

(Pieczęć firmy), dnia

Dane Wykonawcy

Nazwa:

.....

Siedziba:

Dane składającego oświadczenie:

Imię i nazwisko:

Sposób reprezentacji Wykonawcy: pełnomocnictwo / wpis w rejestrze lub ewidencji*

FORMULARZ TECHNICZNY PRZEDMIOTU ZAMÓWIENIA

**TABELA NR I - DOSTAWA SYSTEMU ELEKTRONICZNEGO POCZTY E-MAIL DLA DOMENY ITWL.PL,
WRAZ Z MECHANIZMAMI PODWÓJNEJ AUTENTYKACJI - 1 KPL.**

Wymagania szczegółowe dla przedmiotu zamówienia:

A Wymagania zamawiającego		B Wskazania wykonawcy	
<i>Charakterystyka i cechy funkcjonalne przedmiotu zamówienia.</i> Wymagania minimalne	<i>Ilość zamawiana</i>	<i>Specyfikacja oferowanego przedmiotu zamówienia</i> Parametry oferowanego sprzętu	<i>Ilość oferowana</i>
SYSTEM ELEKTRONICZNY POCZTY E-MAIL DLA DOMENY ITWL.PL, WRAZ Z MECHANIZMAMI PODWÓJNEJ AUTENTYKACJI	kpl. 1	 (nazwa, typ, producent)	 kpl.
SYSTEM			
1. Wymagania ogólne: System ochrony poczty 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 ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systemu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016,		1. Wymagania ogólne: System ochrony poczty zapewnia kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systemu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016,	

Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów: 1) Tryb Gateway. 2) Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).	Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie pracować będzie w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie posiada możliwość pracy w każdym trybów: 1) Tryb Gateway. TAK* / NIE * 2) Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej). TAK* / NIE *
2. Parametry fizyczne systemu antyspamowego 1) System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 2 TB.	2. Parametry fizyczne systemu antyspamowego 1) System obsługuje co najmniej 4 interfejsy sieciowe oraz wspiera powierzchnię dyskową o pojemności co najmniej 2 TB. TAK* / NIE *
3. Funkcja serwera poczty: W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 400 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługującym tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.	3. Funkcja serwera poczty: W ramach oferowanego systemu będzie dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 400 lokalnych skrzynek pocztowych. TAK* / NIE * Moduł serwera poczty będzie integrować się z serwerem LDAP obsługującym tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych. TAK* / NIE *
4. 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. Funkcje serwera poczty: W tym zakresie dostarczony system zapewnia: 1) Obsługę serwisów pocztowych: SMTP, POP3, IMAP. TAK* / NIE * 2) Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1 oraz TLS 1.2). TAK* / NIE * 3) Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników. TAK* / NIE *

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.	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). TAK* / NIE * 5) Polski interfejs użytkownika przy dostępie przez WebMail. TAK* / NIE * 6) Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP. TAK* / NIE * 7) Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP. TAK* / NIE *
5. Ogólne funkcje systemu ochrony poczty Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje: 1) Wsparcie dla co najmniej 70 domen pocztowych. 2) System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 50 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.	5. Ogólne funkcje systemu ochrony poczty Dostarczany system obsługi i ochrony poczty zapewnia poniższe funkcje: 1) Wsparcie dla co najmniej 70 domen pocztowych. TAK* / NIE * 2) System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 50 tys. wiadomości/godzinę. TAK* / NIE * 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). TAK* / NIE * 4) Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP. TAK* / NIE * 5) Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości). TAK* / NIE * 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. TAK* / NIE * 7) Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. TAK* / NIE *

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 (antyvirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. 12) Dostęp do kwarantanny użytkownika możliwy poprzez WebMail. 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) Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention). 18) Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.	8) Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. TAK* / NIE * 9) Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP. TAK* / NIE * 10) Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. TAK* / NIE * 11) Możliwość poddania ponownemu skanowaniu (antyvirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. TAK* / NIE * 12) Dostęp do kwarantanny użytkownika możliwy poprzez WebMail. TAK* / NIE * 13) Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. TAK* / NIE * 14) Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. TAK* / NIE * 15) Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. TAK* / NIE * 16) Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. TAK* / NIE * 17) Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention). TAK* / NIE * 18) Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika. TAK* / NIE *
--	--

