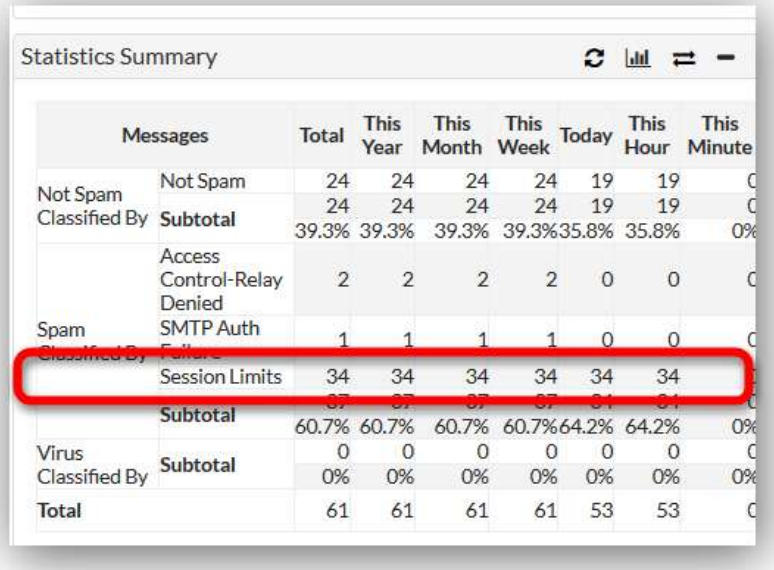
8. Czekamy chwilę, aż zostanie wysłane 20 e-maili, a następnie przechodzimy do *Monitor*> *Log* i sprawdzamy logi. Powinniśmy zaobserwować wpisy podobne do następującego.



Powyższy log informuje o powodzie niedostarczenia wiadomości: *Classifier Session Limits*.

Ponadto w logach można zaobserwować brak informacji o nadawcy, odbiorcy I temacie. Dzieje się tak, ponieważ sesja SMTP została odrzucona na poziomie IP przed przystąpieniem do analizy wiadomości.

9. Przechodząc do *Dashboard* > *Status*, możemy sprawdzić statystyki, oraz ilość wiadomości, które zostały zaklasyfikowane przez Limit sesji.



Statistics Summary

Messages		Total	This Year	This Month	This Week	Today	This Hour	This Minute
Not Spam Classified By	Not Spam	24	24	24	24	19	19	0
	Subtotal	24 39.3%	24 39.3%	24 39.3%	24 39.3%	19 35.8%	19 35.8%	0 0%
Spam Classified By	Access Control-Relay Denied	2	2	2	2	0	0	0
	SMTP Auth Failure	1	1	1	1	0	0	0
	Session Limits	34	34	34	34	34	34	0
	Subtotal	37 60.7%	37 60.7%	37 60.7%	37 60.7%	34 64.2%	34 64.2%	0 0%
Virus Classified By	**Subtotal**	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%
Total		61	61	61	61	53	53	0

10. Aby zatrzymać skrypt korzystamy ze skrótu (CTRL + C), a następnie możemy ponownie go uruchomić

Opcjonalnie możemy wykorzystać manipulacje nagłówka w profilu sesyjnym.

VIII. Profile antyspamowe dla ruchu przychodzącego

W tym ćwiczeniu utworzymy i przetestujemy profil antyspamowy dla poczty przychodzącej na urządzeniu FortiMail w trybie gateway. Każdy profil antyspamowy jest skojarzony z profilem akcji. Zanim utworzymy profil antyspamowy, najpierw musimy utworzyć profil akcji.

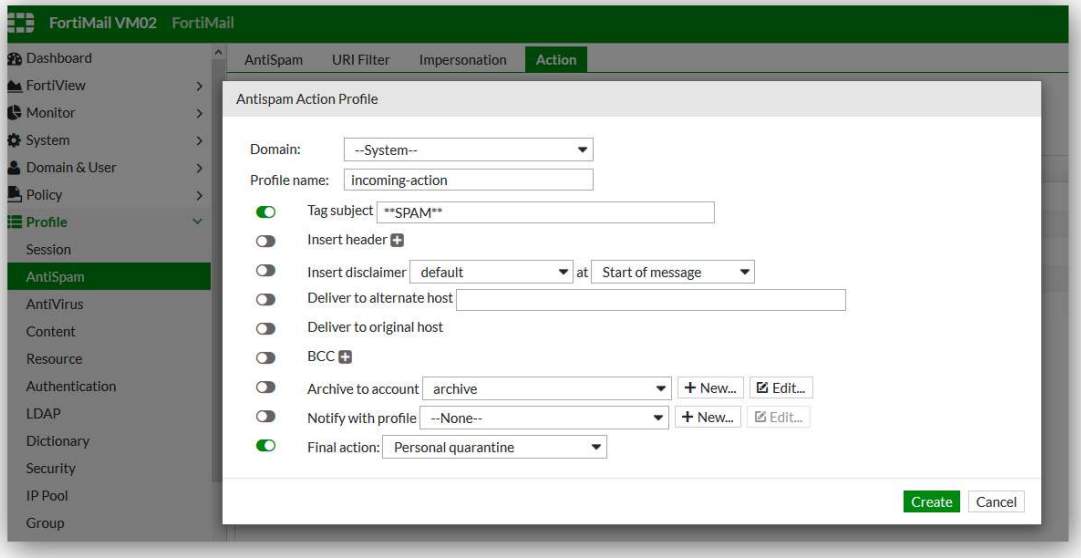
1. Logujemy się na FortiMail w trybie gateway URL: *https://poczta.vfml.pl:XX443/admin/* **TABELA !!!**

2. przechodzimy do *Profile* > *AntiSpam* > *Action*.

Wybieramy *New* i konfigurujemy profil akcji zgodnie z poniższymi ustawieniami:

Domain: --System--
Profile name: incoming-action
Tag email's subject line: **SPAM**
Final action: Personal quarantine

Pozostałe parametry zostawiamy bez zmian.

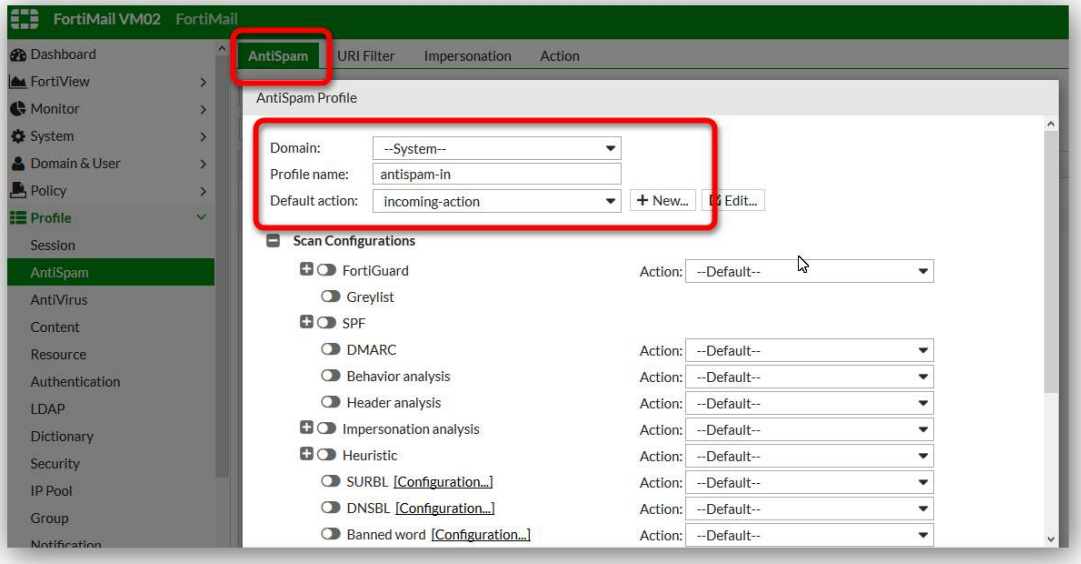


3. Następnie tworzymy nowy profil antyspamowy. Przechodzimy do *Profile* > *Antispam* > *Antispam* i klikamy *New*.

Konfigurujemy poniższe wartości:

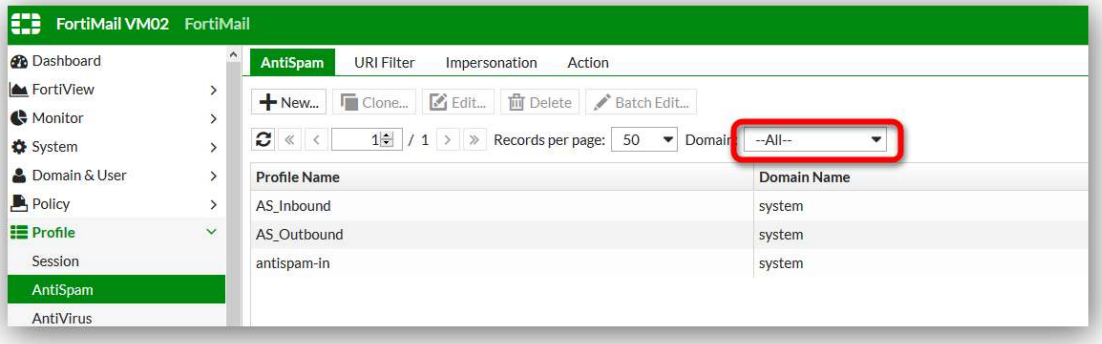
Domain: --System--
Profile name: antispam-in
Default Action: incoming-action

Zatwierdzamy: *Create*.



W kolejnych krokach będziemy uruchamiać różne opcje filtrowania spamu, a następnie uruchomimy test spamu. Po każdym teście będziemy sprawdzać skrzynkę pocztową, aby zweryfikować, ile wiadomości zostało zablokowanych. Każdy wykryty spam zostanie oznaczony i trzymany w kwarantannie.

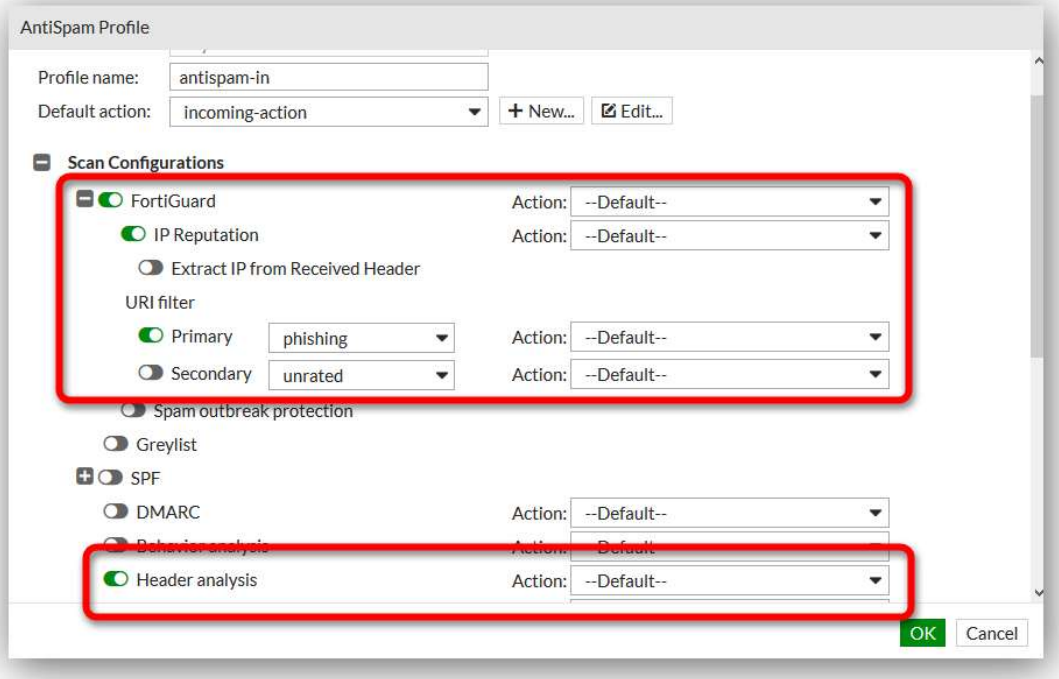
4. Przechodzimy do *Profile* > *Antispam* > *Antispam* i wybieramy –All—z listy dostępnych domen.



5. Edytujemy profil *antispam-in* włączając poniższe opcje:

- FortiGuard oraz IP Reputation
- URI filter :phishing
- Headers analysis
- Opcjonalnie można zaznaczyć zewnętrzne bazy SURBL (Spam URL Realtime Block List) lub/oraz DNSBL (Domain Name System block list). np:
    - multi.surbl.org
    - bl.spamcop.net
    - zen.spamhaus.org

Aby zatwierdzić ustawienia klikamy *OK*.



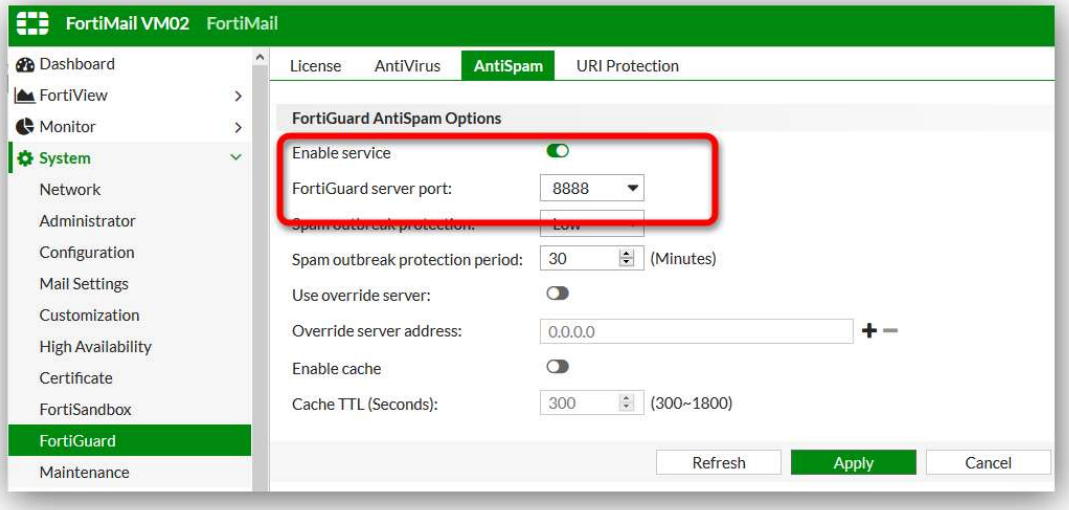
6. Przechodzimy do *System > FortiGuard > AntiSpam* konfigurujemy poniższe ustawienia.

Enable service: enable

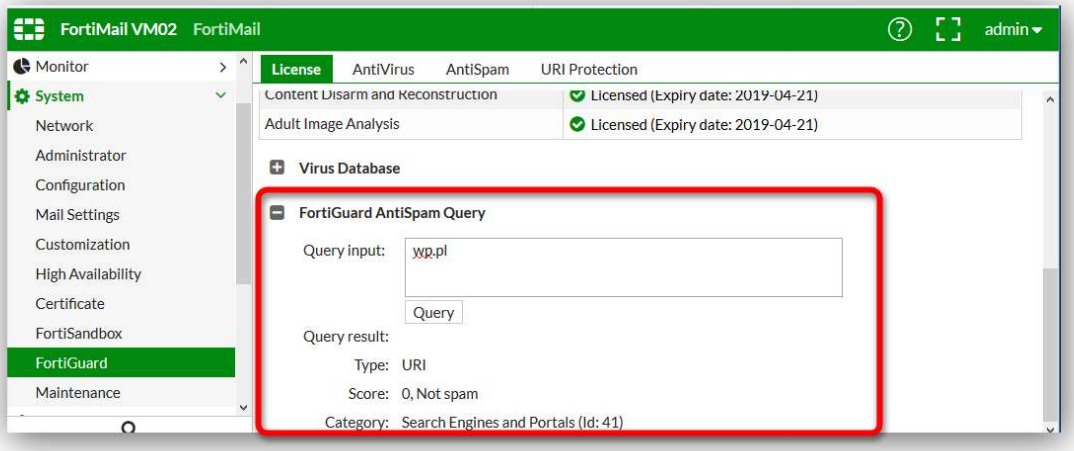
FortiGuard server port: 8888

Zmiany zatwierdzamy Apply.

Ustawienie to zmienia port, którym FortiMail łączy się z siecią FortiGuard, Często pozwala to na połączenie się z siecią FortiGuard w przypadku, kiedy operator blokuje niskie porty.



7. Aby przetestować połączenie z FortiGuard, przechodzimy do zakładki License i w sekcji *FortiGuard AntiSpam Query*, wprowadzamy adres w polu Query. Klikamy przycisk Query, poniżej przykładowy wynik:



8. Następnie przechodzimy do *System* > *FortiGuard* > *AntiVirus* i konfigurujemy opcje aktualizowania:

Allow push update: enable
Scheduled update: every 2 hours
Zatwierdzamy poprzez *Apply* oraz klikamy *Update Now*.

9. Teraz musimy aktywować profil antyspamowy, w regułach przychodzących. Przechodzimy do *Policy* > *Recipient Policies* wybieramy *New* i konfigurujemy poniższe ustawienia:

Sender Pattern: *@*
Recipient Pattern: *@domenaXX.int **TABELA !!!**
Profiles AntiSpam: antispam-in
Pozostałe opcje pozostawiamy z ustawieniami domyślnymi.

W naszym środowisku testowym pod adresem `poczta.vfml.pl 16022` znajduje się wirtualna maszyna, z której w celu wygenerowania i wysłania testowych wiadomości spamowych do skrzynki odbiorczej **test@domenaXX.int.** Do generowania spamu korzystamy ze skryptu o nazwie *spamengine.pl*. Szczegóły dotyczące używania tego skryptu zostaną przedstawione w kolejnych krokach.

10. Korzystając z *putty.exe* łączymy się za pomocą SSH z serwerem spamującym: `poczta.vfml.pl 15022`

Logujemy się użytkownikiem: ***malware-client*** oraz hasłem: ***fortinet***

11. Uruchamiamy poniższy skrypt

```
./spamengine.pl -host 192.168.44.150 -mbox spam -recipient test@domena.int -sender spam@spam.lab
```

Aby przerwać wykonywanie skryptu korzystamy ze skrótu Ctrl+C

12. Sprawdzamy skrzynkę odbiorczą logując sie do webmaila:

Adres: URL: *https://poczta.vfml.pl:XX443/* **TABELA !!!**
Użytkownik ***test***
hasło ***test***
Na tym etapie część wiadomości spamowych może zostać dostarczona.

