Załącznik nr 1 do SWZ
Nr postępowania:368/2023/PN/DZP

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Przedmiotem zamówienia jest dostawa systemu bezpieczeństwa opartego na sprzętowych zabezpieczeniach sieciowych typu Next Generation Firewall (NGFW) wraz z subskrypcjami, wsparciem technicznym i wdrożeniem systemu oraz przeprowadzeniem warsztatów szkoleniowych.
Osiągnięcie przez System bezpieczeństwa odpowiedniej funkcjonalności wymaga spełnienia warunków określonych w Opisie Przedmiotu Zamówienia, w tym dotyczy to także komponentów sprzętowych wchodzących w skład systemu. Zamawiający nie może ponosić dodatkowych kosztów związanych z przedmiotem zamówienia dlatego też jeżeli są wymagane dodatkowe elementy do jego realizacji w tym np. licencje, subskrypcje, patchordy, itp. Termin gwarancji oraz realizacja wsparcia technicznego i licencji na niezbędne do funkcjonowania elementy jest wyznaczona przez zamawiającego na okres min.12 miesięcy od daty odbioru.
Wykonawca musi przeprowadzić wdrożenie systemu i jego integracje z obecnymi systemami a także dostarczyć dokumentacje powykonawczą z wykonanych czynności w tym także przeprowadzić warsztaty szkoleniowe, których plan warunki są opisane w punkcie IV.

Termin realizacji zamówienia – do 10 tygodni od daty podpisania umowy.

Komponenty, które należy dostarczyć w tym zamówieniu oraz elementy zawierające się w nich wymienione są w tabeli poniżej:

LP	Nazwa komponentu	Element komponentu
1	Komponent zabezpieczający	Dwa jednakowe urządzenie sprzętowe Next Generation Firewall (NGFW) połączone w klaster wysokiej dostępności (HA)
		Wkładki/moduły światłowodowe
		Urządzenie sandbox oraz inspekcji SSL/TLS (o ile będzie to konieczne do spełnienia wymagań Zamawiającego)
2	Wdrożenie wraz z dokumentacją	Zamawiający wymaga wykonania wdrożenia systemu pod kontrolą administratorów oraz wykonania z tych czynności dokumentacji powykonawczej, zawierającej informacje dotyczące procesu instalacji jak i z wdrożenia, które powinno zawierać wszystkie niezbędne informacje jakie mogą posłużyć ponownemu uruchomieniu systemu, w tym opisać miejsce instalacji, dokonać oznaczeń zgodnych z zastosowanym systemem wewnątrz uczelnianych urządzeń i systemów. Dokumentacja powinna zostać stworzona w 2 egz. w formie papierowej oraz w formie elektronicznej w postaci pliku, powinna zawierać pliki konfiguracyjne oraz opisy poszczególnych czynności które należy wykonać aby spełnić wcześniejsze zapisy odnośnie odtworzenia systemu.
3	Warsztaty szkoleniowe	Opisane w punkcie IV
4	Komponent zarządczy	Urządzenia konsoli zarządzającej pracujące w modelu redundantnym (o ile będzie to konieczne do spełnienia wymagań Zamawiającego)

		Licencja na system obsługujący aplikację łączącą się z konsolą zarządzającą z możliwością pracy zdalnej 10 osób. (o ile będzie to konieczne do spełnienia wymagań Zamawiającego)

