**ZAŁĄCZNIK NR 2b do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA – ZADANIE NR 2**

**OPIS RÓWNOWAŻNOŚCI:**

W przypadku gdy w dokumencie stanowiącym element opisu przedmiotu zamówienia pojawią się wskazania znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego dostawcę (jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub jego produktów), należy rozumieć, zgodnie z przepisem art. 99 ust. 5 ustawy Pzp, że zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób i w takich okolicznościach Zamawiający dopuszcza możliwość składania w ofercie rozwiązań równoważnych, wskazując, iż minimalne wymagania, jakim mają odpowiadać rozwiązania równoważne, to wymagania nie gorsze od parametrów wskazanych w tych dokumentach, a ich kryteria w celu oceny równoważności wskazane są w opisie przedmiotu zamówienia.

W przypadku, gdy Zamawiający opisuje przedmiot zamówienia przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy, zamawiający dopuszcza rozwiązania równoważne opisywanym.

Wykonawcy mogą składać oferty zawierające rozwiązania równoważne w stosunku do przedmiotu zamówienia przedstawionego w SWZ – zgodnie z art. 101 ust. 4, 5 i 6 ustawy PZP, jednak są zobowiązani wykazać, że oferowane przez nich rozwiązania spełniają wymagania określone przez Zamawiającego. Równoważność pod względem parametrów technicznych, użytkowych oraz eksploatacyjnych ma w szczególności zapewnić uzyskanie parametrów nie gorszych od założonych w niniejszym SWZ

Za równoważne uznaje się rozwiązania, jak również elementy, materiały, urządzenia o właściwościach funkcjonalnych i jakościowych takich samych, które zostały określone w opisie przedmiotu zamówienia, lecz oznaczonych innym znakiem towarowym, patentem lub pochodzeniem. Przy czym istotne jest to, że produkt równoważny to produkt, który nie jest identyczny, tożsamy z produktem referencyjnym, ale posiada pewne, istotne dla Zamawiającego, zbliżone do produktu referencyjnego cechy i parametry.

Istotne dla Zamawiającego cechy i parametry, to takie, które pozwolą zachować wszystkim systemom, urządzeniom, wyrobom, parametry i cechy pozwalające przede wszystkim na prawidłową współpracę z innymi systemami i/lub urządzeniami i/lub wyrobami w sposób założony przez Zamawiającego oraz pozwalające przy tym uzyskać parametry nie gorsze od założonych w niniejszym załączniku. Ciężar udowodnienia równoważności spoczywa na Wykonawcy

Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowany przedmiot zamówienia spełnia wymagania określone przez Zamawiającego poprzez złożenie opisu zaoferowanych produktów wraz z wykazaniem cech równoważności w stosunku do wymagań opisanych przez Zamawiającego w niniejszym załączniku oraz podanie nazwy handlowej i producenta.

W celu wykazania cech równoważności Zamawiający dopuszcza załączenie do opisu etykiet, zdjęć, kart katalogowych itp., z dopiskiem której pozycji asortymentowej (jakiego sprzętu) dotyczy dana informacja z zastrzeżeniem, że z tych dokumentów muszą wynikać parametry co najmniej określone przez Zamawiającego w załącznikach do OPZ i dane identyfikujące produkt.

**DOSTAWA INFRASTRUKTURY SPRZĘTOWEJ, OPROGRAMOWANIA ORAZ USŁUG – PAKIET NR 2**

Przedmiotem zamówienia jest łączne dostarczenie i wdrożenie rozwiązania zawierającego następujące elementy:

1. **Dostarczenie i wdrożenie rozwiązania do ochrony stacji roboczych wraz z mechanizmami centralnego zarządzania,**
2. **Dostarczenie i wdrożenie modułu realizującego funkcję serwera poczty**
3. **Dostarczenie i wdrożenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń**

Poniżej wyspecyfikowano minimalne parametry sprzętu, oprogramowania oraz usług, które należy dostarczyć i wdrożyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

**Wymagania ogólne:**

* Całość dostarczanego sprzętu i oprogramowania standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
* Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, musi być nowe, wcześniej nieużywane, rok produkcji nie starszy niż 2021.
* Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, w którym nie wskazano szczegółowych warunków gwarancji, musi być objęte minimum 12 miesięczną gwarancją jeśli w opisie parametrów nie wskazano inaczej
* Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
* Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
* Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
* Wszystkie urządzenia muszą posiadać oznakowanie CE.
* Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
* Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
* Wymagane jest, aby infrastruktura sprzętowa była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
* Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).

Zamawiający wymaga aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:

* posiadane środowisko domenowe,
* posiadaną konfigurację sieci wraz z wdrożoną w ramach postępowania segmentacją VLAN, oraz strefą DMZ,
* konfigurację stacji roboczych.