Spróbujmy dostosować profil antispam-in korzystając z różnych technik wykrywania spamu takich jak heurystyka oraz wykrywanie spamu w obrazach.

13. Logujemu sie do GUI na FortiMail w trybie gateway (URL: *https://poczta.vfml.pl:XX443/admin/* **TABELA !!!**

14. przechodzimy do *Dashboard* widżet *Statistics summary*

Tutaj możemy zapoznać się z informacjami na temat całkowitej liczby otrzymanych wiadomości e-mail, odsetkiem spamu i rodzajami technik antyspamowych wykorzystywanych do wykrywania większości spamu.

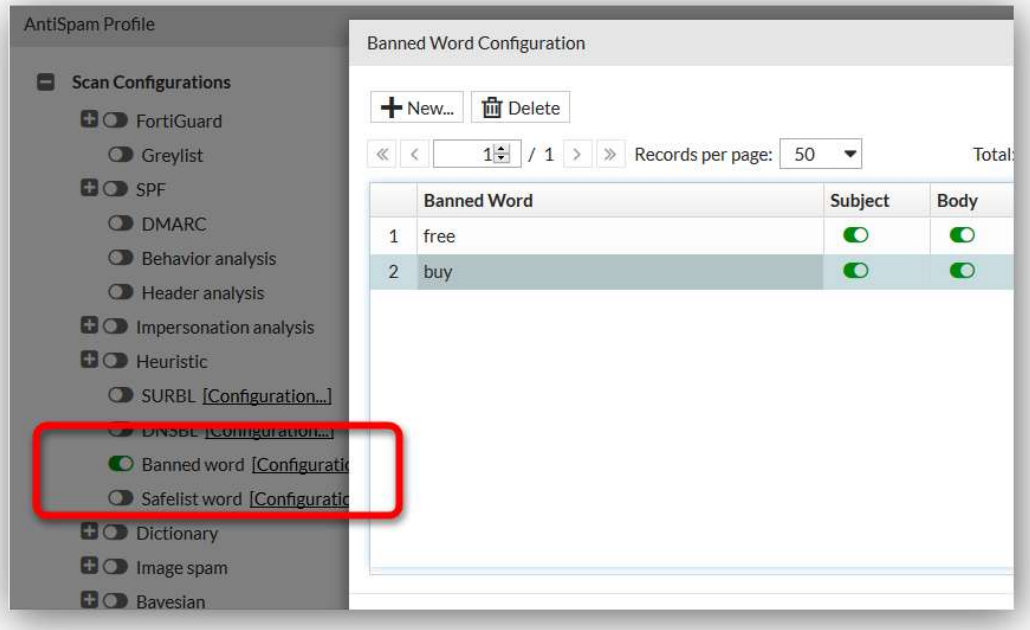
IX. Antyspam dla ruchu wychodzącego

W tym ćwiczeniu skonfigurujemy profil antyspamowy dla poczty wychodzącej, aby filtrować wychodzące wiadomości e-mail.

1. Logujemy się do GUI na FortiMail w trybie gateway (URL: https://poczta.vfml.pl:XX443/admin/ **TABELA !!!**), przechodzimy do *Profile* > *Antispam* > *Antispam* i klikamy *New*.

Konfigurujemy poniższe wartości:
Domain: --System--
Profile name antispam-out
Default action: SystemQuarantine

2. Włączamy *Banned word* klikamy *Configuration.* Dodajemy kilka słów do listy. Po wpisaniu słowa możemy wybrać gdzie w wiadomości może znajdować się słowo w treści lub w temacie:

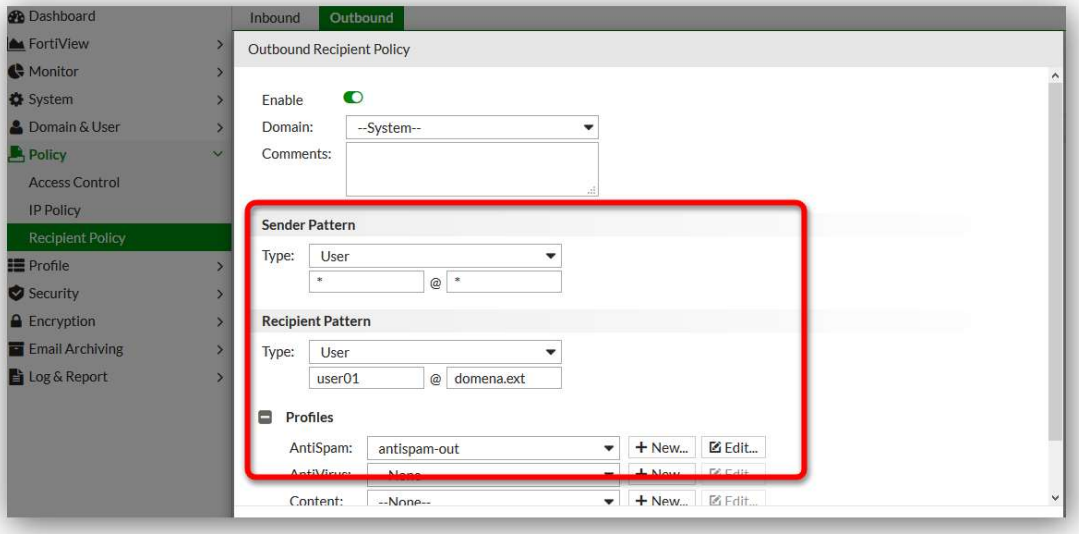


Wybieramy *OK* aby zamknąć konfiguracje *Banned Word* oraz zatwierdzamy poprzez Create aby zapisać profil.

3. Teraz, gdy mamy utworzony profil antyspamowy dla poczty wychodzącej, musimy go aktywować dodając go do polityki *Recipient Policies* w kierunku *Outgoing*

Przechodzimy do *Policy* > *Recipient Policies* wybieramy zakładkę *Outbound* wybieramy *New* konfigurujemy nową politykę jak poniżej:

Sender: *@*
Recipient: userXX@domena.ext **TABELA!!!**
Profiles AntiSpam: antispam-out
Pozostałe parametry zostawiamy z ustawieniami domyślnymi, zatwierdzamy *Create*.



4. Wysyłamy wiadomość pocztowa logując się do webmaila:

Użytkownik ***test*** hasło ***test***

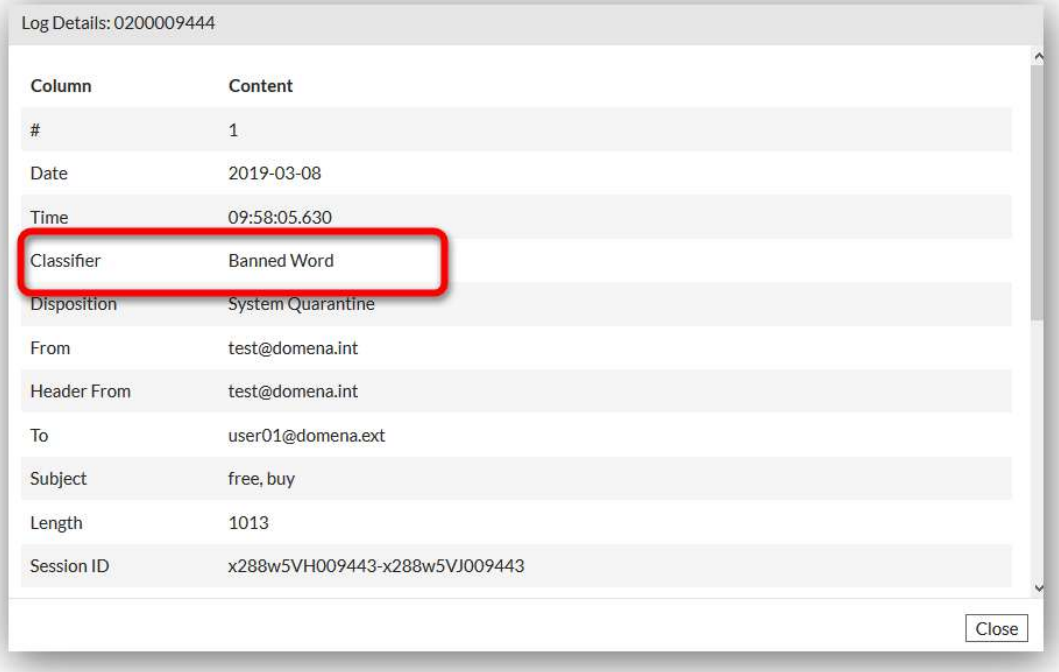
5. URL: *https://poczta.vfml.pl:XX443/admin/* **TABELA !!!**

6. Wysyłamy wiadomość na adres *userXX@domena.ext* korzystając z zabronionych słów *free, buy*

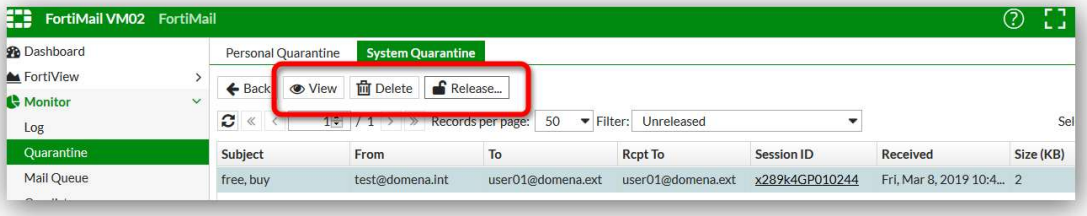
Wiadomość powinna zostać zablokowana przez FML w trybie gateway.

7. Logując się do GUI na *Gateway* FortiMail (URL: https://poczta.vfml.pl:XX443/admin/ **TABELA !!!**

8. przechodzimy do *Monitor* > *Log* przeglądamy logi *Event, Mail Event* oraz *AntiSpam*.



9. Zablokowaną wiadomość możemy znaleźć w systemowej kwarantannie, przechodzimy do zakładki: *Monitor* → *Quarantine* → *System Quarantine*, gdzie możemy wspomnianą wiadomość odczytać, usunąć lub przesłać dalej.



Relay host

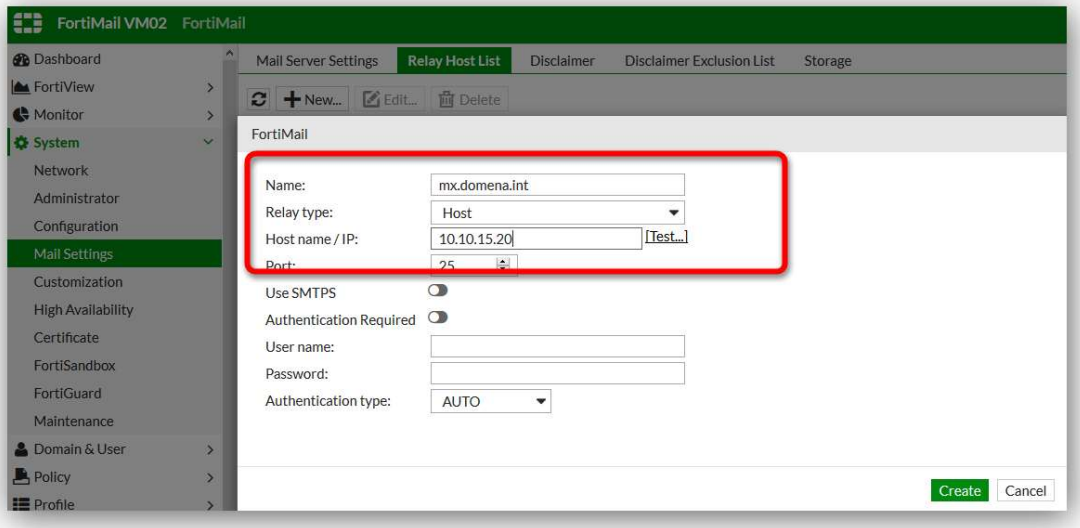
Jeśli nie udało nam się uzyskać spodziewanego efektu w poprzednim ćwiczeniu a wiadomość do user01@domena.ext została dostarczona, należy sprawdzić czy mamy prawidłowo skonfigurowany relay host na serwerze mail. Robimy to w następujący sposób:

1. Logujemy się na serwerze mail (URL: *https://poczta.vfml.pl:XX443/* **TABELA !!!**

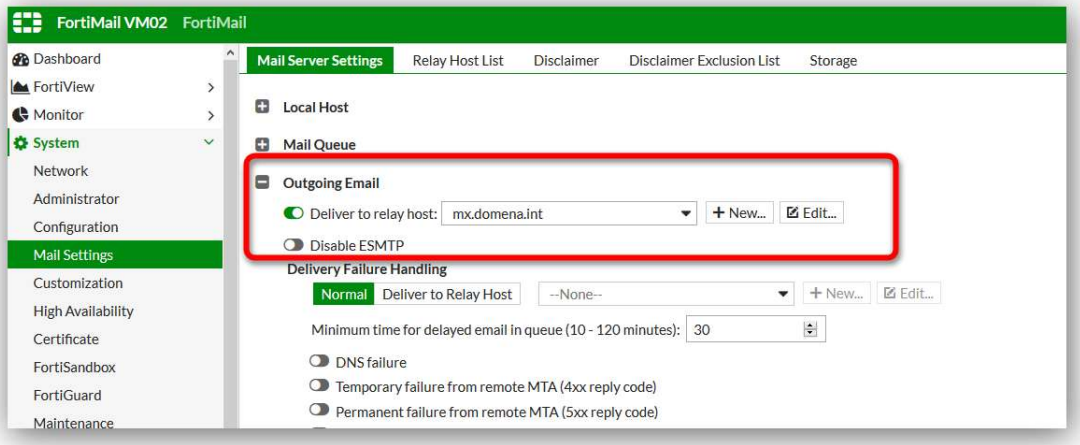
2. Przechodzimy do zakładki *system → mail Settings → relay host list* i klikamy *new*

3. Podajemy:

name: mx.domena.int
Host name / IP: Loklany adres IP FML-GW !!!



4. Przechodzimy do zakładki *System → mail settings → Mail Server Settings* i w części *Outgoing Email* włączamy *Deliver to relay host.* Z listy rozwijanej wybieramy wcześniej utworzony relay host.



X. Profile antywirusowe

FortiMail korzysta z usługi antywirusowej w oparciu o licencje FortiGuard, oraz niektóre wbudowane technik antywirusowe w celu zwalczania wirusów, które są przesyłane z ruchem SMTP, dodatkowo może korzystać usługi antywirusowej FortiSandbox

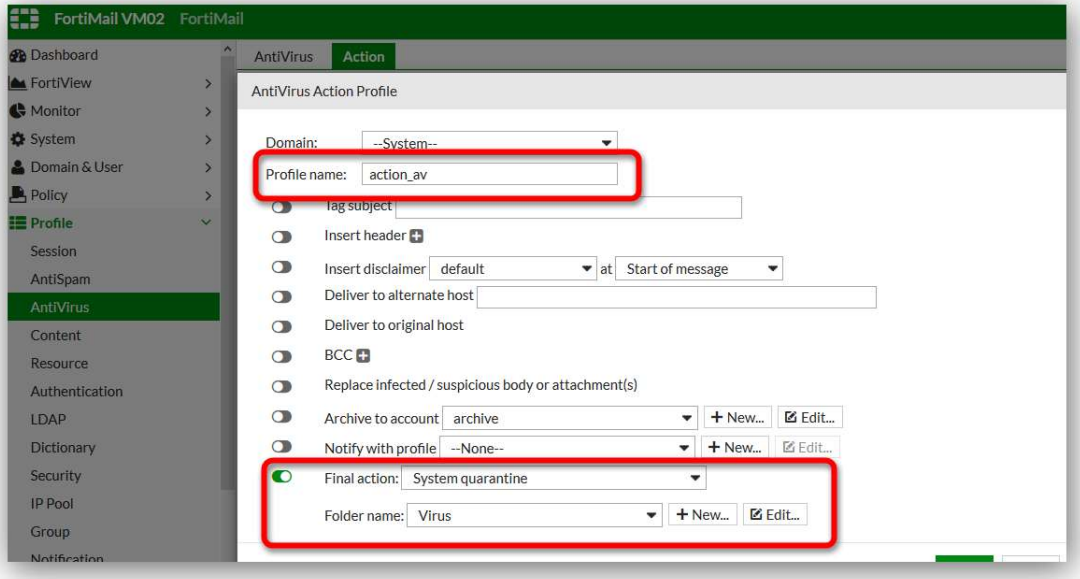
1. Logujemy się do GUI na FortiMail w trybie gateway (URL: *https://poczta.vfml.pl:XX443/admin/* **TABELA !!!**

2. przechodzimy do *Profile > AntiVirus* zakładka *Action* i klikamy *New*.