I. Szczegółowe wymagania dotyczące systemu zabezpieczeń

1. Wszystkie elementy oferowanego zaawansowanego urządzenia do zabezpieczenia sieci teleinformatycznej muszą pochodzić z oficjalnych kanałów dystrybucyjnych producenta obejmujących także Unię Europejską, muszą dopuszczone do obrotu, spełniać normy CE (jeśli dotyczą).
2. Wszystkie elementy oferowanego zaawansowanego urządzenia do zabezpieczenia sieci teleinformatycznej muszą być dostępne w ofercie produktowej producenta aktualnej na dzień złożenia oferty oraz nie mogą być przeznaczone do wycofania z produkcji, sprzedaży bądź wsparcia (end-of-life, end-of-sale, end-of-support).
3. W momencie oferowania wszystkie elementy oferowanego zaawansowanego urządzenia do zabezpieczenia sieci teleinformatycznej muszą być dostępne (dostarczane) przez producenta.
4. Urządzenia i ich komponenty oferowanego zaawansowanego urządzenia do zabezpieczenia sieci teleinformatycznej muszą być oznakowane przez producentów w taki sposób, żeby była możliwa identyfikacja zarówno produktu jak i producenta. Muszą także być dostarczone w oryginalnych opakowaniach fabrycznych producenta a także zawierać komplet standardowej dokumentacji technicznej.
5. Wszystkie elementy oferowanego zaawansowanego urządzenia do zabezpieczenia sieci teleinformatycznej muszą być dostarczone z najnowszą (na dzień złożenia oferty) wersją oprogramowania systemowego (firmware) lub z wersją oprogramowania rekomendowaną przez producenta oferowanego rozwiązania. Jeżeli urządzenia są fabrycznie wysyłane z inną wersją oprogramowania to Wykonawca zobowiązany jest do dostarczenia wersji najnowszej lub wersji rekomendowanej przez producenta (na nośniku, poprzez wskazanie jej lokalizacji w portalu producenta z możliwością jej pobrania lub też poprzez pobranie jej bezpośrednio na urządzenie, itp.).
6. W przypadku wymiany nośników danych, które uległy awarii, uszkodzone nośniki muszą pozostać w całości u Zamawiającego. Nie przewiduje się opcji demontażu nośników danych i pozostawienia u Zamawiającego fragmentów nośników z danymi, np. talerzy dysków.
7. Urządzenia składające się na oferowany produkt muszą być wyposażone w redundantne zasilacze typu AC z możliwością wymiany hot-swap.
8. Urządzenia składające się na oferowany podsystem zabezpieczeń muszą przewidywać redundancję zasilania z zachowaniem następujących cech:
   a) awaria połowy zasilaczy zainstalowanych w urządzeniu nie może wpływać na działanie urządzenia;
   b) awaria lub wyłączenie połowy przyłączy elektrycznych dołączonych do zasilaczy urządzenia nie wpływa na działanie urządzenia;
   c) wymiana zasilacza, kabli zasilających musi być możliwa przy włączonym urządzeniu i nie może wpływać na jego działanie.
9. Urządzenia muszą być przystosowane do montażu w szafie Rack 19” oraz dostarczone wraz z szynami montażowymi i okablowaniem zasilającym i działać przy zasilaniu z jednej fazy 230V/50Hz z sieci elektrycznej.

II. Specyfikacja komponentu zabezpieczającego

1. Komponent zabezpieczający musi składać się z dwóch jednakowych sprzętowych rozwiązań Next Generation Firewall (NGFW) połączonych w klaster wysokiej dostępności (HA) oraz ewentualny

dodatkowy element (również w konfiguracji wysokiej wydajności) realizujący funkcje inspekcji SSS/TLS (o ile ta funkcja nie jest zawarta w samym urządzeniu).