**Wymagania szczegółowe**:

* Szpital posiada urządzenie UTM FORTIGATE 300E wraz z aktualizacjami - Unified Threat Protection (UTP) (IPS, Advanced Malware Protection,  Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare) Zaproponowane rozwiązania muszą umożliwiać integrację z tym urządzeniem za pomocą „Fortinet Security Fabric”, które zapewni inteligentną architekturę, łączącą oddzielne rozwiązania zabezpieczające w zintegrowaną całość w celu wykrywania, monitorowania, blokowania i korygowania ataków na całej powierzchni ataku. Połączenia zaproponowanych rozwiązań z UTM FORTIGATE 300E, muszą być realizowane za pomocą „Fortinet Security Fabric” na poziomie „Core Network Security”
* W celu zapewnienia wysokiej jakości usług Wykonawca w celu wykonania instalacji i konfiguracji powinien dysponować co najmniej czterema inżynierami z certyfikatem NSE4 oraz minimum jednym inżynierem legitymującym się certyfikatem minimum NSE7.

**Opis parametrów minimalnych dostarczanej infrastruktury oraz oprogramowania.**

Wymagania dla Wykonawcy który dostarczy infrastrukturę sprzętową oraz oprogramowanie:

Zaproponowane rozwiązanie musi być rozwiązaniem całościowym, kompletnym zawierającym następujące elementy:

1. **Dostarczenie i wdrożenie rozwiązania do ochrony stacji roboczych wraz z mechanizmami centralnego zarządzania**
2. **Dostarczenie i wdrożenie modułu realizującego funkcję serwera poczty**
3. **Dostarczenie i wdrożenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń**

Zamawiający wymaga, aby Wykonawca spełniała wymagania w zakresie:

**Pkt 1. W zakresie dostarczenie i wdrożenia rozwiązania do ochrony stacji roboczych wraz z mechanizmami centralnego zarządzania:**

Przedmiotem postępowania jest rozbudowa istniejącego systemu bezpieczeństwa infrastruktury teleinformatycznej wraz z wdrożeniem o elementy zabezpieczeń dla stacji roboczych wraz z mechanizmami centralnego zarządzania.

Dostarczone rozwiązanie do ochrony stacji roboczych musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.

# Parametry systemu ochrony dla stacji roboczych.

1. Elementy systemu ochrony dla stacji roboczych powinny zapewniać następujące funkcje i mechanizmy:
* Kontrola antywirusowa.
* Funkcja analizy plików w zewnętrznym systemie Sandbox.
* Opcja kwarantanny lokalnej plików przesłanych do Sandbox na czas analizy.
* URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków.
* Kontrola aplikacji - w oparciu o wbudowany Firewall aplikacyjny.
* Mechanizmy analizy podatności na stacji roboczej - pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach.
* Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
* Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
* Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń.
* Mechanizmy uwierzytelniania dwuskładnikowego
* AntiExploit,
* blokowanie dysków przenośnych typu USB,
1. Poszczególne mechanizmy muszą być dostępne dla następujących systemów operacyjnych: Microsoft Windows 10 (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Windows 7 (32-bit, 64-bit),Windows Serwer 2019,Windows Server 2016, Windows Server 2008 R2, Windows Server 2012, 2012 R2, MacOS X v10.15, OS X v10.14, OS X v10.13, Linux OS, Ubuntu 16.04 i późniejsze, Red Hat 7.4 i późniejsze, CentOS 7.4 i późniejsze.
2. Wymaganym jest aby system ochrony stacji końcowej umożliwiał wysyłanie plików do platformy typu Sandbox zlokalizowanego w chmurze producenta (co najmniej w ilości 300 plików dziennie dla każdej stacji klienckiej) lub w ramach postępowania powinna zostać dostarczona komercyjna platforma typu sandbox - zainstalowana lokalnie i współpracująca z oferowanym rozwiązaniem do ochrony stacji roboczych. W ramach postępowania muszą zostać dostarczone niezbędne licencje upoważniająca zrealizowania wymaganej powyżej funkcji.