3. Zanim utworzymy profil antywirusowy, musimy najpierw utworzyć profil akcji. Konfigurujemy profil zgodnie z poniższym:

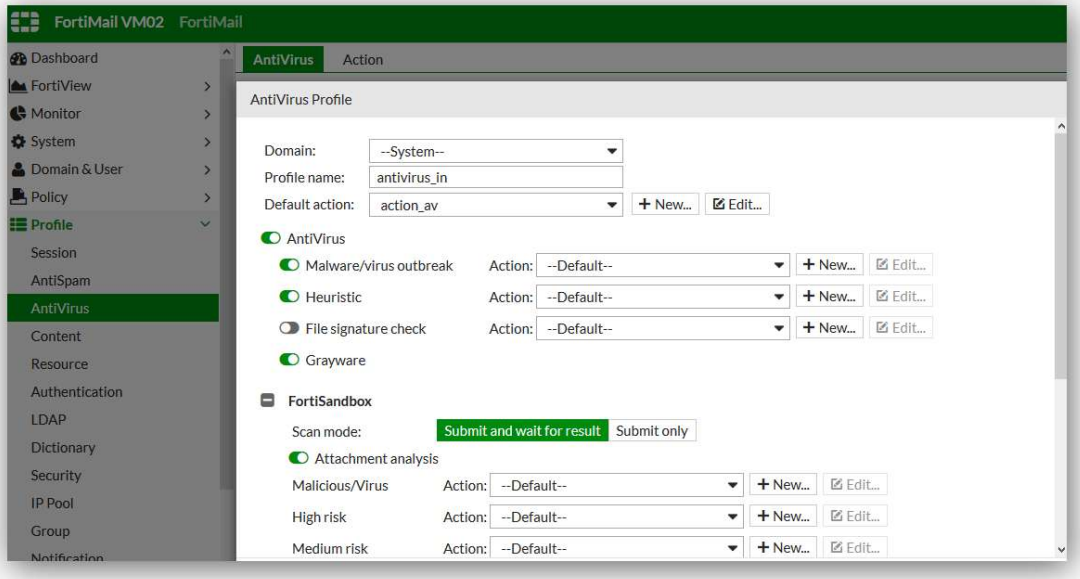
Profile name: action_av

Final action: System quarantine
Folder name: Virus

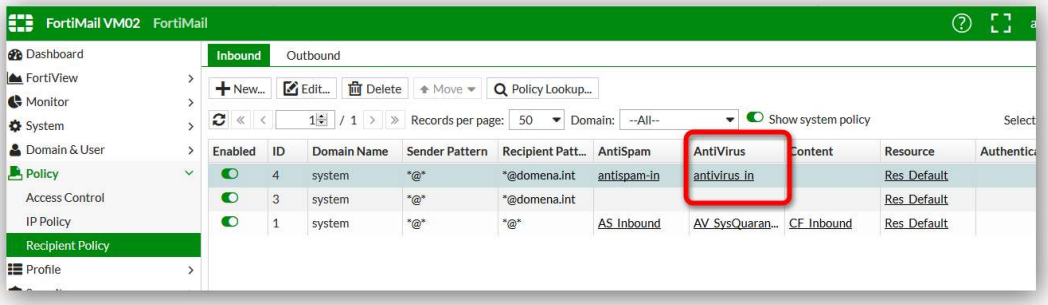


4. Następnie konfigurujemy nowy profil antywirusowy w zakładce (*System -> Antivirus ->Antivirus)* zgodnie z poniższą tabelą:

Profile name	Antivirus_in
Default action	Action_av
Fortisandbox → Attachment analysis	Włączamy
Fortisandbox → URI analysis	Włączamy
Pozostałe opcje	Wartości domyślne



5. Przechodzimy do zakładki *Policy → Recipient Policy → zakładka Inbound i* Utworzony profil podpinamy do naszej polityki

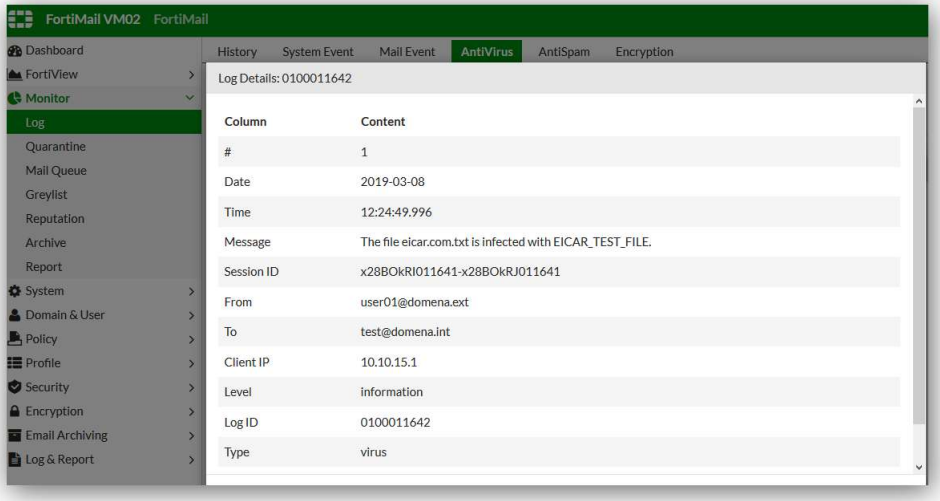


6. Wykonujemy test z próbą przesłania pliku, który powinien zostać zablokowany. W tym celu możemy skorzystać z wirtualnej maszyny „malware-client”

http://poczta.vfml.pl:16022/squirrelmail/src/login.php

Logujemy się za pomocą użytkownika ***userXX*** oraz hasłem ***fortinet***

7. Weryfikujemy logi na urządzeniu przechodząc do *Monitor>Log* zakładka *AntiVirus.* Powinniśmy otrzymać log podobny do poniższego.



UWAGA: najczęstszymi problemami w prawidłowym teście tego ćwiczenia są:

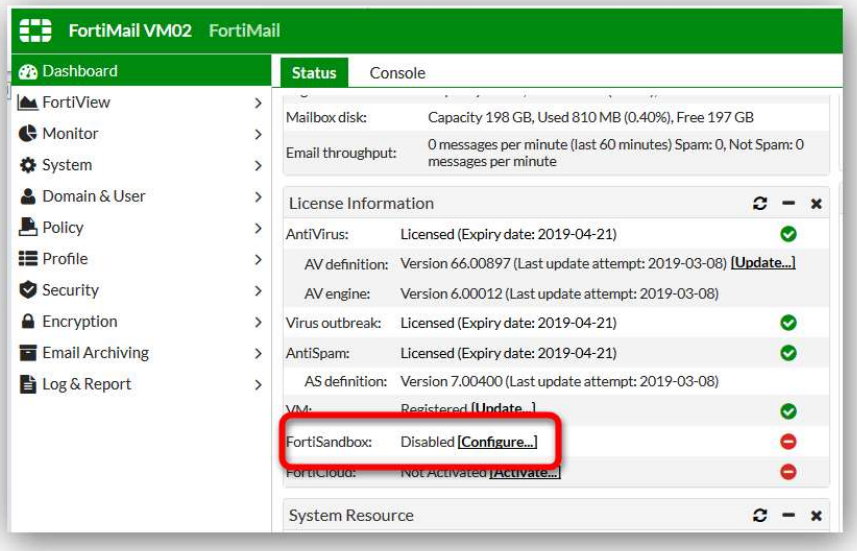
- Osiągnięty limit połączeń w ciągu 30 minut (konfigurowaliśmy to w rozdziale: Omówienie i konfiguracja profilu sesji)
- Włączony Profil sesyjny na serwerze (wyłączany w rozdziale: Konfiguracja chronionej domeny)

Omówienie oraz konfiguracja Integracji z Sandbox

FortiMail może współpracować z zewnętrznym rozwiązaniem FortiSandbox w celu eliminacji nieznanych dotąd zagrożeń. Może być do dedykowane urządzenie w postaci platformy lub wirtualnej maszyny, może być to również jako dodatkowa licencja na usługę w chmurze.

Aby skonfigurować Sandbox na FortiMailu postępujemy zgodnie z poniższą instrukcją.

1. Logujemy się do GUI na FortiMail w trybie gateway (URL: https://poczta.vfml.pl:XX443/admin/ **TABELA !!!**), przechodzimy do *Dashboard > Status, w sekcji License Information* wybieramy *Configure* przy FortiSandbox

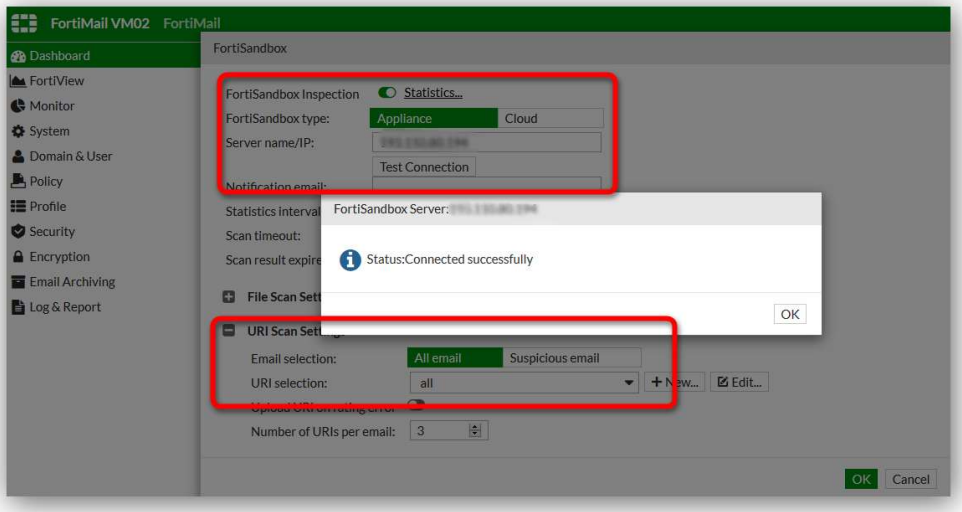


2. Zaznaczamy

FortiSandbox Inspection: włączony
FortiSandbox type: Appliance
Server name/IP: adres platformy podany przez prowadzącego
URI Scan Settings:
Email selection All email
URl selection All

3. Następnie możemy przeprowadzić test połączenia klikając w *Test Connection*

Powinniśmy otrzymać poniższy komunikat:



Zatwierdzamy poprzez *OK*

Należy pamiętać, że jeśli jest to nowe urządzenie to musi zostać ono aktywowane na samym FortiSandbox'ie.

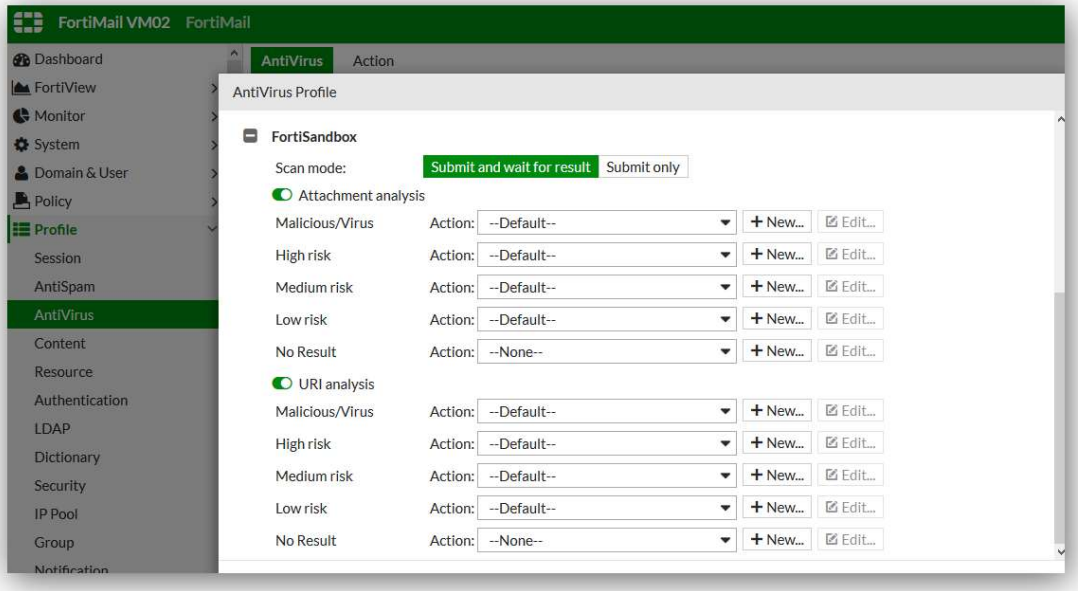
Następnie przechodzimy do naszego profilu antywirusowego (zakładka *Profile → AntiVirus)* *zaznaczamy profil antivirus_in* i klikamy *Edit.*

4. W części FortiSanbox zaznaczamy:

Scan mode: Submit and wait for result

Attachment analysis: włączone

URl analysis: włączone



5. W chwili obecnej nasze urządzenie będzie przesyłało nieznane dotąd zagrożenia do FortiSandbox'a w celu analizy.

XI. Profile kontroli treści

Za pomocą *Content* profili możemy tworzyć profile treści, których można używać w zależności od dopasowywania wiadomości w oparciu o jego temat, treść wiadomości i załączniki. W przeciwieństwie do profili antyspamowych, które dotyczą przede wszystkim spamu, profile zawartości odpowiadają innym typów wiadomości.

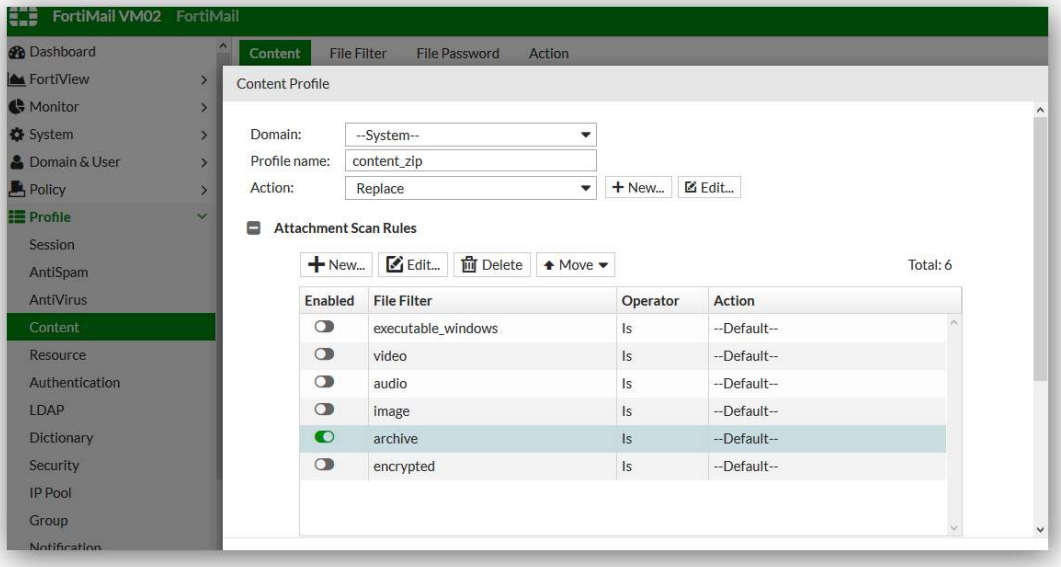
Content profili można używać do szyfrowania lub blokowania opartego na zawartości wiadomości e-mail. Profile te działają w oparciu o: słowa, frazy, nazwy plików i załączniki, które są przesyłane pocztą e-mail z niestandardowymi treściami.

Aby skonfigurować profil na FortiMailu, który będzie usuwał pliki spakowane, należy skonfigurować urządzenie zgodnie z instrukcją:

1. Logujemy się do GUI na FortiMail w trybie gateway (URL: *https://poczta.vfml.pl:XX443/admin/* **TABELA !!!**), przechodzimy do *Profile* > *Content* zakładka *Content* wybieramy *New*

2. Konfigurujemy nowy profil zgodnie z poniższym:

Domain: --System—
Action: replace
Attachment Scan Rules: włączamy *Archive*
Pozostałe wartości zostawiamy domyślnie

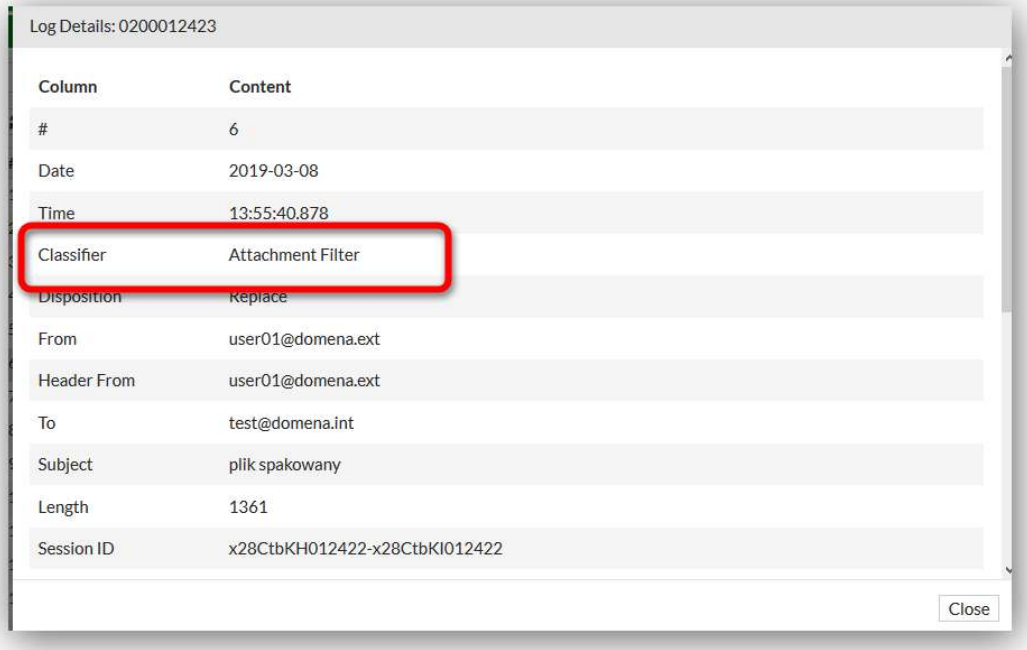


Zatwierdzamy poprzez *Create*

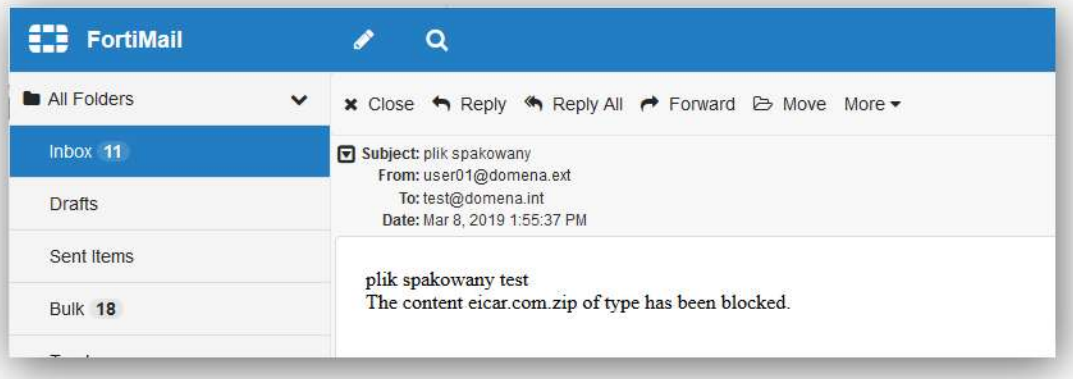
3. Utworzony profil podpinamy do polityki Recipient Policies: (Policy → Recipient Policy)

4. Wykonujemy test z próbą przesłania pliku *.zip, który powinien zostać zablokowany. W tym celu możemy skorzystać z wirtualnej maszyny „malware-client”

5. W logach powinniśmy otrzymać informację.



6. Odbiorca powinien otrzymać poniższą wiadomość?



UWAGA:, Jeśli chcemy zmienić wiadomość, którą zastępujemy spakowany plik, możemy to zrobić w *System →Customization → Custom Message*

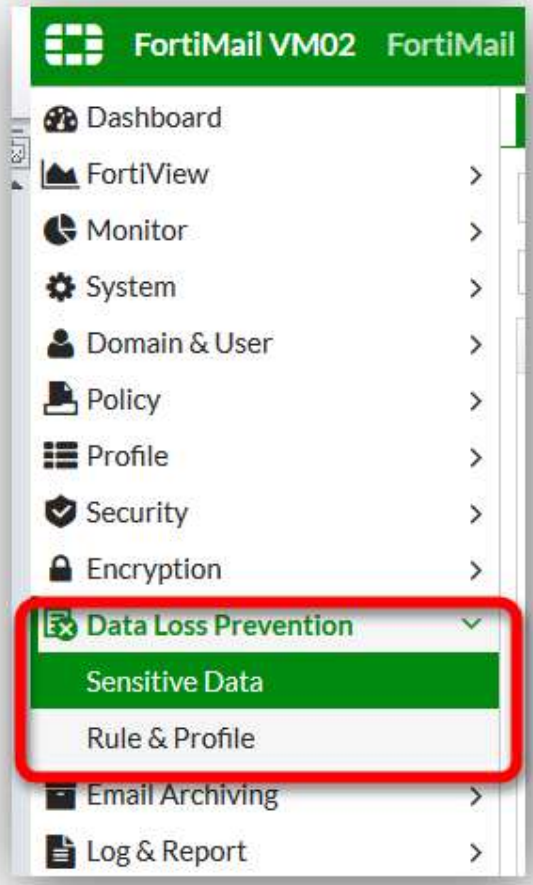
XII. DLP

System zapobiegania wyciekom danych w systemie FortiMail (DLP) pozwala zapobiec przesłaniu poufnych danych przez wiadomości pocztowe. Po zdefiniowaniu profili można podejmować działania przeciwko wiadomościom zawierającym dane pasujące do tych wzorców.