6. 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 200 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.	6. Kontrola antywirusowa i ochrona przed malware: W tym zakresie dostarczony system ochrony poczty zapewnia: 1) Skanowanie antywirusowe wiadomości SMTP. TAK* / NIE * 2) Kwarantannę dla zainfekowanych plików. TAK* / NIE * 3) Skanowanie załączników skompresowanych. TAK* / NIE * 4) Definiowanie komunikatów powiadomień w języku polskim. TAK* / NIE * 5) Blokowanie załączników w oparciu o typ pliku. TAK* / NIE * 6) Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antywirusowej. TAK* / NIE * 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. TAK* / NIE * 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. TAK* / NIE * 9) Ochronę typu wirus outbrake. TAK* / NIE * 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. TAK* / NIE *
7. Kontrola antyspamowa System musi zapewniać poniższe funkcje i metody filtrowania spamu:	7. Kontrola antyspamowa System zapewnia 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 200 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	1) Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. TAK* / NIE * 2) Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. TAK* / NIE * 3) Szczegółowa kontrola nagłówka wiadomości. TAK* / NIE * 4) Analiza Heurystyczna. TAK* / NIE * 5) Współpraca z zewnętrznymi serwerami RBL, SURBL. TAK* / NIE * 6) Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen. TAK* / NIE * 7) Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników. TAK* / NIE * 8) Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF. TAK* / NIE * 9) Kontrola w oparciu o Greylisting oraz SPF. TAK* / NIE * 10) Filtrowanie treści wiadomości i załączników. TAK* / NIE * 11) Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. TAK* / NIE * 12) Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej. TAK* / NIE * 13) Ochrona typu outbrake. TAK* / NIE * 14) Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking). TAK* / NIE * 15) Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata. TAK* / NIE * 16) Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level) TAK* / NIE * 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.	spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. TAK* / NIE *
8. 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) Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. 4) Kontrola Reverse DNS (ochrona przed Anty-Spoofing). 5) Weryfikacja poprawności adresu e-mail nadawcy.	8. Ochrona przed atakami na usługę poczty System zapewnia poniższe funkcje i metody filtrowania: 1) Ochrona przed atakami na adres odbiorcy (m.in. email bombing). TAK* / NIE * 2) Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. TAK* / NIE * 3) Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. TAK* / NIE * 4) Kontrola Reverse DNS (ochrona przed Anty-Spoofing). TAK* / NIE * 5) Weryfikacja poprawności adresu e-mail nadawcy. TAK* / NIE *
9. 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	9. Funkcje logowania i raportowania W tym zakresie dostarczony system ochrony poczty zapewnia: 1) Logowanie do zewnętrznego serwera SYSLOG. TAK* / NIE * 2) Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. TAK* / NIE * 3) Logowanie informacji na temat spamu oraz niedozwolonych załączników. TAK* / NIE * 4) Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. TAK* / NIE * 5) Możliwość analizy przebiegu sesji SMTP. TAK* / NIE * 6) Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. TAK* / NIE * 7) Predefiniowane szablony raportów oraz możliwość ich edycji przez

administratora systemu. 8) Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.	administratora systemu. TAK* / NIE * 8) Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu. TAK* / NIE *
10. 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.	10. Funkcje pracy w trybie wysokiej dostępności (HA) System ochrony poczty zapewnia poniższe funkcje: 1) Konfigurację HA w każdym z trybów: gateway, transparent. TAK* / NIE * 2) Tryb synchronizacji konfiguracji dla scenariuszy, gdy każde z urządzeń występuje pod innym adresem IP. TAK* / NIE * 3) Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. TAK* / NIE * 4) Monitorowanie stanu pracy klastra. TAK* / NIE *
11. 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.	11. Aktualizacje sygnatur, dostęp do bazy spamu W tym zakresie dostarczony system ochrony poczty zapewnia: 1) Pracę w oparciu o bazę spamu oraz URL uaktualniane w czasie rzeczywistym. TAK* / NIE * 2) Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę. TAK* / NIE *
12. 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.	12. Zarządzanie System ochrony poczty zapewnia poniższe funkcje: 1) System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. TAK* / NIE * 2) Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy. TAK* / NIE *

3) Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.	3) Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych. TAK* / NIE *
13. Certyfikaty Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji: 1) VBSpam, 2) VB100 rated, 3) Common Criteria NDPP, 4) FIPS 140-2 Certified.	13. Certyfikaty Dostarczony system posiada co najmniej dwie z poniższych certyfikacji: 1) VBSpam, TAK* / NIE * 2) VB100 rated, TAK* / NIE * 3) Common Criteria NDPP, TAK* / NIE * 4) FIPS 140-2 Certified. TAK* / NIE *
14. Serwisy i licencje System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. 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 Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres minimum 60 miesięcy.	14. Serwisy i licencje System będzie dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. W ramach postępowania zostaną dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Obejmują one: 1) Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres minimum 60 miesięcy. TAK* / NIE *
15. Gwarancja oraz wsparcie 1) System musi być objęty serwisem producenta przez okres minimum 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz	15. Gwarancja oraz wsparcie 1) System będzie objęty serwisem producenta przez okres minimum 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz

wsparcia technicznego w trybie 24x7.	wsparcia technicznego w trybie 24x7. TAK* / NIE *
16. Opisy do wymagań ogólnych 1) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2023 poz. 1582) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.	16. Opisy do wymagań ogólnych 1) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca, przed realizacją zamówienia, winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2023 poz. 1582) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. TAK* / NIE * 2) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien <u>przedłożyć oświadczenie</u> producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. TAK* / NIE *
17. Dodatkowe wsparcie: Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego świadczone przez Producenta lub Autoryzowanego Dystrybutora Producenta świadczone w języku polskim w zakresie: 1) wsparcie telefoniczne zespołu certyfikowanych inżynierów,	17. Dodatkowe wsparcie: Do zamawianego sprzętu zapewniamy usługi wsparcia technicznego świadczone przez Producenta lub Autoryzowanego Dystrybutora Producenta świadczone w języku polskim w zakresie: 1) wsparcie telefoniczne zespołu certyfikowanych inżynierów, TAK* / NIE *

2) pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu, 3) doradztwo w zakresie konfiguracji, 4) zdalne wsparcie techniczne, 5) pomoc w zakładaniu zgłoszeń serwisowych u producenta, 6) pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą), 7) przygotowanie urządzenia do zdalnej konfiguracji, 8) zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika, 9) rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań klienta, 10) usługa upoważnia do maksymalnie 10 zdalnych zmian w konfiguracji. Dostęp do usługi świadczonej przez dedykowaną infolinię (należy podać numer telefonu) oraz przez dedykowany moduł internetowy (należy podać adres). Usługa ta ma być świadczona przez: ▪ podmiot posiadający certyfikat ISO 9001 w zakresie świadczenia usług serwisowych – podmiotu serwisującego; ▪ oświadczanie Producenta lub Autoryzowanego Dystrybutora o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001 oraz oświadczenie o posiadaniu minimum 4 certyfikowanych inżynierów w zakresie oferowanego rozwiązania.	2) pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu, TAK* / NIE * 3) doradztwo w zakresie konfiguracji, TAK* / NIE * 4) zdalne wsparcie techniczne, TAK* / NIE * 5) pomoc w zakładaniu zgłoszeń serwisowych u producenta, TAK* / NIE * 6) pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą), TAK* / NIE * 7) przygotowanie urządzenia do zdalnej konfiguracji, TAK* / NIE * 8) zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika, TAK* / NIE * 9) rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań klienta, TAK* / NIE * 10) usługa upoważnia do maksymalnie 10 zdalnych zmian w konfiguracji. TAK* / NIE * Dostęp do usługi świadczonej przez dedykowaną infolinię (należy podać numer telefonu) oraz przez dedykowany moduł internetowy (należy podać adres) TAK* / NIE * Usługa ta będzie świadczona przez: ▪ podmiot posiadający certyfikat ISO 9001 w zakresie świadczenia usług serwisowych – podmiotu serwisującego; TAK* / NIE * ▪ oświadczanie Producenta lub Autoryzowanego Dystrybutora o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001; TAK* / NIE * oraz oświadczenie o posiadaniu minimum 4 certyfikowanych inżynierów w zakresie oferowanego rozwiązania: TAK* / NIE *
--	--

18. Zakres wdrożenia:

Zakres usług wchodzących w skład instalacji i konfiguracji urządzenia onsite:

- 1) Relokacji urządzeń w szafie rackowej klienta w celu zapewnienia miejsca do instalacji urządzenia.
- 2) Instalacja sprzętu w szafie 19".
- 3) Podłączenie zasilania do urządzenia.
- 4) Podłączenie okablowania strukturalnego do urządzenia.
- 5) Porządkowania okablowania strukturalnego klienta.
- 6) Uruchomienie urządzenia.
- 7) Rejestracja urządzenia na stronie producenta.
- 8) Aktualizacja oprogramowania.
- 9) Zmiana domyślnych haseł.
- 10) Podanie klientowi parametrów do dokonania koniecznych zmian środowiska (zmiany DNS, przekierowania portów, konfiguracja łączników mail na obecnym systemie poczty).
- 11) Konfiguracja urządzenia / maszyny wirtualnej w trybie Gateway / Serwer.
- 12) Konfiguracja urządzenia / maszyny wirtualnej (Hostname, serwery DNS, Adres IP, Serwery strefy czasowej i serwerów synchronizacji czasu).
- 13) Konfiguracja zabezpieczanych domen (max.1).
- 14) Konfiguracja polityk Access Control (poczta przychodząca/wychodząca, zabezpieczenie przed OpenRelay).
- 15) Konfiguracja polityk Recipient dla domyślnej domeny.
- 16) Konfiguracja profili bezpieczeństwa (Session, AntiSpam, Antivirus) na zalecanych ustawieniach.
- 17) W trybie serwer utworzenie do 5 użytkowników poczty.
- 18) Zmiany na środowisku klienta (zmiany DNS, przekierowania portów,

18. Zakres wdrożenia:

Zakres usług wchodzących w skład instalacji i konfiguracji urządzenia onsite:

- 1) Relokacji urządzeń w szafie rackowej klienta w celu zapewnienia miejsca do instalacji urządzenia. **TAK* / NIE ***
- 2) Instalacja sprzętu w szafie 19". **TAK* / NIE ***
- 3) Podłączenie zasilania do urządzenia. **TAK* / NIE ***
- 4) Podłączenie okablowania strukturalnego do urządzenia. **TAK* / NIE ***
- 5) Porządkowania okablowania strukturalnego klienta. **TAK* / NIE ***
- 6) Uruchomienie urządzenia. **TAK* / NIE ***
- 7) Rejestracja urządzenia na stronie producenta. **TAK* / NIE ***
- 8) Aktualizacja oprogramowania. **TAK* / NIE ***
- 9) Zmiana domyślnych haseł. **TAK* / NIE ***
- 10) Podanie klientowi parametrów do dokonania koniecznych zmian środowiska (zmiany DNS, przekierowania portów, konfiguracja łączników mail na obecnym systemie poczty). **TAK* / NIE ***
- 11) Konfiguracja urządzenia / maszyny wirtualnej w trybie Gateway / Serwer. **TAK* / NIE ***
- 12) Konfiguracja urządzenia / maszyny wirtualnej (Hostname, serwery DNS, Adres IP, Serwery strefy czasowej i serwerów synchronizacji czasu). **TAK* / NIE ***
- 13) Konfiguracja zabezpieczanych domen (max.1). **TAK* / NIE ***
- 14) Konfiguracja polityk Access Control (poczta przychodząca /wychodząca, zabezpieczenie przed OpenRelay). **TAK* / NIE ***
- 15) Konfiguracja polityk Recipient dla domyślnej domeny. **TAK* / NIE ***
- 16) Konfiguracja profili bezpieczeństwa (Session, AntiSpam, Antivirus) na zalecanych ustawieniach. **TAK* / NIE ***
- 17) W trybie serwer utworzenie do 5 użytkowników poczty. **TAK* / NIE ***
- 18) Zmiany na środowisku klienta (zmiany DNS, przekierowania portów,