2. Urządzenia muszą pochodzić od jednego producenta, jednak Zamawiający dopuszcza aby okablowanie, wkładki optyczne oraz ewentualne dodatkowe elementy pochodziły od innego producenta.
3. System musi pozwalać na import reguł zgodnych z rozwiązaniami SNORT i/lub Suricata do modułów systemu wykrywania i zapobiegania włamaniom komponentu zabezpieczającego.
4. Wszystkie wymienione poniżej funkcje muszą być dostępne jednocześnie. Nie jest dopuszczalne, aby realizacja jakiejkolwiek funkcjonalności powodowała konieczność przełączenia urządzenia w osobny tryb pracy, który będzie powodował niedostępność lub ograniczenie zakresu działania jakiejkolwiek innej funkcji wymaganej przez Zamawiającego. Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do złożenia wyjaśnień oraz prezentacji działania zaoferowanego urządzenia w przypadku powzięcia wątpliwości w tym zakresie.
5. Element zabezpieczający sieć musi być dostarczony jako dwa jednakowe, dedykowane urządzenia typu appliance. Zamawiający wymaga, aby zaoferowane urządzenia NGFW pochodziły z najnowszej dostępnej serii/linii/modelu producenta.
6. Każde z urządzeń NGFW wchodzące w skład komponentu zabezpieczającego musi być wyposażone w:
   a) minimum 20 interfejsów o przepustowości min. 10 Gbps (10 Gigabit Ethernet) każdy, obsługujące moduły optyczne SFP+ , min. 16 z nich działające jako interfejsy SFP+ i minimum 4 działające jako interfejsy RJ45, które mogą być uzyskane poprzez zastosowanie odpowiednich wkładek
   b) minimum 4 interfejsy o przepustowości minimum 100 Gbps (100 Gigabit Ethernet) każdy, obsługujące moduły optyczne QSFP28
   c) interfejsy potrzebne .
   d) co najmniej 2 dyski o pojemności nie mniejszej niż 480GB działającą w RAID-1, przeznaczoną na system operacyjny oraz dzienniki zdarzeń (logi).
7. Wszystkie interfejsy zainstalowane w urządzeniach muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanych urządzeniach.
8. Dla komponentu zabezpieczającego muszą zostać dostarczone dla każdego urządzenia NGFW:
   a) wkładki światłowodowe SFP+ jednomodowe w ilości co najmniej 16 sztuk i zasięgu transmisji nie mniejszym niż 10 km ze złączem LC,
   b) wkładki światłowodowe QSFP28 jednomodowe w ilości co najmniej 4 sztuki i zasięgu transmisji nie mniejszym niż 10 km ze złączem LC,
   c) niezbędna liczba wkładek światłowodowych, jednomodowych do interfejsów koniecznych do połączenia urządzeń w klaster z najwyższą możliwą przepustowością dla tych interfejsów również na dystansie 10 km.
9. Ponadto wymagane jest obsadzenie wkładkami optycznymi wszystkich dostępnych interfejsów optycznych w każdym urządzeniu NGFW, tak aby interfejsy pracowały z maksymalną możliwą przepustowością i obsługiwały transmisję jednomodową o zasięgu transmisji nie mniejszej niż 10 km oraz były ze złączem LC.
10. System musi spełniać co najmniej następujące parametry wydajnościowe w odniesieniu do pojedynczego urządzenia NGFW:
    a) minimum 45 Gbps przepustowości (ang. throughput) dla ruchu rzeczywistego z włączoną kontrolą aplikacji, włączonym logowaniem
    b) minimum 22 Gbps przepustowości (ang. throughput) dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (Firewall, IPS, antywirus, anty-spyware, współpraca z sandboxem, kontrola aplikacji, włączone logowanie),
    c) minimum 230 tys. nowych połączeń na sekundę,
    d) minimum 3 000 000 równoległych sesji.

Wszystkie parametry dotyczące wydajności, pod kątem przepustowości (ang. throughput), wymaganej na komponencie zabezpieczającym zakładają, iż będą to parametry wskazane przez producentów w kartach katalogowych jako HTTP 64K (lub HTTP dla mniejszych sesji np. HTTP 44K, HTTP 40K).

11. Urządzenie zabezpieczające (komponent) musi umożliwiać działanie w co najmniej dwóch trybach pracy:
    a) routera (tzn. w warstwie 3 modelu OSI),
    b) przełącznika (tzn. w warstwie 2 modelu OSI).
12. Obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać min. 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3.
13. Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
14. Zestaw zabezpieczający musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej:
    a) oznaczania pakietów znacznikami DiffServ,
    b) ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego,
    c) utworzenia co najmniej 8 klas ruchu sieciowego.
15. Komponent zabezpieczający musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN).
16. Komponent zabezpieczający musi spełniać co najmniej następujące parametry wydajnościowe:
    a) minimum 15 Gbps dla IPSEC VPN
    b) minimum 1 000 tuneli IPSEC VPN (site-to-site)