Domyślnie urządzenie ma wyłączoną funkcjonalność DLP, alby ją uruchomić musimy zalogować się poprzez SSH na naszym FortiMailem w trybie gatewaya i skorzystać z poniższych komend:

```
# config system global
(global) # set data-loss-prevention enable
(global) # end
```

W chwili obecnej powinniśmy mieć dostęp do DLP z GUI



W naszym teście zablokujemy możliwość przesyłania w wiadomościach nr PESEL

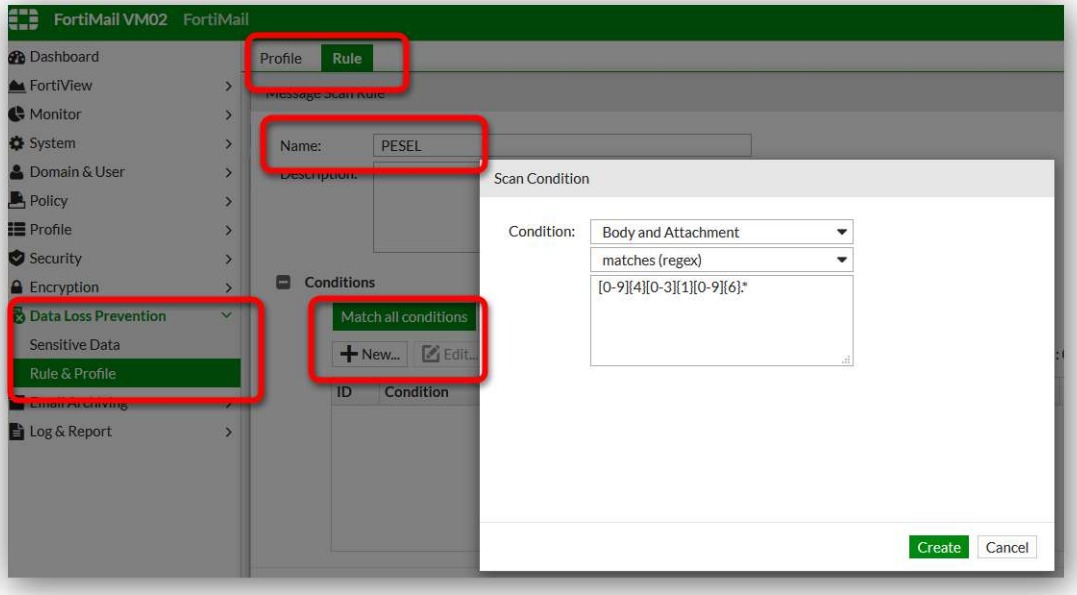
1. Logujemy się do GUI na FortiMail w trybie gateway (URL: https://poczta.vfml.pl:XX443/admin/ **TABELA !!!**

2. , przechodzimy do *Data Loss Prevention* > *Rule and Profile* zakładka *Rule* wybieramy *New*

W polu *name* wpisujemy PESEL oraz poniżej w *Conditions* przy zaznaczonej opcji

Match all conditions ponownie wybieramy New

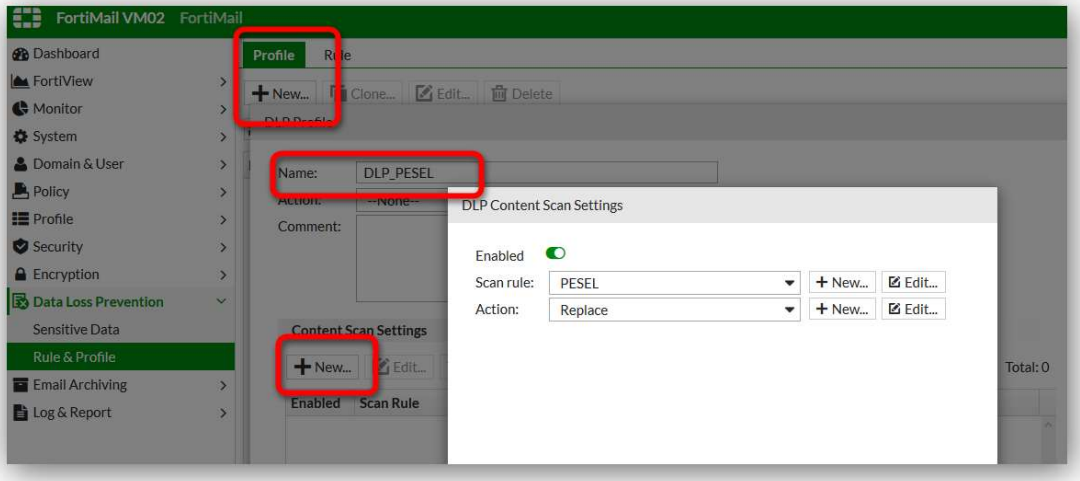
3. Kreujemy *Scan Condition* zgodnie z przykładam [0-9]{4}[0-3]{1}[0-9]{6}.* (jest to tylko przykład pokazujący możliwość wykorzystania wyrażeń regularnych)



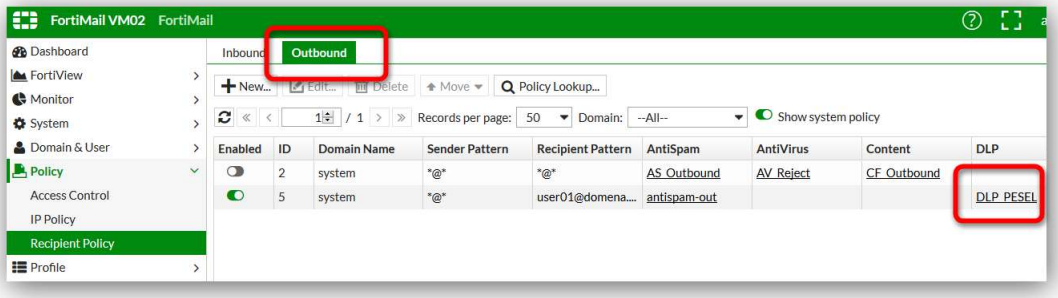
Zatwierdzamy *Scan Condition* poprzez przycisk *Create* a następnie poprzez *Create* zapisujemy regułę.

4. Następnie przechodzimy do zakładki *profile* Wybieramy New i Konfigurujemy profil zgodnie z przykładem:

Name: DLP_PESEL
Content Scan Settings → New
w *DLP Content Scan* Settings ustawiamy:
Scan Rule: PESEL
Action: Replace

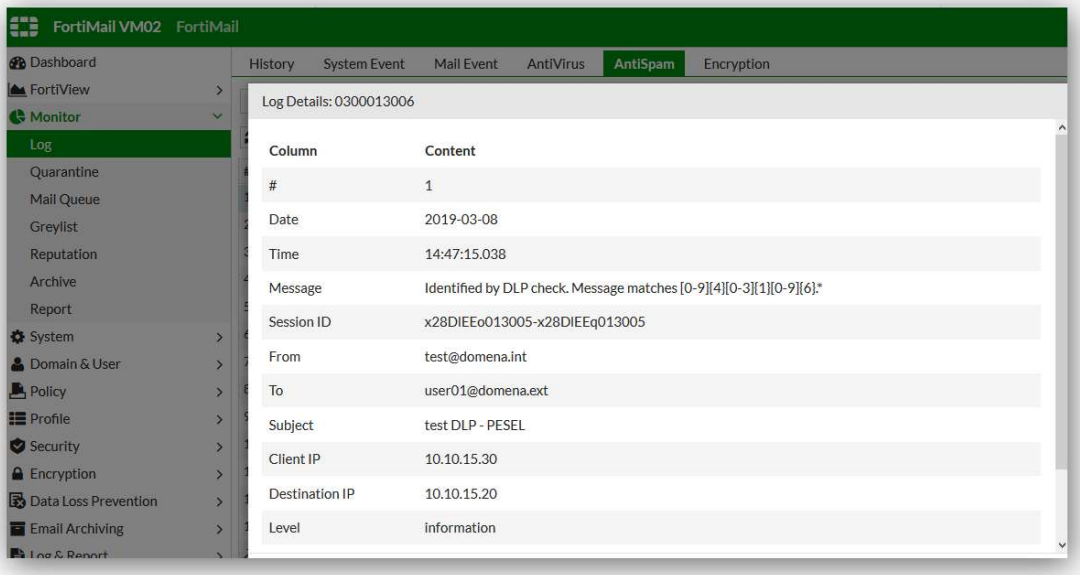


5. Ostatnim krokiem jest przypisanie profilu DLP do polityki Recipient Policy tylko tym razem w kierunku *Outbound*



6. Przeprowadzamy test próbując przesłać wiadomość do użytkownika *userXX@domena.ext*. W tym celu logujemy się do webmaila poprzez (https://poczta.vfml.pl:XX443/admin/ TABELA!!!, Login: `test`, hasło: `test`

7. Następnie logujemy się do FML w trybie Gateway i sprawdzamy logi czy poprawny filtr zadziałał do zablokowania wiadomości zawierające nr PESEL.



8. W jaki inny sposób moglibyśmy zablokować nr PESEL?

XIII. White/Black listy

Na FortiMail mamy możliwość skonfigurowania *Block/Safe List*, dla których można przypisać akcje umożliwiającą odrzucenie lub zezwolenie przesłania wiadomości na podstawie adresów e-mail, nazw domen i adresów IP.

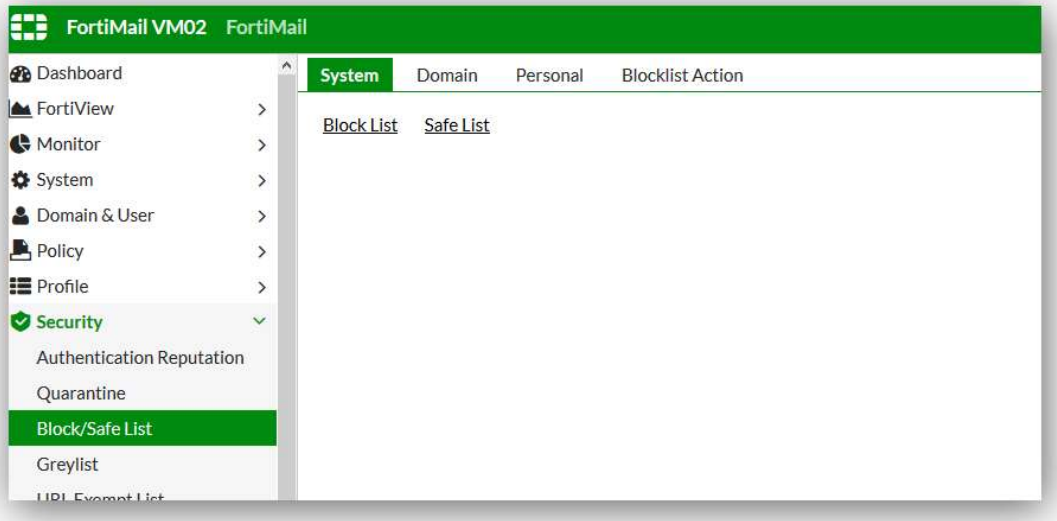
Dostępne są różne typy *Block/Safe List*: systemowe, domenowe, użytkownika oraz sesyjne. W interfejsie znajduje się kilka miejsc, w których można skonfigurować wspomniane listy

Jednym z pierwszych kroków w celu wykrycia spamu jest sprawdzenie tych właśnie list.

Ogólnie rzecz biorąc, safe listy mają pierwszeństwo przed black listami. Jeśli na obu listach pojawi się ten sam wpis, wpis zostanie uznany za bezpieczny. Podobnie listy systemowe mają pierwszeństwo przed listami domenowymi, natomiast listy domenowe mają pierwszeństwo przed listami użytkowników.

Jeśli FortiMail znajdzie dopasowanie na którejś z ww list nie szuka już dodatkowych wpisów dla tej wiadomości i nie stosuje profili antyspamowych (skanowanie antywirusowe oraz zawartości nadal jest aktywne).

Podstawowym miejscem gdzie możemy konfigurować *Block/Safe List* to zakładka *Security > Block/Safe List* następnie zgodnie z zakładkami konfigurujemy listy per system, per domena, per user oraz domyślną akcję dla *Blocklist*



XIV. Filtry Bayesa

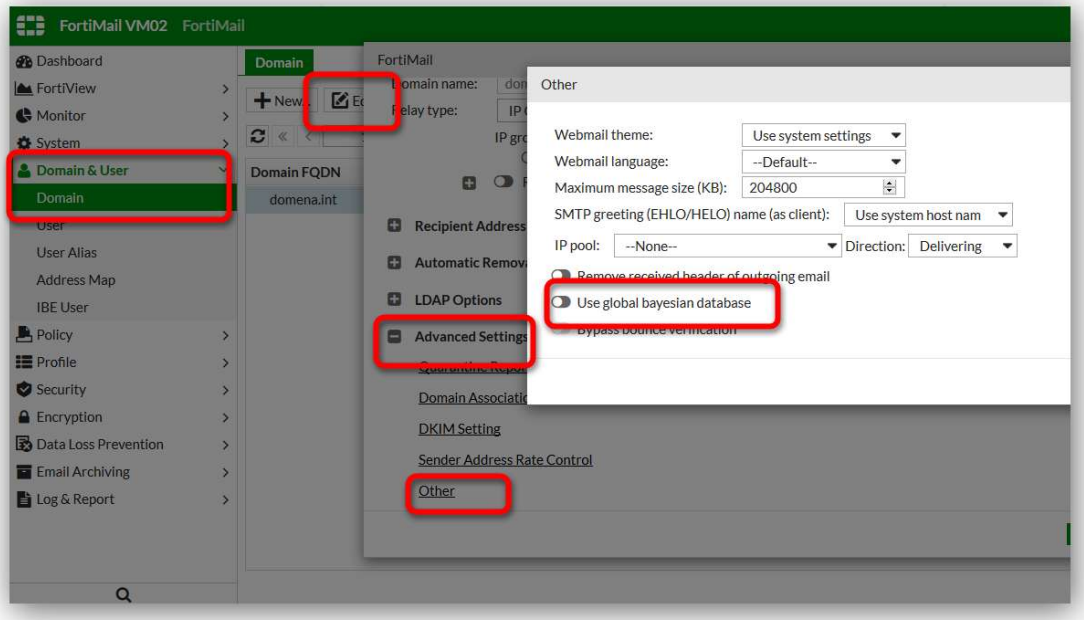
Filtrowanie spamu metodą Bayesa jest skuteczną formą filtrowania poczty e-mail stosowaną przez FortiMail w celu walki ze spamem. Metoda ta umożliwia identyfikację niepożądanej poczty e-mail z dużym stopniem dokładności.

Jego działanie opiera się na następującej zasadzie: W pierwszej fazie odbywa się proces uczenia. Użytkownik ręcznie oznacza wystarczającą liczbę wiadomości e-mail, jako wiarygodną pocztę lub jako spam. Filtr analizuje każdą kategorię i na podstawie trendów dotyczących wiadomości tworzy reguły filtrowania. Po przetworzeniu wystarczającej liczby wiadomości filtr Bayesa może przypisać każdej wiadomości odpowiednią wartość „wskaźnika spamu" i określić, czy kwalifikuje się ona jako spam.

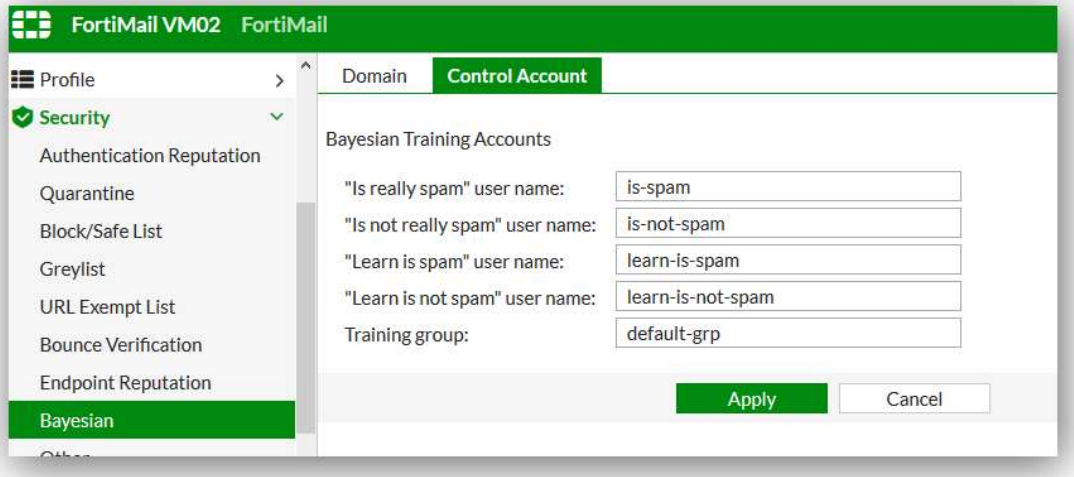
Aby zachować skuteczność, należy ciągle aktualizować bazę zarówno pod względem wiadomości pozytywnych jak i negatywnych. Na urządzeniu mamy dwa typy filtrów Bayesa: systemowe oraz domenowe.