konfiguracja łączników mail na obecnym systemie poczty). 19) Konfiguracji połączenia z serwerem autoryzacji LDAP/RADIUS. 20) Konfiguracji Książki Adresowej. 21) Konfiguracji Kalendarza. 22) Zmian w standardowych komunikatach. 23) Konfiguracji używania wielu portów LAN. 24) Konfiguracji DLP i Content Inspection. 25) Konfiguracji szyfrowania wiadomości wychodzących IBE. 26) Konfiguracji dodatkowych łączników do zewnętrznych serwerów poczty. 27) Konfiguracji i integracji z FortiSandbox. 28) Przygotowania certyfikatów SSL dla nazw FortiMail. 29) W trybie Serwer nie wystawiamy WebMails na publicznym adresie IP (Dostęp wewnętrzny będzie działać).	konfiguracja łączników mail na obecnym systemie poczty). TAK* / NIE * 19) Konfiguracji połączenia z serwerem autoryzacji LDAP/RADIUS. TAK* / NIE * 20) Konfiguracji Książki Adresowej. TAK* / NIE * 21) Konfiguracji Kalendarza. TAK* / NIE * 22) Zmian w standardowych komunikatach. TAK* / NIE * 23) Konfiguracji używania wielu portów LAN. TAK* / NIE * 24) Konfiguracji DLP i Content Inspection. TAK* / NIE * 25) Konfiguracji szyfrowania wiadomości wychodzących IBE. TAK* / NIE * 26) Konfiguracji dodatkowych łączników do zewnętrznych serwerów poczty. TAK* / NIE * 27) Konfiguracji i integracji z FortiSandbox. TAK* / NIE * 28) Przygotowania certyfikatów SSL dla nazw FortiMail. TAK* / NIE * 29) W trybie Serwer nie wystawiamy WebMails na publicznym adresie IP (Dostęp wewnętrzny będzie działać). TAK* / NIE *
POCZTA	
	 (nazwa, typ, producent)
1. System uwierzytelniania, autoryzacji i kontroli dostępu Oferowane rozwiązanie musi pozwalać na centralne zarządzanie kontami użytkowników oraz procesem uwierzytelnienia - w tym celu musi zapewniać wszystkie wymienione poniżej funkcje. Dopuszcza się aby poszczególne elementy wchodzące w skład	1. System uwierzytelniania, autoryzacji i kontroli dostępu Oferowane rozwiązanie pozwala na centralne zarządzanie kontami użytkowników oraz procesem uwierzytelnienia - w tym celu zapewnia wszystkie wymienione poniżej funkcje. TAK* / NIE * Poszczególne elementy wchodzące w skład systemu były

systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne, odpowiednio zabezpieczone systemy operacyjne dla poszczególnych komponentów.	zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. TAK* / NIE * W przypadku implementacji programowej zapewniamy niezbędne, odpowiednio zabezpieczone systemy operacyjne dla poszczególnych komponentów. TAK* / NIE *
2. Parametry systemu Poszczególne elementy wchodzące w skład systemu muszą zapewniać obsługę: 1) 4 wirtualnych interfejsów sieciowych. 2) Możliwość uruchomienia w środowiskach: Microsoft Hyper-V Server 2010, 2012 R2 oraz 2016; VMware ESXi, ESX wersje:4,5,6; KVM, Xen, Microsoft Azure, AWS, Oracle OCI.	2. Parametry systemu Poszczególne elementy wchodzące w skład systemu zapewniają obsługę: 1) 4 wirtualnych interfejsów sieciowych. TAK* / NIE * 2) Możliwość uruchomienia w środowiskach: Microsoft Hyper-V Server 2010, 2012 R2 oraz 2016; VMware ESXi, ESX wersje:4,5,6; KVM, Xen, Microsoft Azure, AWS, Oracle OCI. TAK* / NIE *
3. Parametry wydajnościowe i licencyjne System musi obsługiwać co najmniej: 1) Uwierzytelnianie dla 1000 użytkowników. 2) 2000 tokenów dla uwierzytelniania dwuskładnikowego. 3) 300 klientów protokołu RADIUS (urządzeń NAS, które można podpiąć do systemu). 4) Możliwość zdefiniowania co najmniej 100 grup użytkowników, 5) 50 lokalnych centrów certyfikacji (CA). 6) Możliwość wygenerowania 4 tys. certyfikatów dla użytkowników.	3. Parametry wydajnościowe i licencyjne System obsługuje co najmniej: 1) Uwierzytelnianie dla 1000 użytkowników. TAK* / NIE * 2) 2000 tokenów dla uwierzytelniania dwuskładnikowego. TAK* / NIE * 3) 300 klientów protokołu RADIUS (urządzeń NAS, które można podpiąć do systemu). TAK* / NIE * 4) Możliwość zdefiniowania co najmniej 100 grup użytkowników. TAK* / NIE * 5) 50 lokalnych centrów certyfikacji (CA). TAK* / NIE * 6) Możliwość wygenerowania 4 tys. certyfikatów dla użytkowników. TAK* / NIE *
4. Wymagania ogólne	4. Wymagania ogólne