# Parametry systemu centralnego zarządzania.

1. Dostarczony system centralnego zarządzania aplikacjami klienckimi musi zapewniać wszystkie wymienione poniżej funkcje. Wymaga się aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych platform wirtualnych lub aplikacji instalowanych na systemach operacyjnych: Microsoft Windows Server 2019,Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2.
2. System powinien umożliwiać automatyczną aktualizację oprogramowania zabezpieczającego na urządzeniach końcowych oraz musi zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa, w tym co najmniej: Firewall, Sandbox.
3. Ponadto wymagane jest aby system zapewniał:
* integrację z systemami zarządzania tożsamością użytkowników – co najmniej AD,
* definiowanie różnych profilów (wersji konfiguracji) ochrony dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie,
* zautomatyzowany proces zarządzania aplikacja kliencką,
* przygotowywanie paczek instalacyjnych przynajmniej dla systemu Windows 32/64 bit i MacOS w których administrator może określić komponenty dla ochrony stacji roboczych takich jak AV, WebFiler, Skaner Podatności.
* możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym,
* panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych,
* panel w którym wyświetlane są informacje o podłączonych i zarządzanych stacjach roboczych,
* możliwość wymuszenia patchowania wykrytych podatności na stacjach roboczych,
* automatyczne wykrywanie stacji klienckich w grupach roboczych,
* logowanie zdarzeń z aplikacji klienckich, możliwość ich przeglądania z funkcja filtrów oraz możliwością pobierania logów przez administratora,
* generowanie alarmów: związanych z zarządzeniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach oraz w sytuacji zaistnienia zdarzeń związanych z aktywnością złośliwego kodu, aktywności aplikacji botnet z wykorzystaniem komunikacji C&C, nieaktualnej bazy danych dla sygnatur antywirusa.
* definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcja przypisywania uprawnień do elementów panelu konfiguracyjnego,
* zarządzenie certyfikatami na potrzeby połączeń IPSec VPN oraz SSL VPN,
* automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji,
* możliwość przeniesienia użytkownika przez administratora do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi,
* możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie,
* możliwość skonfigurowania weryfikacji zgodności (compliance) w celu sprawdzenia czy na stacji końcowej jest aktualna baza sygnatur dla AV, czy jest odpowiednia wersja systemu operacyjnego, czy jest uruchomiony odpowiedni proces.
1. Administrator musi mieć możliwość wykonywania backupu i odtwarzania bazy danych, w oparciu o którą działają elementy system.
2. Centralny system zarządzania musi zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach postępowania koniecznym jest dostarczenie i wdrożenie odpowiednio zabezpieczonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować paczki instalacyjne.

Licencje oraz serwisy.

W ramach postępowania wraz z konsolą centralnego zarządzania muszą zostać dostarczone niezbędne licencje upoważniające do:

1. Zainstalowania i centralnego zarządzania [300]aplikacjami klienckimi na stacjach roboczych.
2. Dla wskazanej powyżej ilości stacji roboczych licencje powinny obejmować:
3. Kontrola Aplikacji, Antywirus, Web Filtering, Skaner podatności, Software inventory, Remote Access,ThreatOutbreakDetection, Sandbox Agent with CloudSandboxsubscription, centralne zarządzaniena z licencją na [36] miesięcy.

System musi być objęty licencją przez okres [36] miesięcy.

**Pkt 2. W zakresie dostarczenie i wdrożenia modułu realizującego funkcję serwera poczty**

System ochrony poczty musi być wdrożony i musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym z trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

# **Parametry fizyczne systemu antyspamowego**

1. System musi być wyposażony w interfejsy:
* 4 porty Gigabit Ethernet RJ-45.
1. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB .
2. System musi posiadać wbudowany port konsoli szeregowej.
3. Zasilanie z sieci 230V/50Hz.

# **Funkcja serwera poczty**

W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 150 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.

# **Funkcje serwera poczty**

W tym zakresie dostarczony system musi zapewniać:

1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP.
2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1 oraz TLS 1.2).
3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.
4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3).
5. Polski interfejs użytkownika przy dostępie przez WebMail.
6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.
7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.

# **Ogólne funkcje systemu ochrony poczty**

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 28 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, antyspam, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail lub IMAP.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

# **Kontrola antywirusowa i ochrona przed malware**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.
10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.

# **Kontrola antyspamowa**

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level).
17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

# **Ochrona przed atakami na usługę poczty**

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

# **Funkcje logowania i raportowania**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

# **Funkcje pracy w trybie wysokiej dostępności (HA)**

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

# **Aktualizacje sygnatur, dostęp do bazy spamu**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

# **Zarządzanie**

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.

# **Certyfikaty**

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

# **Serwisy i licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu VirusOutbrake, Sandbox w chmurze, ochrona typu ClickProtect, Content Disarm&Reconstruction, Business Email Compromise na okres [36] miesięcy.

# **Gwarancja**

System musi być objęty serwisem gwarancyjnym producenta przez okres [36] miesięcy, oraz

musi być objęty rozszerzoną gwarancją udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [36] miesięcy.

Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty:

* Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
* Certyfikat ISO 9001 podmiotu serwisującego.

# **Pozostałe wymagania:**

Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

**Pkt. 3. W zakresie dostarczenie i wdrożenia centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń**

W ramach postępowania wymaganym jest dostarczenie i wdrożenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXiwerje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; CitrixXenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

# **Interfejsy, Dysk:**

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.

# **Parametry wydajnościowe:**

1. System musi być w stanie przyjmować minimum 15 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

# **Logowanie**

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.

b. Listę najbardziej aktywnych użytkowników.

c. Listę najczęściej wykorzystywanych aplikacji.

d. Listę najczęściej odwiedzanych stron www.

e. Listę krajów , do których nawiązywane są połączenia.

f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
2. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
3. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

# **Raportowanie**

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

# **Korelacja logów**

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System musi korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
* Malware.
* Aplikacje sieciowe.
* Email.
* IPS.
* Traffic.
* Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
1. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.

# **Zarządzanie**

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

1. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

# **Licencje**

1. System musi być objęty licencją przez okres 36 miesięcy.

# **Pozostałe wymagania:**

1. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.