Aby umożliwić korzystanie z baz Bayesian musimy skonfigurować urządzenie dla każdej chronionej domeny:

1. Logujemy się do GUI na FortiMail w trybie gateway (https://poczta.vfml.pl:XX443/admin/ **TABELA!!!**
2. Przechodzimy do Domain&User > Domain
3. Wybieramy naszą chronioną domenę *domena.int* i kliknij przycisk *Edit*.
4. Rozwijamy Advanced Settings > Other, odznaczamy *Use global bayesian database*
5. Klikamy OK



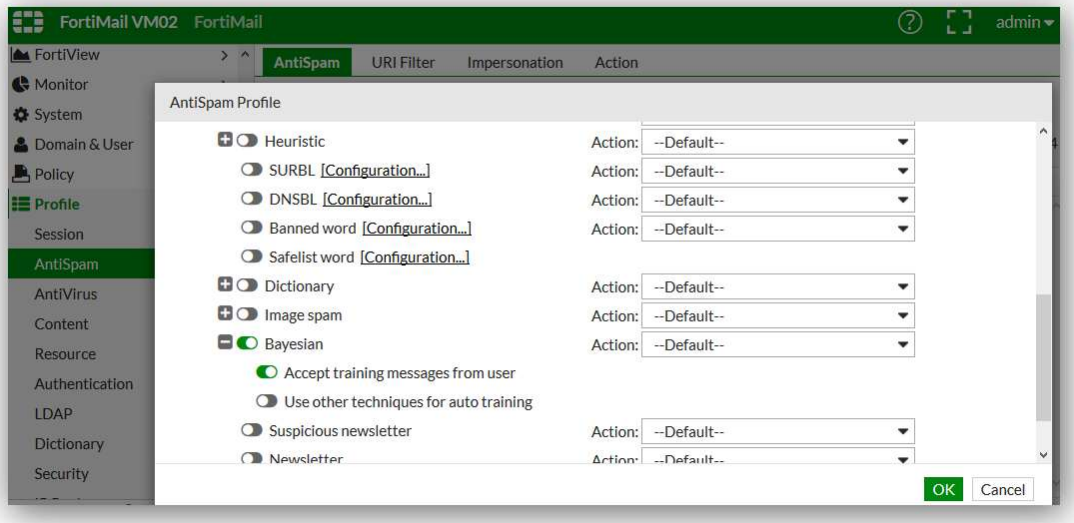
6. Następnie przechodzimy do *Security* → *Bayesian* → *Control Account* gdzie możemy zweryfikować konta, które są wykorzystywane do określania typu danej wiadomości.



7. Ostatnim elementem konfiguracyjnym jest możliwość wykorzystania bazy przez profil antyspamowy

8. Przechodząc do *Profile* → *AntiSpam* wybieramy stworzony przez nas profil i go edytujemy

9. Zaznaczamy Bayesian, dodatkowo mamy możliwość ustawienia, aby nasz system akceptował wiadomości od naszych użytkowników poprzez zaznaczenie opcji *Accept training messages from user*



10. Zatwierdzamy, *OK*

XV. Ochrona przed blacklistingiem

Omówienie przez prowadzącego:

1. Profile sesyjne
2. Polityki Access Control
3. Polityki Recipient Policy

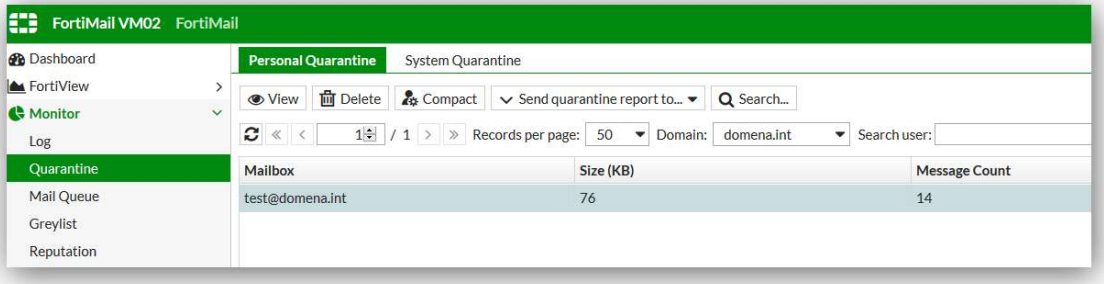
XVI. Kwarantanna

Kwarantanna na FortiMail'u została podzielona na kwarantannę systemową oraz kwarantannę użytkowników

FortiMail może poddać kwarantannie wiadomości e-mail, które zostały oznaczone jako spam, zawierają zabronione słowo, frazę lub w wiadomości został wykryty wirus.

Wiadomości poddane kwarantannie są przechowywane w folderach. Administrator systemu ma dostęp zarówno do kwarantanny systemowej oraz użytkowników. W chwili obecnej nasz system jest już tak skonfigurowany, że działa zarówno kwarantanna użytkowników dla wiadomości oznaczonych, jako spam oraz kwarantanna systemowa w przypadku wykrycia wirusa.

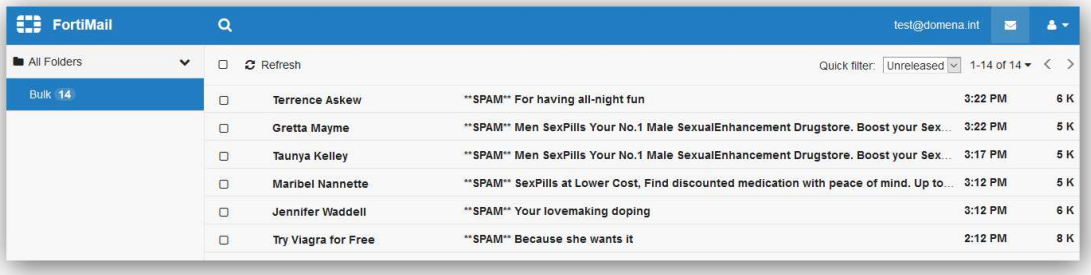
Logując się do urządzenia i przechodząc do *Monitor > Quarantine* mamy podgląd wiadomości, które wpadły w kwarantannę.



Administrator z tego poziomu ma możliwość usunięcia wiadomości, bądź przesłania jej do adresata lub innego użytkownika poprzez przycisk *Release.* Administrator z tego poziomu może również przesłać raport z kwarantanny do wszystkich lub wybranych osób, ale o tym będzie mowa w kolejnych ćwiczeniach.

Użytkownicy również mają dostęp do własnej kwarantanny po skonfigurowaniu profilu uwierzytelniającego.

Logujemy się do Fortimaila w trybie Gateway tym razem za pomocą linku https://poczta.vfml.pl:XX443/admin/ TABELA!!! użytkownik *test* hasło *test*



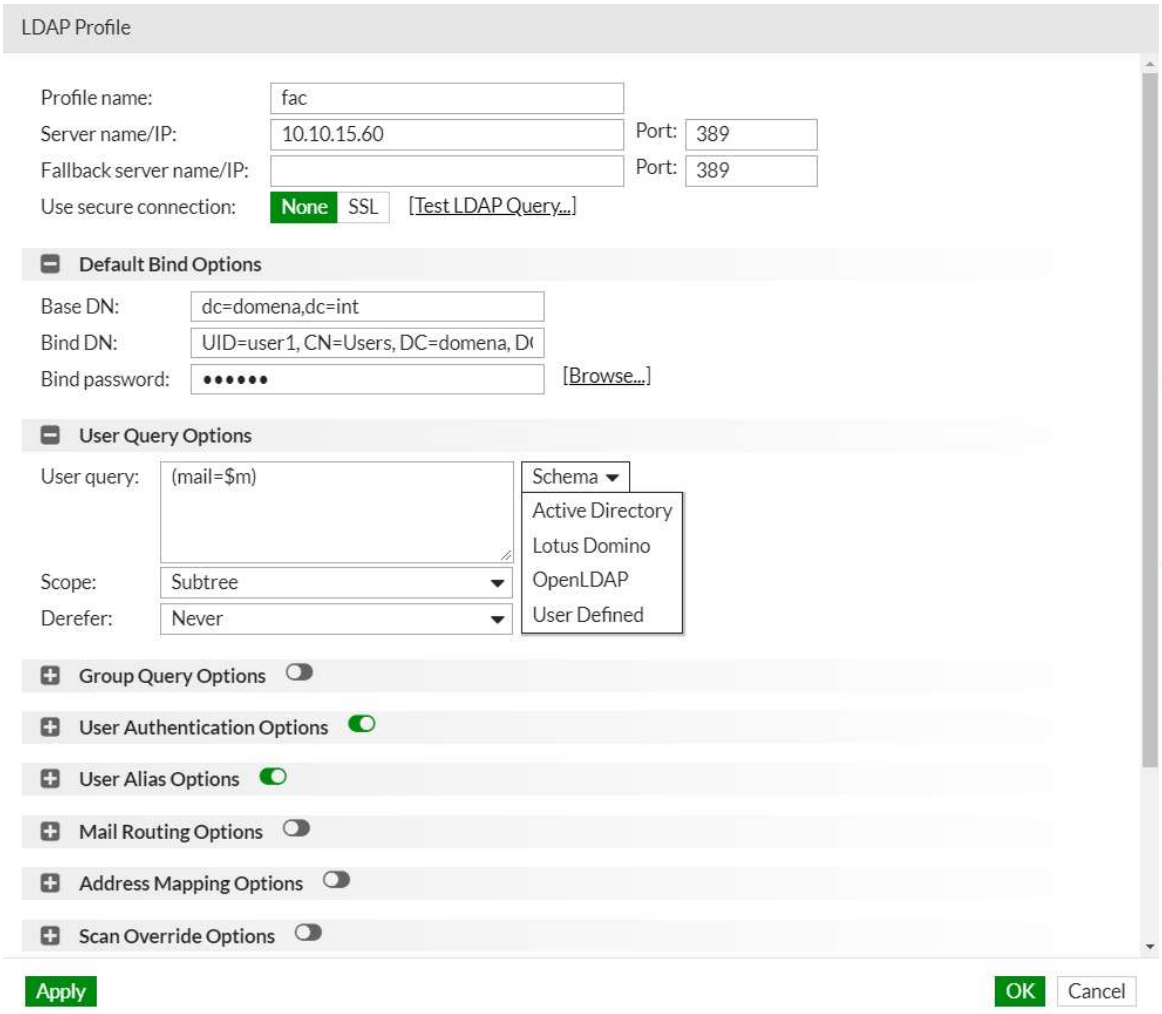
XVII. Integracja z LDAP

Informacja o użytkownikach na serwerze przechowywana jest w usłudze katalogowej opartej o LDAP. Aby z niej skorzystać należy skonfigurować profil LDAP

W naszym środowisku skorzystamy z wirtualnej maszyny FortiAuthenticator, do którego będziemy się łączyć w celu pobrania informacji o użytkownikach.

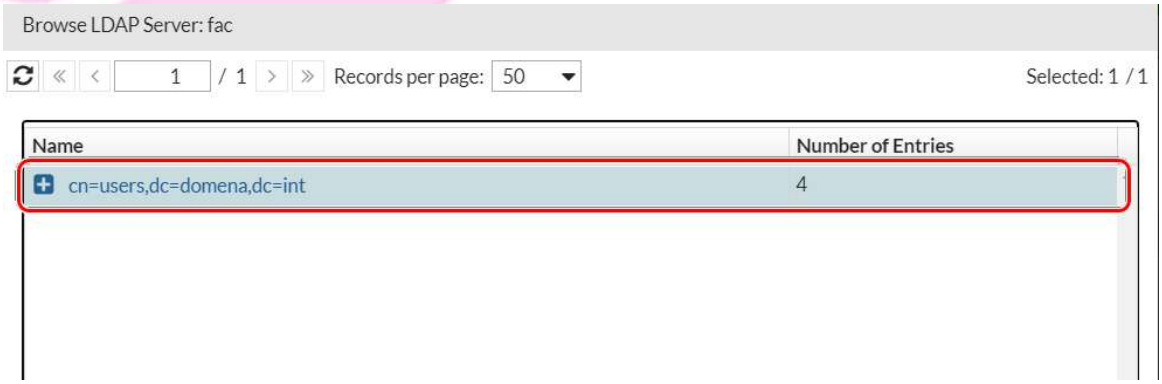
1. Logujemy się do GUI na FortiMail w trybie Gateway: https://poczta.vfml.pl:XX443/admin/ TABELA!!!,
2. Przechodzimy do *Profile > LDAP* zakładka LDAP wybieramy *New*
3. Konfigurujemy profil zgodnie z poniższą tabelą:

Profile name	LDAP
Server name/IP:	192.168.1.101
Default Bind Options	Rozwijamy
Base DN:	DC=veracomp, DC=local
Bind DN:	CN=Administrator,CN=Users,DC=veracomp,DC=local
Bind Password:	P@ssw0rd123
User Query Options	Rozwijamy
User query	Schema → User Defined
Pozostałe	Zostawiamy domyślne



4. Zapisujemy poprzez *Create*

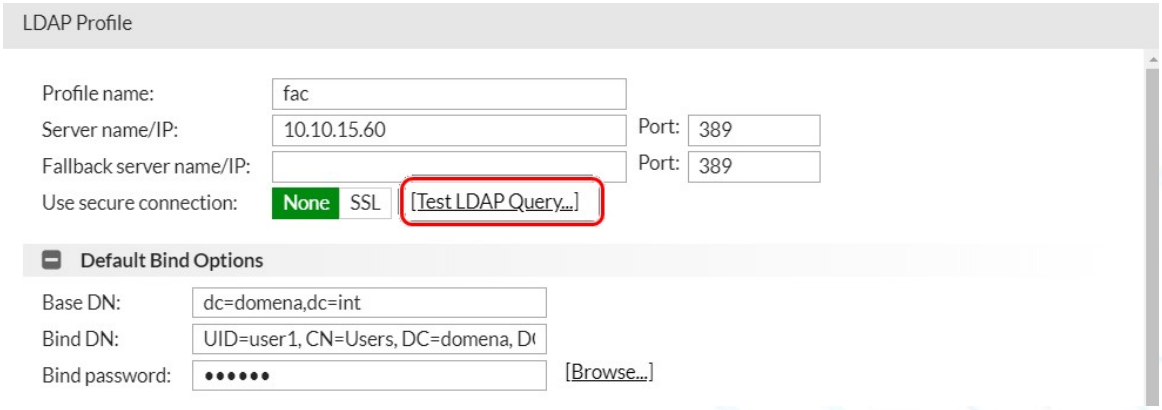
5. Aby sprawdzić, czy LDAP został prawidłowo skonfigurowany w nowym profilu, edytujemy właśnie utworzony profil, a następnie w obszarze *Default Bind Options* klikamy *Browse*. Powinniśmy mieć możliwość przeglądania drzewa LDAP.



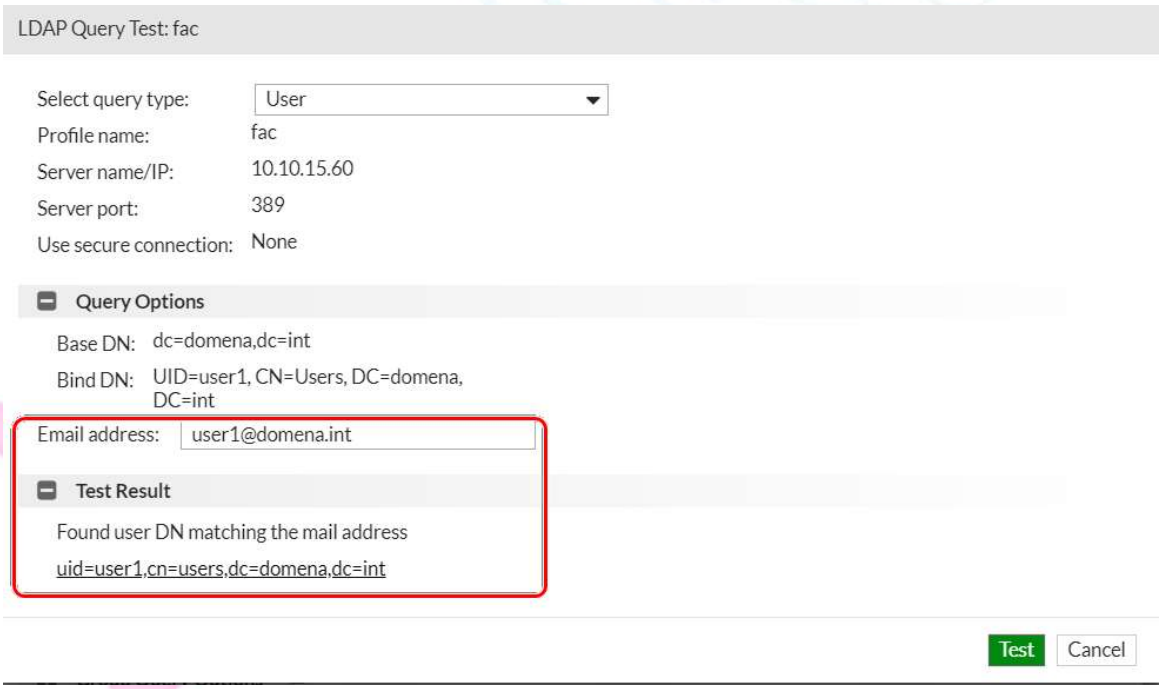
6. Rozwijając powyższa grupę użytkowników możemy poznać szczegóły dotyczące wpisu specyficznego dla użytkownika