System musi zapewniać nie mniej niż: 1) Możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności. 2) Graficzną reprezentację statusu uwierzytelnionych użytkowników. 3) Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia oraz nazwą użytkownika: a) Lokalnie. b) Zdalnie w oparciu o protokół Syslog. 4) Konfigurację Captive Portalu.	System zapewnia nie mniej niż: 1) Możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności. TAK* / NIE * 2) Graficzną reprezentację statusu uwierzytelnionych użytkowników. TAK* / NIE * 3) Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia oraz nazwą użytkownika: a) Lokalnie. TAK* / NIE * b) Zdalnie w oparciu o protokół Syslog. TAK* / NIE * 4) Konfigurację Captive Portalu. TAK* / NIE *
5. Wymagania funkcjonalne - uwierzytelnianie Celem realizacji funkcji uwierzytelniających, system musi zapewniać nie mniej niż: 1) Lokalną, wbudowaną bazę użytkowników. 2) Przechowywanie następujących informacji o użytkowniku: nazwa, imię i nazwisko, adres email, numer telefonu, adres, kraj, województwo. 3) Możliwość zdefiniowania co najmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników. 4) Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV. 5) Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie: a) poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych), b) czasu ważności hasła,	5. Wymagania funkcjonalne - uwierzytelnianie Celem realizacji funkcji uwierzytelniających, system zapewnia nie mniej niż: 1) Lokalną, wbudowaną bazę użytkowników. TAK* / NIE * 2) Przechowywanie następujących informacji o użytkowniku: nazwa, imię i nazwisko, adres email, numer telefonu, adres, kraj, województwo. TAK* / NIE * 3) Możliwość zdefiniowania co najmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników. TAK* / NIE * 4) Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV. TAK* / NIE * 5) Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie: a) poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych), TAK* / NIE * b) czasu ważności hasła, TAK* / NIE *

6) Konfigurowalną politykę blokowania kont, która będzie uwzględniać: a) ilość nieudanych logowań, b) czas blokowania konta, c) okres nieaktywności, po którym konto jest blokowane. 7) Możliwość odzyskiwania haseł: a) z wykorzystaniem adresu email, b) z wykorzystaniem pytania pomocniczego. 8) Obsługę protokołu RADIUS zgodną z RFC, w tym zakresie system musi oferować: a) wbudowany serwer RADIUS, b) integrację z zewnętrznymi serwerami RADIUS - praca jako klient. 9) Obsługę protokołu LDAP, w tym zakresie system musi oferować: a) wbudowany serwer LDAP, b) możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP). 10) Obsługę protokołu SAML - Identity Provider (IdP) proxy. 11) Realizację funkcji SSO (Single Sign On) w oparciu o: a) integrację z Active Directory, również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny, b) dedykowaną aplikację instalowaną na stacjach roboczych z systemem Windows, c) kontekst użytkownika przesyłany z serwera RADIUS, d) informacje uzyskiwane poprzez protokół Syslog,	6) Konfigurowalną politykę blokowania kont, która będzie uwzględniać: a) ilość nieudanych logowań, TAK* / NIE * b) czas blokowania konta, TAK* / NIE * c) okres nieaktywności, po którym konto jest blokowane. TAK* / NIE * 7) Możliwość odzyskiwania haseł: a) z wykorzystaniem adresu email, TAK* / NIE * b) z wykorzystaniem pytania pomocniczego. TAK* / NIE * 8) Obsługę protokołu RADIUS zgodną z RFC, w tym zakresie system oferuje: a) wbudowany serwer RADIUS, TAK* / NIE * b) integrację z zewnętrznymi serwerami RADIUS - praca jako klient. TAK* / NIE * 9) Obsługę protokołu LDAP, w tym zakresie system musi oferować: a) wbudowany serwer LDAP, TAK* / NIE * b) możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP). TAK* / NIE * 10) Obsługę protokołu SAML - Identity Provider (IdP) proxy. TAK* / NIE * 11) Realizację funkcji SSO (Single Sign On) w oparciu o: a) integrację z Active Directory, również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny, TAK* / NIE * b) dedykowaną aplikację instalowaną na stacjach roboczych z systemem Windows, TAK* / NIE * c) kontekst użytkownika przesyłany z serwera RADIUS, TAK* / NIE * d) informacje uzyskiwane poprzez protokół Syslog, TAK* / NIE *
6. Wymagania funkcjonalne - uwierzytelnianie dwuskładnikowe Realizując uwierzytelnianie dwuskładnikowe, system musi zapewniać nie	6. Wymagania funkcjonalne - uwierzytelnianie dwuskładnikowe Realizując uwierzytelnianie dwuskładnikowe, system zapewnia nie mniej