7. Do testów mamy użytkowników userXX, wszyscy z hasłem Passw0rd123

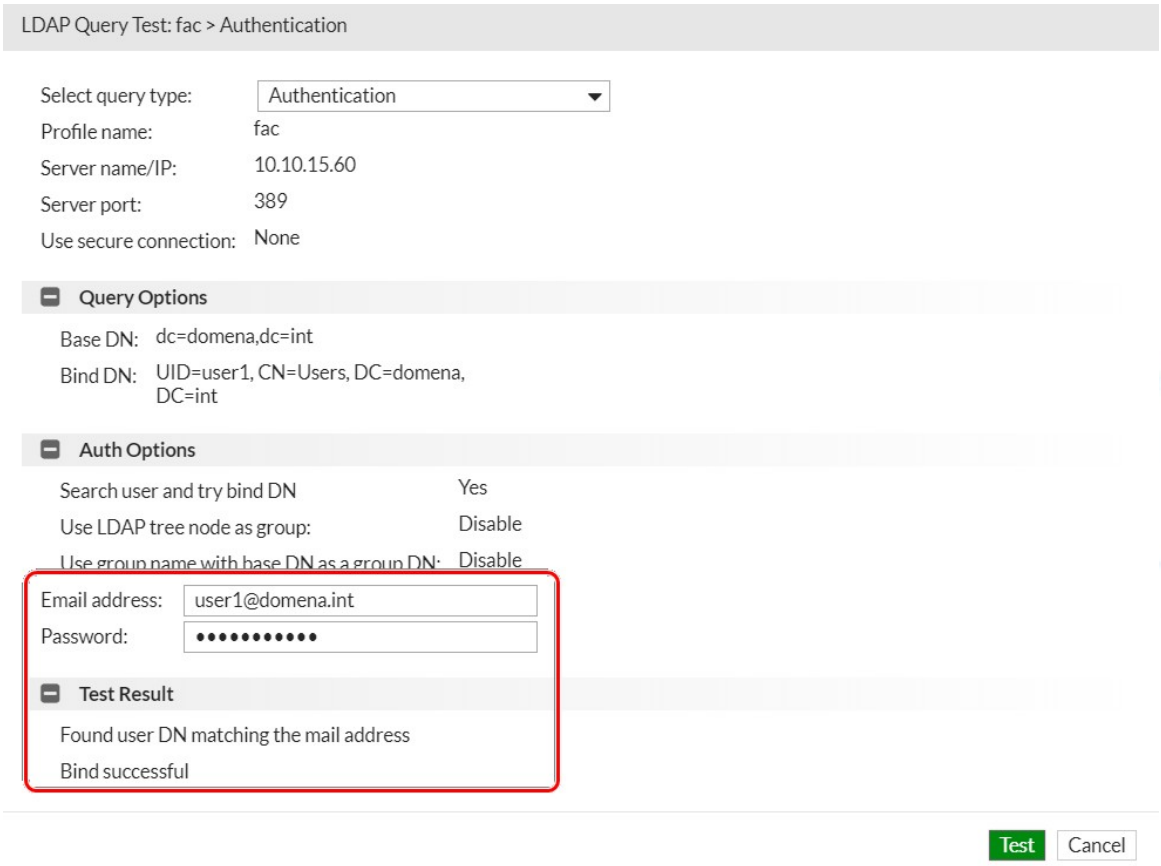
Aby przetestować zapytania LDAP możemy skorzystać z *Test LDAP Query*



8. Wybierając *query type* możemy zweryfikować do jakiego użytkownika należy dany adres e-mail

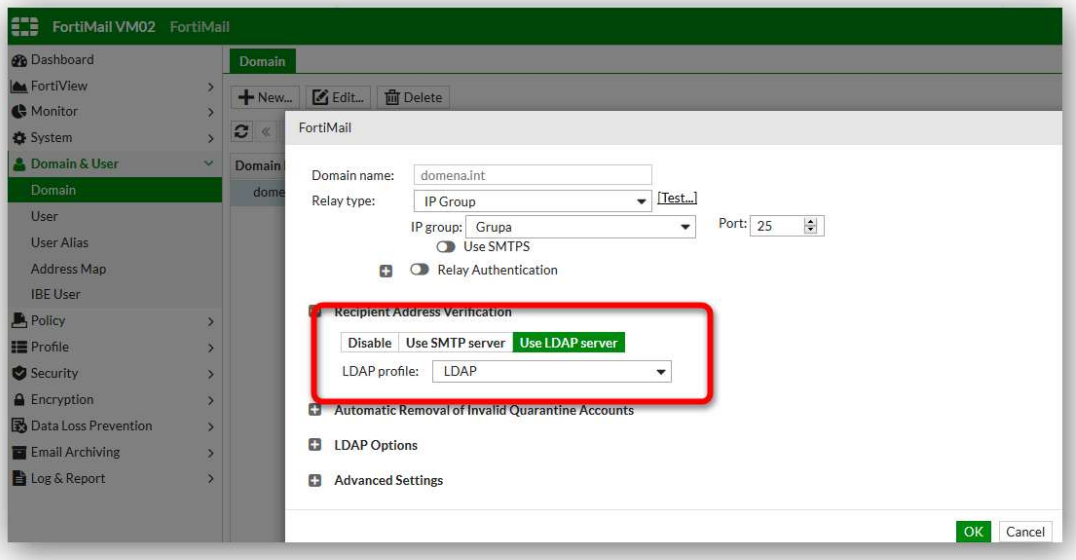


Oraz czy dla działają poświadczenia:



9. Ostatnim elementem konfiguracyjnym jest włączenie weryfikacji odbiorców w oparciu o poświadczenia LDAP:

Przechodzimy do zakładki *domain & user* → *Domain*, wybieramy naszą chronioną domenę *domena.int* w sekcji *Recipient Address Verification* zaznaczamy *Use LDAP server* i wybieramy utworzony profil LDAP.



10. Teraz możemy wykonać test wysyłając wiadomość z zewnętrznej domeny od użytkownika *userXX@domena.ext* do użytkownika w naszej chronionej dominie *userXX@domenaXX.int*

Logujemy się na witrynie: http://poczta.vfml.pl:15022/squirrelmail/src/login.php za pomocą użytkownika ***userXX*** oraz hasłem ***fortinet***

11. Czy wiadomość została dostarczona?

12. (Sprawdzamy logi na FML Gateway oraz FML Server)

Log Details: 0200002880

Column	Content
#	1
Date	2017-10-31
Time	13:09:25
Classifier	Not Spam
Disposition	Accept
From	user01@domena.ext
Header From	user01@domena.ext
To	user1@domena.int
Subject	Re: test
Length	958
Session ID	v9VC9Pad002879-v9VC9Paf002879
Client	[10.10.15.20]
Direction	in
Policy IDs	1:1:1
Domain	domena.int
Destination IP	10.10.15.30
Mailer	mta
Resolved	FAIL
Level	information
Log ID	0200002880

13. Następnie przechodząc do ustawień chronionej domeny *Domain&User > Domain* edycja domeny *domena.int* w sekcji *Recipient Address Verification* zaznaczamy *Use LDAP server* i wybieramy utworzony profil LDAP

14. Podobnie konfigurujemy urządzenie w trybie serwera. – Dodatkowo w konfiguracji chronionej domeny *Domain&User > Domain* edycja domeny *domena.int w sekcji LDAP Options* wybieramy utworzony profil LDAP

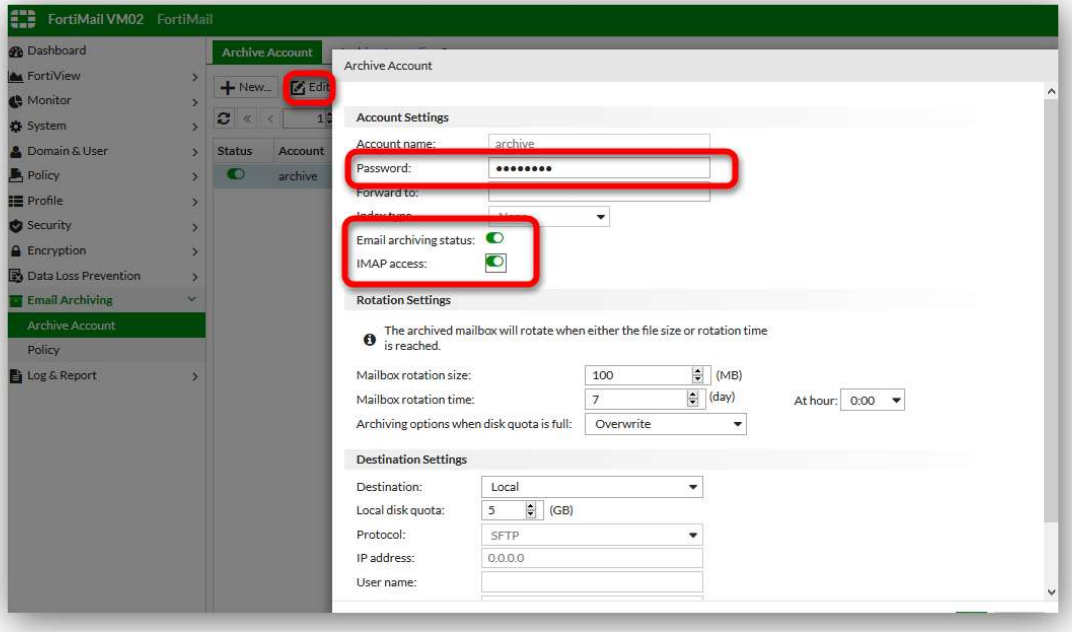
XVIII. Archiwizacja poczty w oparciu o polityki

Kolejną funkcją dostępną na platformie FortiMail jest archiwizacja poczty. Wybór wiadomości, które powinny zostać zarchiwizowane wykonywany jest w oparciu o kryteria, takie jak nadawca wiadomości, odbiorca wiadomości, temat, treść lub załączniki. Do takiego archiwum administrator lub osoba uprawniona ma dostęp przez protokół IMAP. Archiwizacja może odbywać się lokalnie na urządzeniu FortiMail, może też zostać wyniesiona zewnętrzne zasoby dyskowe.

1. Logujemy się do GUI na FortiMail w trybie Gateway: https://poczta.vfml.pl:XX443/admin/ TABELA!!!
2. Przechodzimy do zakładki Email Archiving > Archive Account.
3. Możemy wykorzystać już istniejące konto, które domyślnie jest utworzone na urządzeniu *archive* klikamy *Edit*

- Ustawiamy hasło dla konta *fortinet* zaznaczamy
- Email archiving status: Enabled
- IMAP access: Enabled
- Pozostałe ustawienia zostawiamy z domyślnymi ustawieniami.

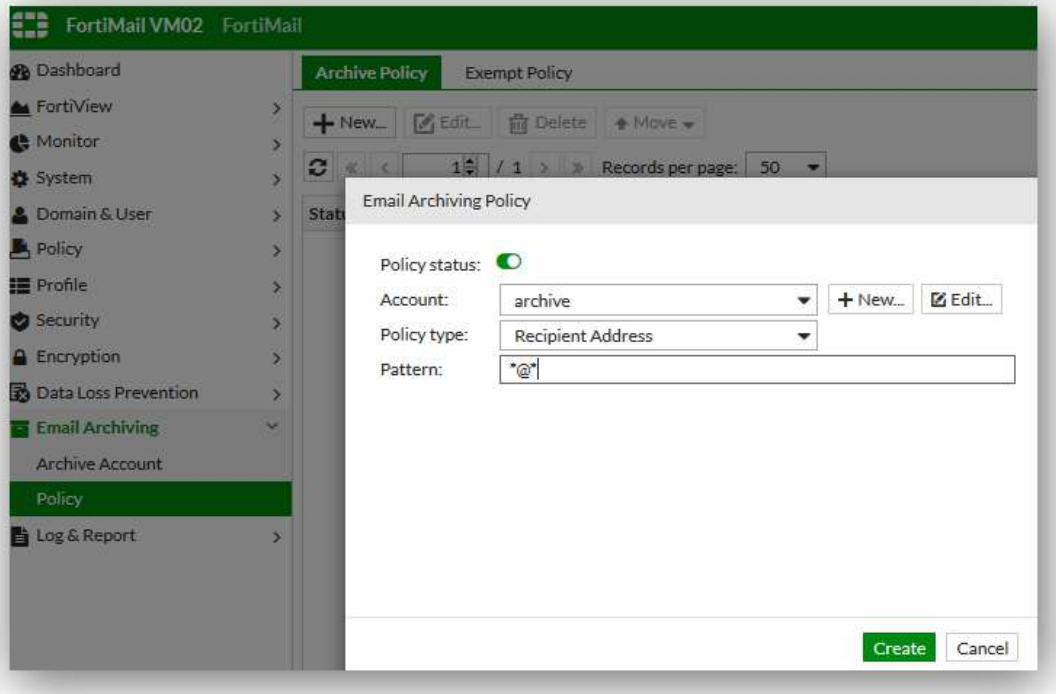
Dla tego konta archiwizacja będzie odbywać się lokalnie na dysku urządzenia.



Następnie przechodzimy do *Email Archiving > Policy* zakładka *Archive Policy* klikamy *New*

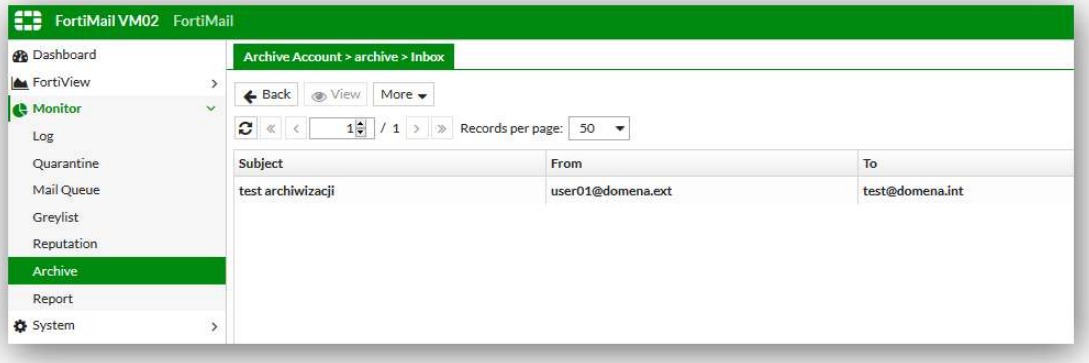
4. Kreujemy politykę, która umożliwia archiwizację wszystkich wiadomości zgodnie z poniższym ustawieniem

Policy status:	Włączone
Account:	archive
Policy type:	Recipient Address
Pattern:	*@*



5. Dostęp do archiwum mamy poprzez GUI przechodząc do *Monitor > Archive* zakładka *Archive Accounts*

Jak widzimy nasze urządzenie archiwizuje teraz wszystkie wiadomości.



UWAGA: Archiwizacja może również zostać realizowana na zewnętrznych zasobach za pomocą protokołu SFTP lub FTP.

XIX. Szyfrowanie poczty w oparciu o polityki (IBE)

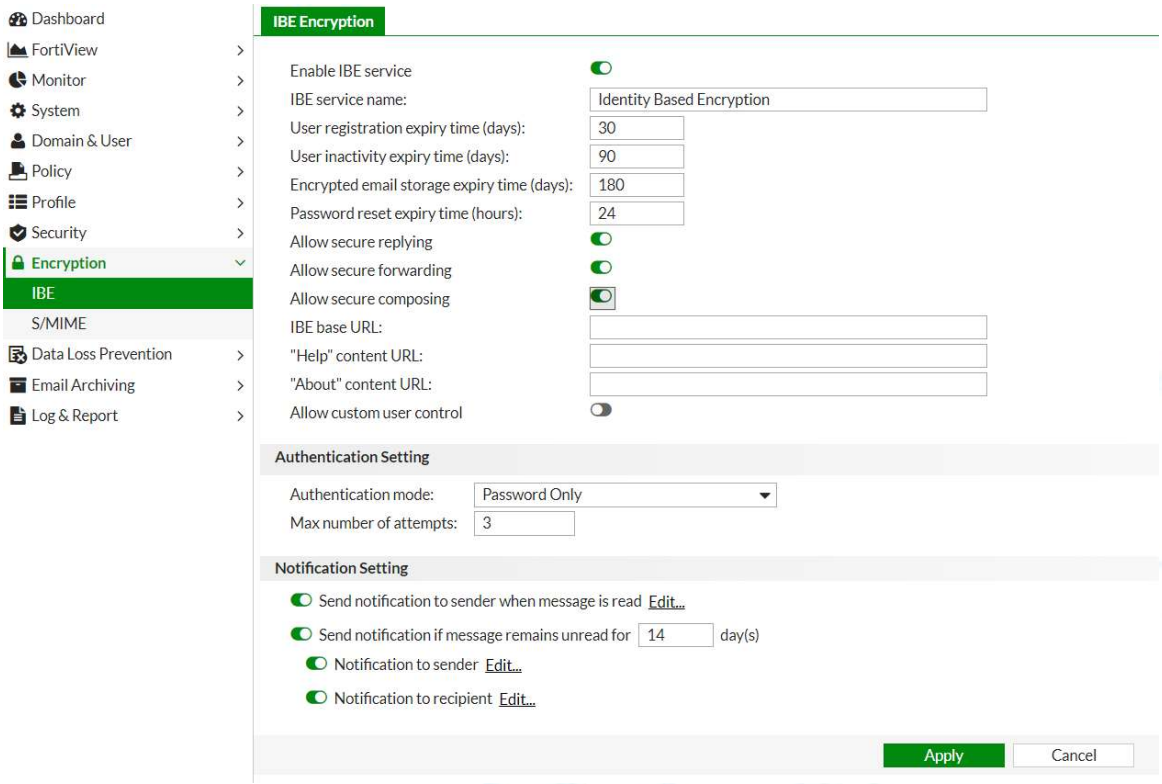
Jedną z ciekawych funkcjonalności, która jest dostępna na platformie jest IBE, czyli *Identity Based Encryption*, zwana również *Policy Based Encryption*. Ta funkcja jest odpowiedzią wprost na potrzebę zagwarantowania dostarczenia przesyłki pocztowej w sposób bezpieczny - zaszyfrowany, najczęściej do odbiorcy zewnętrznego. W przypadku takiego odbiorcy zwykle nie jesteśmy w stanie kontrolować środowiska w jakim on pracuje i konfiguracji jego klienta pocztowego. Jeżeli to jest adresat, u którego nie wiemy, jak skonfigurowany jest klient, nie wiemy czy wykorzystuje szyfrowane protokoły do połączenia z serwerem pocztowym, to nie mamy właściwie żadnej gwarancji, że ta poczta zostanie dostarczona w bezpieczny sposób. Oczywiście można to egzekwować w oparciu o infrastrukturę klucza prywatnego i publicznego, te rozwiązania są działające i skuteczne. Minusem takiego rozwiązania jest fakt, że trzeba wymusić zainstalowanie i konfigurację certyfikatów oraz przeszkolić klienta tak, by potrafił te certyfikaty wykorzystać. Jeżeli adresatem jest organizacja zewnętrzna, to często mamy nikły wpływ na to, w jaki sposób odbiorca korzysta z poczty, tym samym wymuszenie korzystania z kluczy jest w zasadzie niemożliwe. W takim przypadku z pomocą przychodzi nam wyżej wspomniana funkcja.

Funkcja Identity Based Encryption działa na dwa sposoby. W działaniu są one bardzo podobne do siebie. Pierwszym rodzajem jest metoda pull. Polega ona na tym, że w momencie, kiedy użytkownik wysyła pocztę z dowolnego programu pocztowego, a wiadomość ta przechodzi przez FortiMail, następuje sprawdzenie, czy wiadomość zostanie zaklasyfikowana jako wiadomość do bezpiecznego dostarczenia. Kryteria takiego sprawdzania są w pełni konfigurowalne. Jeżeli wiadomość ma zostać bezpiecznie dostarczona, to następuje zatrzymanie wiadomości na urządzeniu. Jest to jedna z niewielu sytuacji, kiedy poczta jest buforowana, z racji tego, że FortiMail pracuje w czasie rzeczywistym. W tym samym czasie do adresata jest wysyłana wiadomość, która zawiera link do wiadomości, która ma zostać bezpiecznie dostarczona. Po otwarciu linku nawiązywane jest bezpieczne połączenie SSL i adresat wiadomości może ją bezpiecznie przeczytać. Dzięki temu w łatwy sposób i bez zbędnej konfiguracji poczta w bezpieczny sposób została dostarczona do adresata o czym się za chwilę przekonamy

Konfigurujemy FortiMail aby szyfrował wiadomości wysyłane z chronionej domeny do użytkownika w domenie *domena.ext*

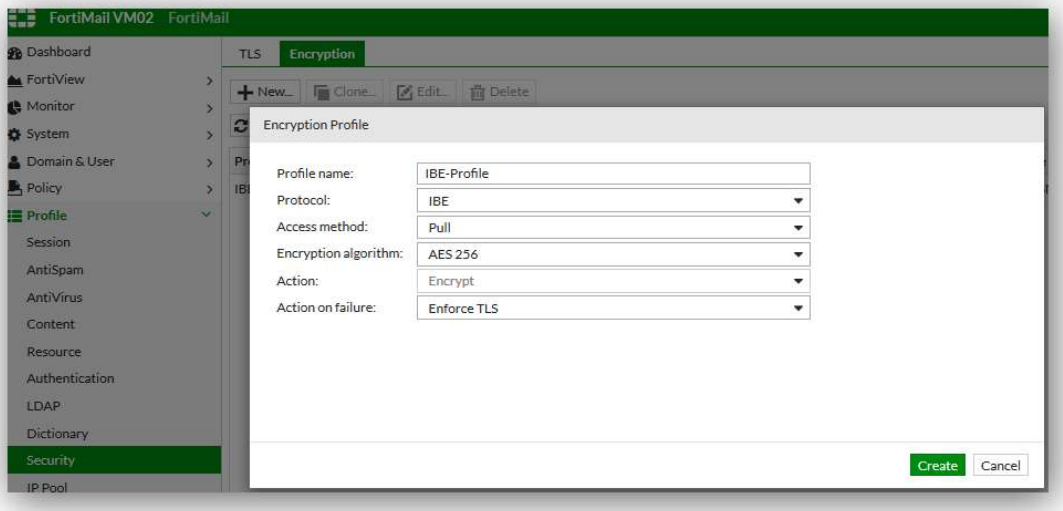
1. Logujemy się do GUI na FortiMail w trybie gateway (https://poczta.vfml.pl:XX443/admin/ TABELA!!!), przechodzimy do *Encryption > IBE > IBE Encryption.* Konfigurujemy następujące ustawienia:

Enable IBE service:	włączamy
IBE service name:	
Allow secure replying:	enabled
Allow secure forwarding:	włączamy
Allow secure composing:	włączamy
Pozostałe opcje:	Zostawiamy wartości domyślne



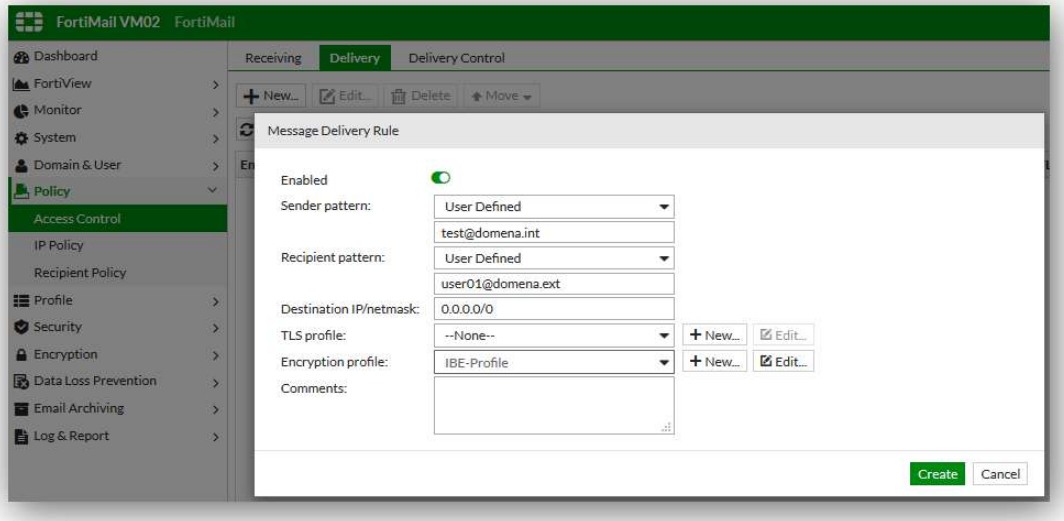
2. Definiujemy algorytm szyfrowania i metodę działania IBE. Przechodzimy do *Profile* > *Security,* zakładka *Encryption* wybieramy New. Konfigurujemy następujące ustawienia nowego profilu:

Profile name	IBE-Profile
Protocol:	IBE
Access method:	Pull
Encryption algorithm:	AES 256
Action on failure:	Enforce TLS



3. Teraz aktywujemy politykę IBE przechodząc do *Policy > Access Control* zakładka *Delivery*. Konfigurujemy ustawienia jak poniżej:

Enabled	włączone
Sender pattern	User defined →test@domenaXX.int
Recipient pattern	User defined →userXX@domena.ext
Encryption profile:	IBE Profile
Pozostałe opcje:	Zostawiamy wartości domyślne

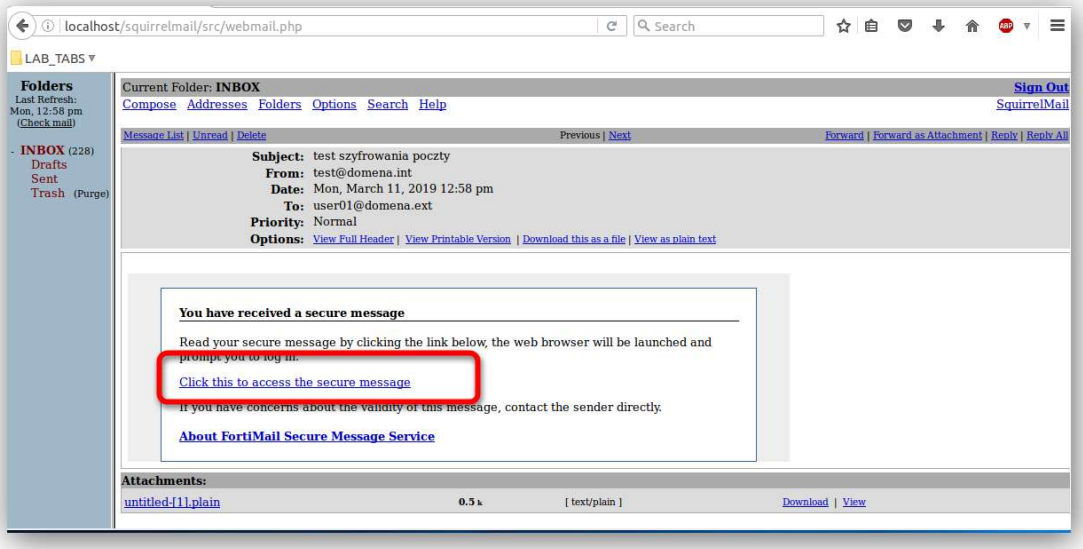


4. Logując się do webmaila na serwer poczty (https://poczta.vfml.pl:XX443/admin/ TABELA!!!)

Użytkownik *test* hasło *test*

Wysyłamy wiadomość o dowolnej treści do użytkownika *userXX@domena.ext*

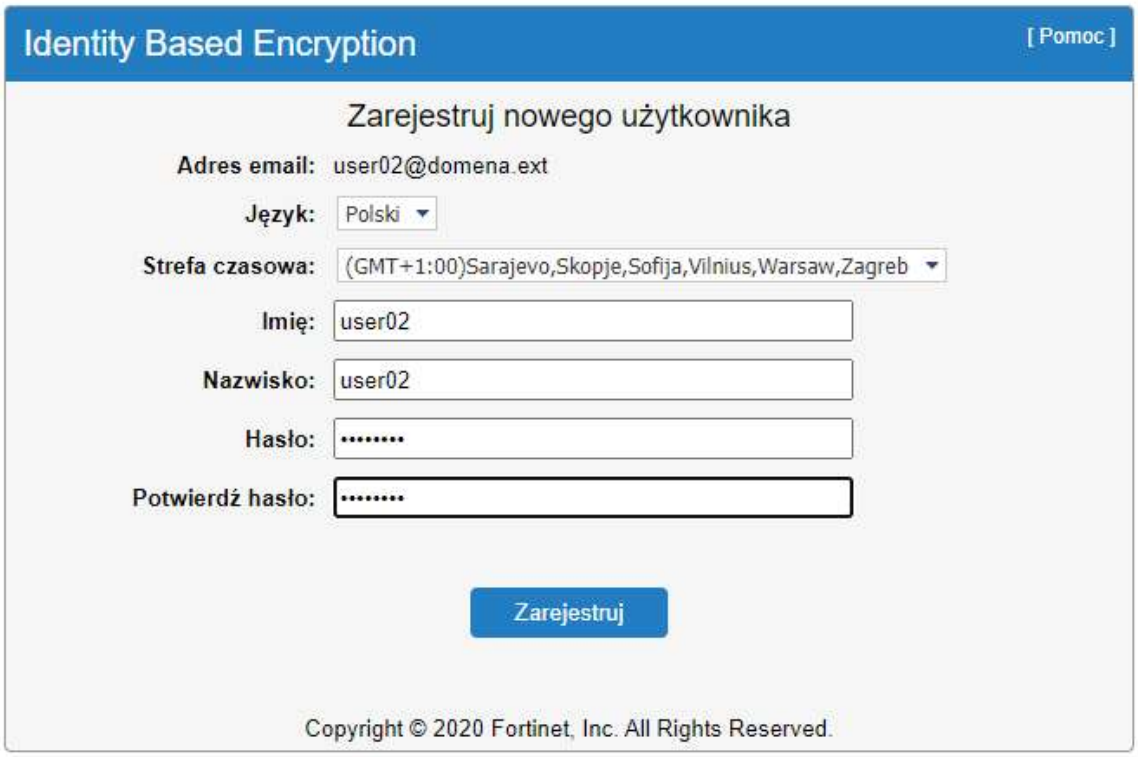
5. Następnie przechodzimy na maszynę „malware-client" i sprawdzamy pocztę użytkownika userXX@domena.ext. User01 powinien potrzymać poniższą wiadomość:



Klikając w załączony w wiadomości link otrzyma dostęp do zaszyfrowanej wiadomości

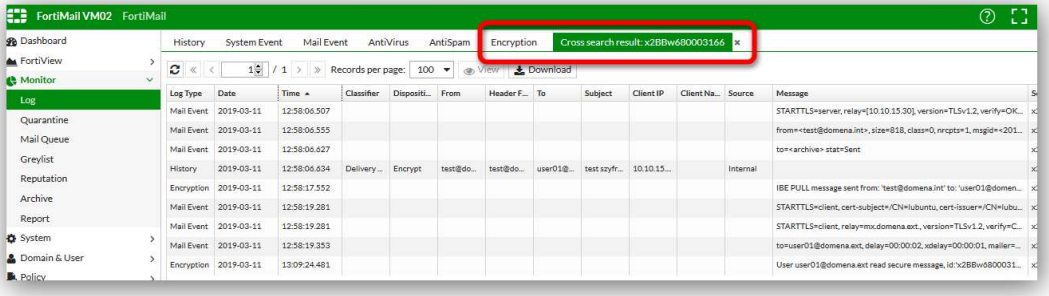
6. User01 nie jest jeszcze zarejestrowany wiec otrzyma poniższy komunikat

7. Więc się rejestrujemy klikając *Register i* uzupełniamy wymagane informacje

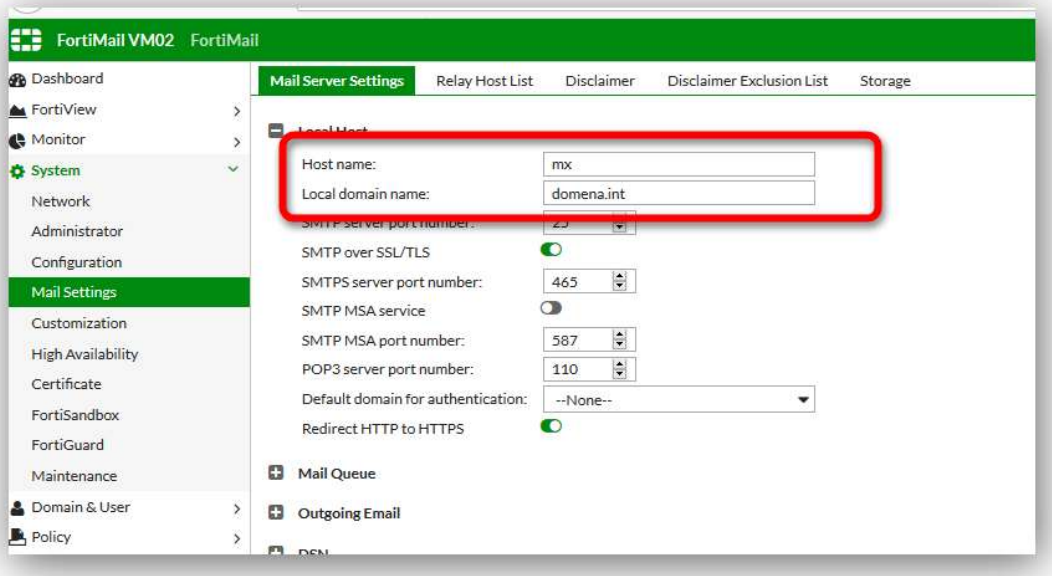


Potwierdzamy rejestrację i możemy zalogować się do webmaila za pomocą hasła, które stworzyliśmy.

8. Na naszym FortiMailu w trybie Gateway możemy sprawdzić przebieg komunikacji przechodząc do *Monitor* > *Log* zakładka *Encryption.* Powinniśmy otrzymać logi podobne do poniższych



UWAGA: najczęstszy problem, Jeśli link do zaszyfrowanej wiadomości nie chce działać, sprawdź czy nazwa fortimaila w trybie gatewaya jest prawidłowa. – Jak na poniższym rysunku:

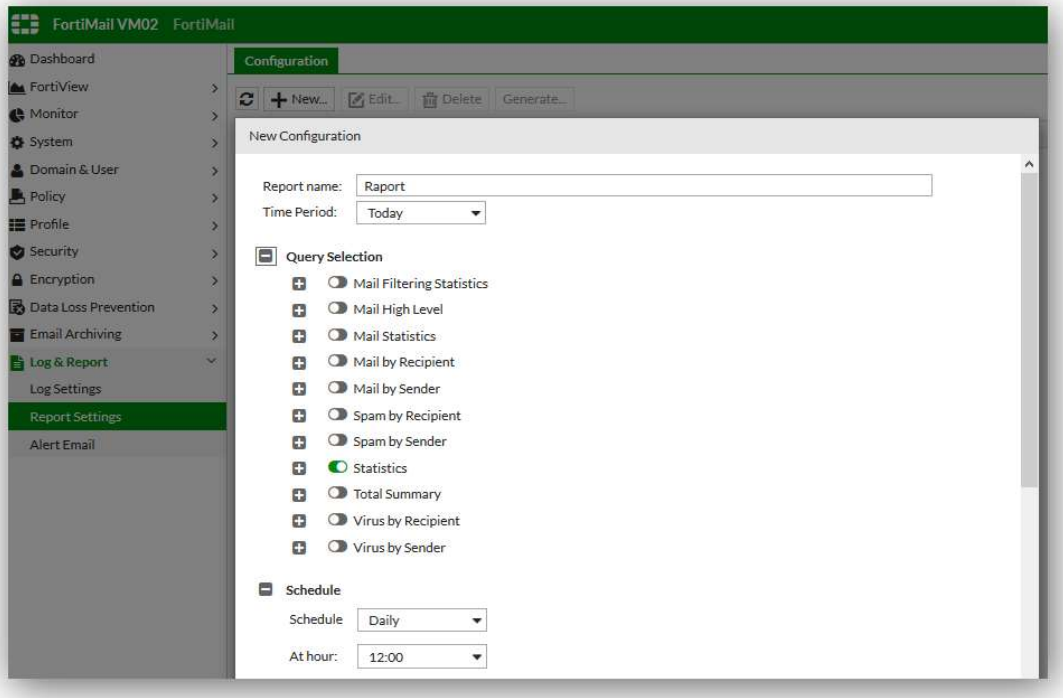


XX. Raportowanie

Na urządzeniu mamy możliwość skonfigurowania profili raportów, które będą generować raporty zgodnie z harmonogramem bądź na żądanie. FortiMail prezentuje informacje w formie graficznej i tabelarycznej.

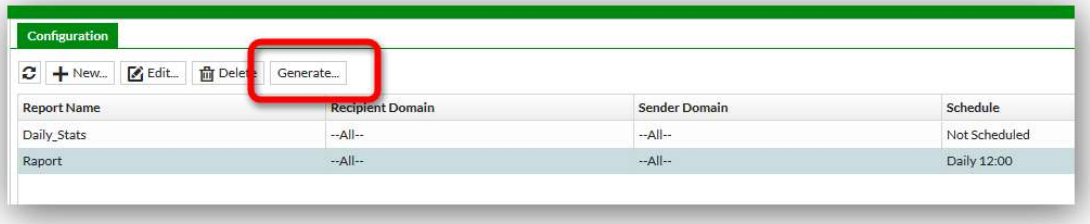
1. Logujemy się do GUI na FortiMail w trybie gateway (https://poczta.vfml.pl:XX443/admin/ TABELA!!!),
2. Przechodzimy do *Log and Report > Report Settings* wybieramy *New* w celu utworzenia nowego raportu
3. Konfigurujemy zgodnie z poniższą tabelą:

Report Name	Raport
Time Period:	Today
Query Selection → statistic	Włączamy
Schedule →	Schedule: Daily , At hour 12:00
Sender Domain	All domain
E-mail *Notification* → Report Format:	pdf

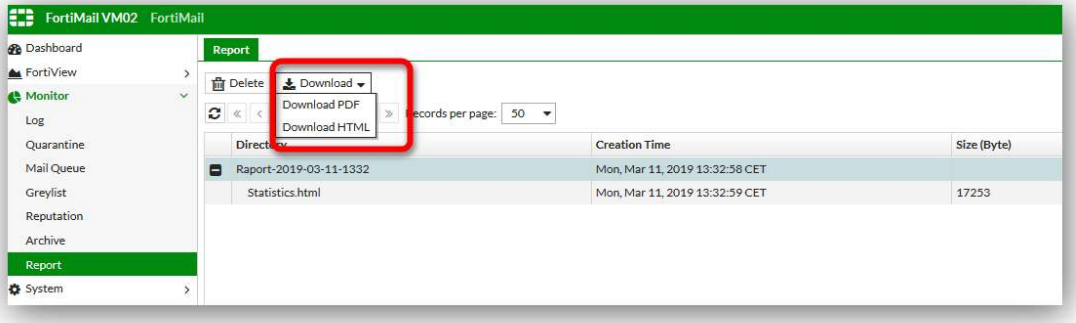


Zgodnie z konfiguracja raport zostanie wygenerowany o godzinie 12:00.