mniej niż: 1) Obsługę dla tokenów sprzętowych (hardware): a) wspomniane tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania. 2) Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile. 3) Dla tokenów na system iOS i Android wymaga się: a) aktywacji z centralnego systemu uwierzytelniania (seed provisioning), b) możliwości konfiguracji ilości generowanych cyfr (6 lub 8), c) generowania kodu (cyfr) co 30 lub 60 sekund, d) możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), e) ochrony dostępu poprzez konfigurowalny kod PIN,	niż: 1) Obsługę dla tokenów sprzętowych (hardware): a) wspomniane tokeny pochodzą od tego samego producenta co system uwierzytelniania. TAK* / NIE * 2) Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile. TAK* / NIE * 3) Dla tokenów na system iOS i Android: a) aktywacja z centralnego systemu uwierzytelniania (seed provisioning), TAK* / NIE * b) możliwość konfiguracji ilości generowanych cyfr (6 lub 8), TAK* / NIE * c) generowanie kodu (cyfr) co 30 lub 60 sekund, TAK* / NIE * d) możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), TAK* / NIE * e) ochrony dostępu poprzez konfigurowalny kod PIN, TAK* / NIE *
7. Możliwość integracji z logowaniem do systemu Windows. Wymagania funkcjonalne - 802.1x System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki: 1) Obsługa co najmniej poniższych protokołów EAP: a) PEAP, b) EAP-TTLS, c) EAP-TLS, d) EAP-GTC. 2) Wsparcie dla uwierzytelnienia w oparciu o adres MAC (MAC based authentication).	7. Możliwość integracji z logowaniem do systemu Windows. Wymagania funkcjonalne - 802.1x System umożliwia realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki: 1) Obsługa co najmniej poniższych protokołów EAP: a) PEAP, TAK* / NIE * b) EAP-TTLS, TAK* / NIE * c) EAP-TLS, TAK* / NIE * d) EAP-GTC. TAK* / NIE * 2) Wsparcie dla uwierzytelnienia w oparciu o adres MAC (MAC based authentication). TAK* / NIE *

3) Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTLS, TLS.	3) Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTLS, TLS. TAK* / NIE *
8. Wymagania funkcjonalne - zarządzanie certyfikatami System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż: 1) Obsługa wbudowanego CA (Certificate Authority). 2) Obsługa CA pośredniczących (Intermediate CA). 3) Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego. 4) Możliwość pobrania wygenerowanych certyfikatów. 5) Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP. 6) Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP. 7) Możliwość generowania certyfikatów typu wildcard. 8) Realizacja CRL (Certificate Revocation List). 9) Wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560). 10) Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.	8. Wymagania funkcjonalne - zarządzanie certyfikatami System spełnia następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż: 1) Obsługa wbudowanego CA (Certificate Authority). TAK* / NIE * 2) Obsługa CA pośredniczących (Intermediate CA). TAK* / NIE * 3) Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego. TAK* / NIE * 4) Możliwość pobrania wygenerowanych certyfikatów. TAK* / NIE * 5) Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP. TAK* / NIE * 6) Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP. TAK* / NIE * 7) Możliwość generowania certyfikatów typu wildcard. TAK* / NIE * 8) Realizacja CRL (Certificate Revocation List). TAK* / NIE * 9) Wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560). TAK* / NIE * 10) Istnieje możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych. TAK* / NIE *
9. Zarządzanie 1) Zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki. 2) System udostępnia graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS. 3) Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego	9. Zarządzanie 1) Zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki. TAK* / NIE * 2) System udostępnia graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS. TAK* / NIE * 3) Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego

interfejsu zarządzającego (GUI) oraz na zewnętrzny serwer FTP/SFTP w oparciu o harmonogram, który będzie umożliwiał wskazanie konkretnego czasu kiedy proces ma się rozpocząć. 4) Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.	interfejsu zarządzającego (GUI) oraz na zewnętrzny serwer FTP/SFTP w oparciu o harmonogram, który będzie umożliwiał wskazanie konkretnego czasu kiedy proces ma się rozpocząć. TAK* / NIE * 4) Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych. TAK* / NIE *
10. Serwis, szkolenia i usługi Wymaga się aby dostawa obejmowała również serwis producenta przez okres minimum 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.	10. Serwis, szkolenia i usługi Wymaga się aby dostawa obejmowała również serwis producenta przez okres minimum 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. TAK* / NIE *
11. Opisy do wymagań ogólnych. 1) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2023 poz. 1582) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system	11. Opisy do wymagań ogólnych. 1) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca, przed realizacją zamówienia, winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2023 poz. 1582) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny

kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.	system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. TAK* / NIE * 2) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. TAK* / NIE *
POZOSTAŁE	
1. Serwis gwarancyjny: 1) Wymagany jest serwis gwarancyjny dla Systemu świadczony przez minimum 60 miesięcy. 2) Wykonawca zapewni bezpośredni dostęp do Centrum serwisowego producenta rozwiązania poprzez: email, web, telefon. 3) Wykonawca przystąpi do napraw gwarancyjnych przedmiotu zamówienia niezwłocznie (maksymalnie w ciągu 24 godz.) licząc od dnia zgłoszenia przez Zamawiającego. 4) Dostępność serwisu 24 godz. na dobę przez 7 dni w tygodniu przez 365 dni w roku. 5) Serwis zapewnia wsparcie w zakresie rozwiązywania problemów ze sprzętem i oprogramowaniem systemu. 6) Wymiana uszkodzonych podzespołów – NBD od momentu potwierdzenia usterki.	1. Serwis gwarancyjny: 1) Serwis gwarancyjny dla Systemu świadczony przez minimum 60 miesięcy. TAK* / NIE * 2) Zapewniamy bezpośredni dostęp do Centrum serwisowego producenta rozwiązania poprzez: email, web, telefon. TAK* / NIE * 3) Przystąpimy do napraw gwarancyjnych przedmiotu zamówienia niezwłocznie (maksymalnie w ciągu 24 godz.) licząc od dnia zgłoszenia przez Zamawiającego. TAK* / NIE * 4) Dostępność serwisu 24 godz. na dobę przez 7 dni w tygodniu przez 365 dni w roku. TAK* / NIE * 5) Serwis zapewnia wsparcie w zakresie rozwiązywania problemów ze sprzętem i oprogramowaniem systemu. TAK* / NIE * 6) Wymiana uszkodzonych podzespołów – NBD od momentu potwierdzenia usterki. TAK* / NIE *

7) Wykonawca zapewni dostęp do poprawek (patch, hotfix, update) i nowych wersji oprogramowania (upgrade) w ramach wykupionego serwisu gwarancyjnego przez okres minimum 5 lat.	7) Zapewniamy dostęp do poprawek (patch, hotfix, update) i nowych wersji oprogramowania (upgrade) w ramach wykupionego serwisu gwarancyjnego przez okres minimum 5 lat. TAK* / NIE *
2. Usługi wdrożeniowe: 1) Wykonawca przeprowadzi fizyczną instalację urządzeń w miejscu wskazanym przez Zamawiającego. 2) Wykonawca wykona pełną konfigurację systemu.	2. Usługi wdrożeniowe: 1) Przeprowadzimy fizyczną instalację urządzeń w miejscu wskazanym przez Zamawiającego. TAK* / NIE * 2) Wykonamy pełną konfigurację systemu. TAK* / NIE *
3. Pozostałe: Zamawiający wymaga aby dostarczone rozwiązanie było w pełni kompletne, jeżeli do spełnienia wymagań, wymagane są dodatkowe licencje lub komponenty należy je dostarczyć.	3. Pozostałe: Dostarczone rozwiązanie będzie w pełni kompletne, jeżeli do spełnienia wymagań, wymagane są dodatkowe licencje lub komponenty zostaną dostarczone. TAK* / NIE *

Oświadczam/my, że oferowane przedmioty pochodzą z bieżącej produkcji 2025 roku.*

Dokument należy złożyć w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym przez osobę uprawnioną.

UWAGA!

Wykonawca obowiązany jest, w kolumnie B „Specyfikacji oferowanego przedmiotu zamówienia”, wpisać oferowany przedmiot zamówienia poprzez jednoznaczne określenie jego nazwy, typu oraz producenta (oferowanego sprzętu) oraz dokładnie opisać jego parametry techniczne, cechy funkcjonalne lub charakterystykę w odniesieniu do pozycji wskazanych w kolumnie A.

TAK* / NIE* * niepotrzebne skreślić / wypełnić właściwe