4. Zawsze możemy wygenerować raport na żądanie klikając przycisk *Generate*…



5. Przechodząc do Monitor > Report możemy przeglądać raporty. Raporty możemy również pobrać w formacie PFD lub HTML.



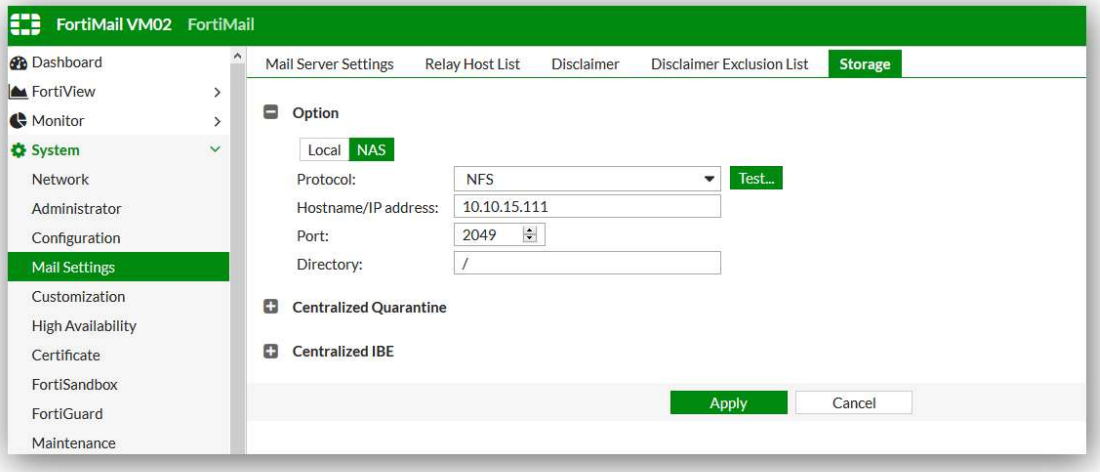
XXI. Przechowywanie poczty na zewnętrznych zasobach

Każde urządzenie FortiMail zarówno wersje sprzętowe jak i wirtualne posiadają ograniczone zasoby na przechowywanie poczty. Pocztę możemy archiwizować ale również składowanie poczty może być realizowane na zewnętrznych zasobach. Zasoby jakie mogą zostać wykorzystane to dowolne urządzenie pracujące jako NAS lub iSCSI.

Dla testu możemy skorzystać z oprogramowanie FreeNFS.

1. Uruchamiamy program FreeNFS
2. Logujemy się do GUI na FortiMail w trybie serwer (https://poczta.vfml.pl:XX443/admin/ TABELA!!!),
3. Przechodzimy do *System* > *Mail Settings* zakładka *Storage*
4. Konfigurujemy urządzenie jak poniżej:

Option:	rozwijamy
Local/NAS:	NAS
Protocol:	NFS
Hostname / IP address:	Adres serwera NFS
Pozostałe opcje:	Zostawiamy wartości domyślne



5. Możemy wykonać test połączenia klikając *Test…*

Na zewnętrznych zasobach może również zostać realizowana kwarantanna lub szyfrowanie poczty w oparciu o polityki IBE.

XXII. Konfiguracja HA

W przypadku platform FortiMail możemy wykonać klastrowanie active-passive HA oraz config-only.

W trybie active-passive jesteśmy ograniczeni do dwóch urządzeń, połączonych ze sobą w konfiguracji redundantnej. W tym trybie następuje pełna synchronizacja wszystkich elementów, w tym skrzynek pocztowych, archiwów, kwarantanny, logów czy ustawień filtrów. W przypadku, gdy aktywna część klastra przestanie odpowiadać, druga część natychmiast uruchomi się i rozpocznie pracę.

Tryb config-only polega na synchronizacji tych elementów, które nie są unikalne i powtarzają się na każdym urządzeniu, przykładowo reguł związanych z analizą wiadomości i ich klasyfikacją. Każde urządzenie działa niezależnie od siebie. W tym trybie możemy stworzyć klaster maksymalnie 25 urządzeń, co więcej - mogą to być różne platformy. Taki klaster musimy dodatkowo wyposażyć w jakieś zewnętrzne rozwiązanie, które będzie rozdzielało ruch pomiędzy te urządzenia, może to być przykładowo urządzenie FortiGate

Porównanie trybów HA:

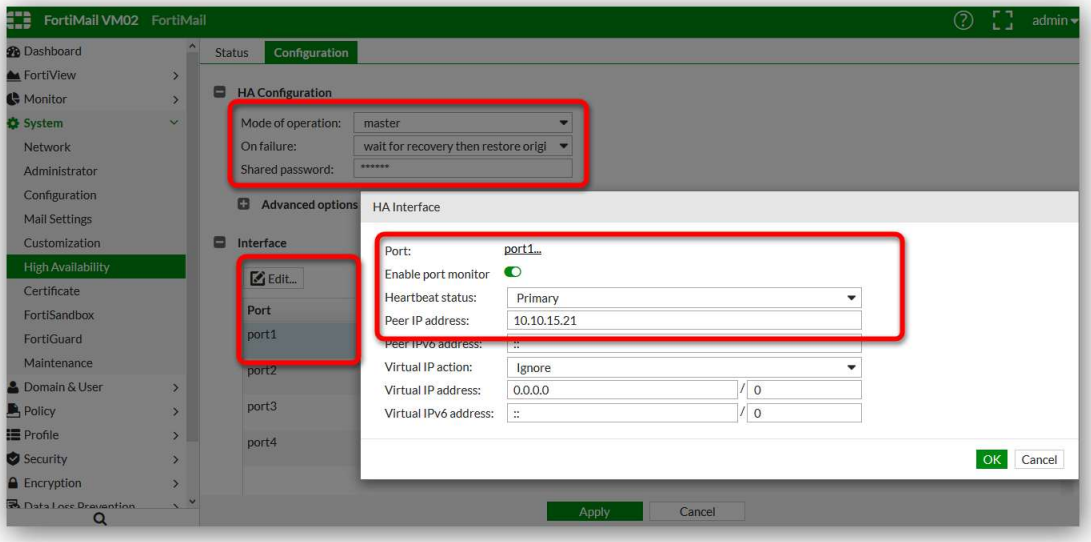
Active-passive HA	**Config-only HA**
2 FortiMail units in the HA group	2-25 FortiMail units in the HA group
Typically deployed behind a switch	Typically deployed behind a load balancer
Both configuration* and data synchronized	Only configuration* synchronized
Only primary unit processes email	All units process email
No data loss when hardware fails	Data loss when hardware fails
Failover protection, but no increased processing capacity	**Increased processing capacity, but no failover protection**

Skonfigurujemy tryb pracy Active – Passive na przykładzie urządzeń pracujących w trybie gateway.

1. Przed przystąpieniem do tego ćwiczenia należy sprawdzić czy mamy licencje dla kolejnego FML, jeśli nie dysponujemy dodatkowymi licencjami - w ramach testu można odłączyć się od Internetu, tak, aby nasze urządzenia nie mogły połączyć się z siecią fortiguard.
2. Robimy klona wirtualnej maszyny FortiMail Gateway. Na sklonowanej maszynie należy zmienić adres IP na 10.10.15.21 (Instrukcja w rozdziale „wstępna konfiguracja …")
3. Logujemy się do GUI na FortiMail w trybie gateway (https://poczta.vfml.pl:XX443/admin/ TABELA!!!),
4. Przechodzimy do *System → High Availability* zakładka Configuration
5. Konfigurujemy urządzanie jako Master jak pokazano poniżej wpisując hasło ***fortinet***

HA configuration:	Rozwijamy
Mode of operation:	Master
On failure:	Wait for recovery then restore original role
Sharef password:	fortinet

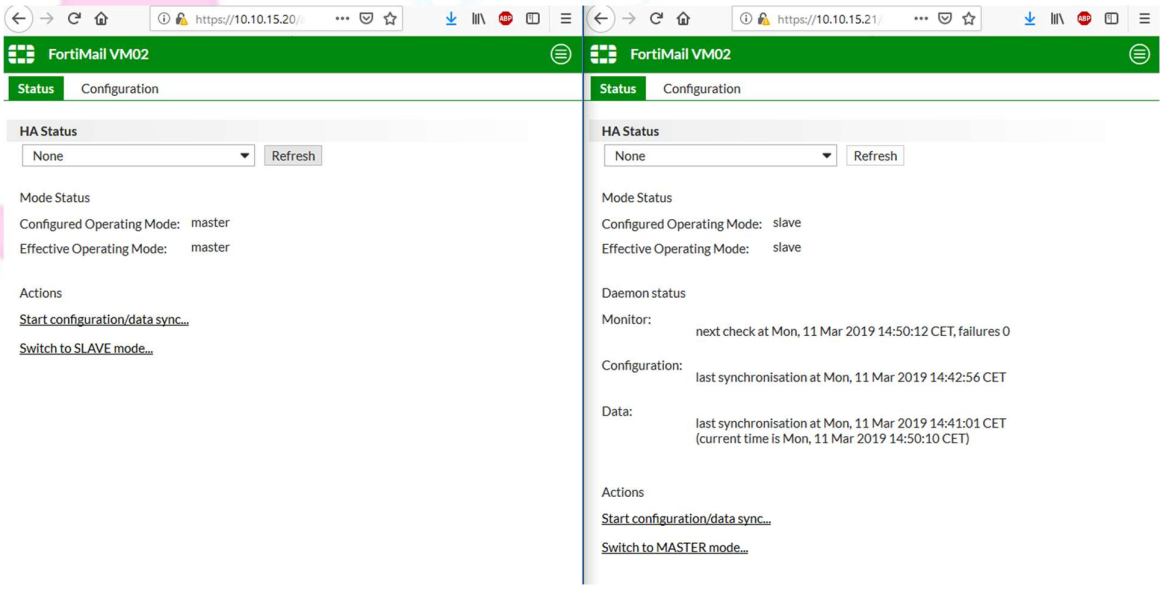
6. Rozwijamy *interface* i edytujemy *port1*. Włączamy Enable port monitor, *hearbeat status* ustawiamy, jako *Primary*, a w polu *Peer IP address* podajemy adres **DRUGIEGO** fortimaila



Dodatkowo możemy uruchomić monitorowanie pracy urządzenie w oparciu o usługi SMTP, HTTS itd.

7. Następnie logujemy się na sklonowaną maszynę za pomocą adresu (https://poczta.vfml.pl:XX443/admin/ TABELA!!!), i konfigurujemy podobnie jak przed chwilą, z tą tylko różnicą, że w polu *HA Configuration* → *Mode of operation* ustawiamy **SLAVE**

8. Przechodząc do zakładki *Status* możemy zweryfikować status pracy urządzeń

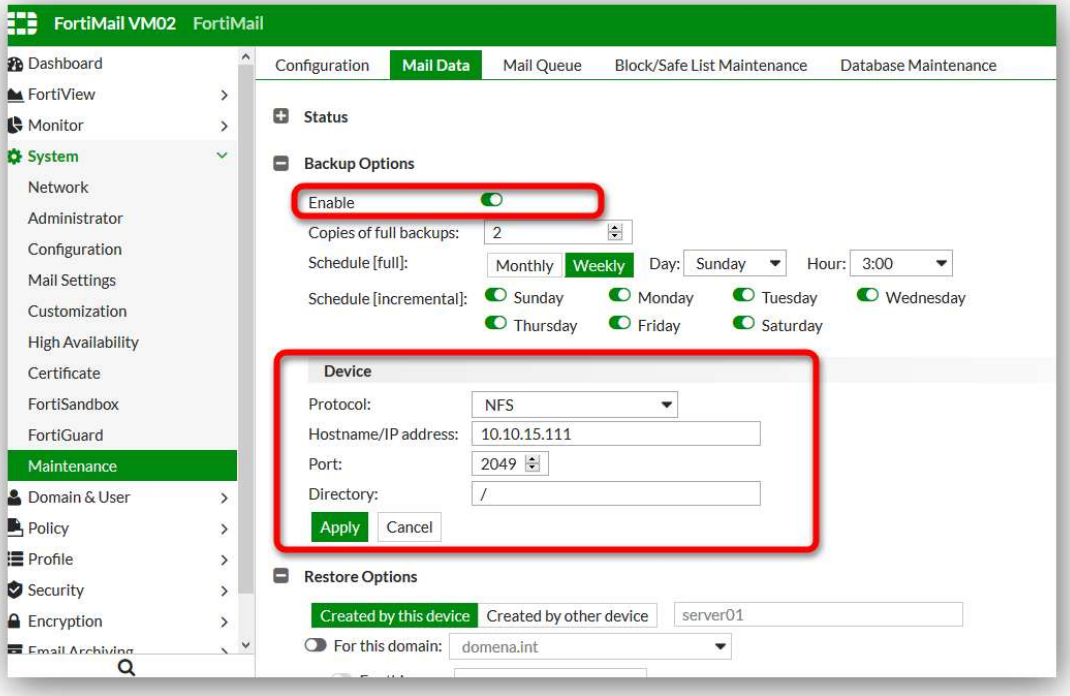


XXIII. Tworzenie kopi zapasowej oraz jej odtwarzanie

FortiMail umożliwia tworzenie kopi zapasowej konfiguracji urządzenia, kopi danych użytkowników oraz ich przywracanie. Kopia zapasowa może być wykonywana ręcznie, zgodnie z harmonogramem, lokalnie lub na zewnętrznych zasobach. W ćwiczeniu skonfigurujemy kopie zapasową wiadomości użytkowników na zewnętrznym zasobie NAS.

Dla testu możemy skorzystać z oprogramowanie FreeNFS.

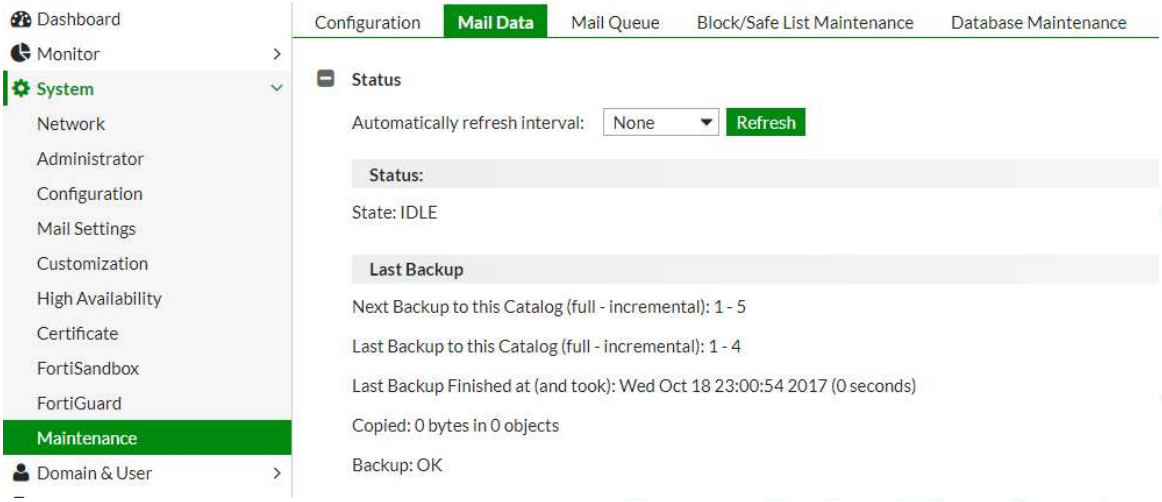
1. Uruchamiamy program FreeNFS
2. Logujemy się do GUI na FortiMail w trybie serwer (https://poczta.vfml.pl:XX443/admin/ TABELA!!!),
3. Przechodzimy do *System → Maintenence* zakładka *Mail Data*
4. Konfigurujemy urządzenie zgodnie z poniższymi ustawieniami podając *Hostname/IP address* komputera z uruchomionym programem FreeNFS



Zatwierdzamy klikając *Apply*

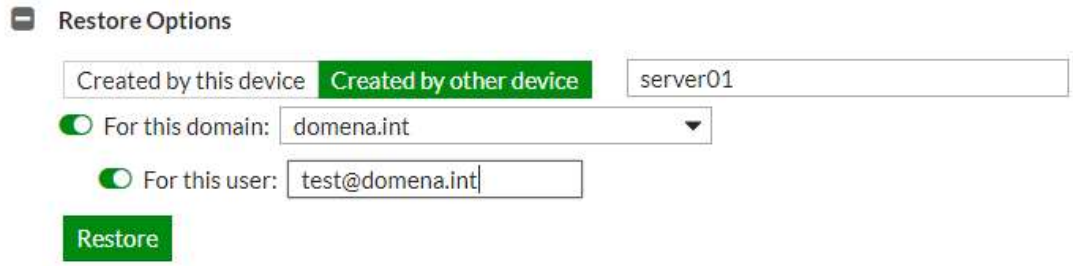
5. Kopia zapasowa wiadomości zostanie wykonana zgodnie z harmonogramem lub możemy uczynić to wcześniej rozwijając sekcje *Status* i klikając *Click here to start a backup*

6. Kopia zapasowa powinna się utworzyć na serwerze NAS i powinniśmy otrzymać poniższą informację:



7. Przywrócić wiadomości użytkownika możemy zrealizować na dwa sposoby:

- poprzez interfejs GUI z ostatniej kopi zapasowej wybierając *Restore Options* jak poniżej:



Zatwierdzamz wybierając *Restore*

- poprzez interfejs CLI z kopi zapasowej którą wybierzemy za pomocą komendy:

```
execute backup-restore old-restore <full> <inc> domain user
```

Zatwierdzając poprzez klawisz *"Y"*

Gdzie *<full>* oznacza pełny backup a *<inc>* oznacza bacakup przyrostowy, z którego przywracamy kopie zapasową

```
server01 # execute backup-restore old-restore 1 1 domain domena.int user test@domena.int
This operation can destroy data on the mail device
Do you want to continue? (y/n)y
2680: status--> 0: finished
```