    Jeżeli wykorzystanie funkcji VPN IPSec wymaga zakupu dodatkowych licencji, to należy je przewidzieć w ofercie dla maksymalnej jego wydajności, w ramach wynagrodzenia wykonawcy. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez dostawcę.
17. Zestaw zabezpieczający musi realizować funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
18. Zestaw zabezpieczający musi umożliwiać obsługę protokołów routingu minimum OSPF w wersji 2 i 3, BGP, wraz z BFD. A także musi obsługiwać nie mniej niż 20 wirtualnych routerów posiadających odrębne tabele routingu.
19. Zestaw zabezpieczający musi wspierać mechanizm PBR (policy based routing) – mechanizm przekierowania ruchu z pominięciem tablicy routingu.
20. Zestaw musi obsługiwać nie mniej niż 10 wirtualnych firewalli/systemów/domen/kontekstów i posiadać możliwość rozbudowy do co najmniej 20 takich systemów. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych:
    a) tablic routingu,
    b) polityk bezpieczeństwa obejmujących:
        i. systemu IPS,
        ii. systemu ochrony antymalware/antyspyware,
        iii. systemu ochrony antywirus,
        iv. tuneli VPN IPSec.

    Zamawiający wymaga dostarczenia licencji na nie mniej niż 10 wirtualnych firewalli/systemów/domen/kontekstów w chwili dostarczenia komponentu zabezpieczającego. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez Wykonawcę.
21. Polityka bezpieczeństwa musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. Komponent zabezpieczający musi umożliwiać zdefiniowanie nie mniej niż 5 000 reguł polityki bezpieczeństwa oraz obsługę minimum 300 stref bezpieczeństwa.

22. Musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, na których działa aplikacja (ang. application/services). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji komponentu zabezpieczającego numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Komponent zabezpieczający musi wykrywać predefiniowane aplikacje wspieranych przez producenta (np. Skype, Tor, BitTorrent, eMule) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu lub w inny sposób ale wschodzący w skład komponentu zarządczego. W przypadku gdy producent nie dostarcza takiej funkcjonalności, Zamawiający dopuszcza dostarczenie zewnętrznego narzędzia w formie oprogramowania, dostarczonego na koszt Wykonawcy oraz bez ponoszenia przez Zamawiającego jakichkolwiek dodatkowych kosztów w terminie późniejszym, z licencją zapewniającą możliwość użytkowania i aktualizacji przez czas nieograniczony i bez możliwości jej wypowiedzenia, realizującego funkcjonalność tworzenia nowych definicji aplikacji, importowanych następnie przez komponent zarządzający lub zabezpieczający.
23. Zestaw musi posiadać i być dostarczony z funkcjonalnością systemu wykrywania i zapobiegania włamaniom (Intrusion Prevention System – IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System musi działać w warstwie 7 modelu OSI. Baza sygnatur systemu wykrywania i zapobiegania włamaniom musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł systemu wykrywania i zapobiegania włamaniom musi mieć możliwość wykluczania z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji lub zdefiniowanych serwisów, np. poprzez numer portu, protokół transportowy. Zamawiający wymaga dostarczenia licencji na system wykrywania i zapobiegania włamaniom w chwili dostarczenia urządzeń wchodzących w skład zestawu. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez Wykonawcę.
24. Zestaw musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Moduł AV musi być uruchamiany per aplikacja (ang. application/services) oraz wybrany dekoder taki jak np. http, smtp, imap, pop3, ftp, smb itp. Baza sygnatur AV musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent urządzenia na którym realizowana jest ta funkcja. Moduł AV musi mieć możliwość wykluczania z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji lub zdefiniowanych serwisów, np. poprzez numer portu, protokół transportowy. Zamawiający wymaga dostarczenia licencji na ochronę antywirusową w chwili dostarczenia urządzenia. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez Wykonawcę.
25. Zestaw musi zapewniać ochronę przed atakami typu Spyware. Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi mieć możliwość wykluczenia z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji bez względu na numery portów, na których działa. Zamawiający wymaga dostarczenia licencji na silnik Antyspyware w chwili dostarczenia urządzeń wchodzących w skład zestawu. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez Wykonawcę.
    Komponent zabezpieczający musi zapewniać możliwość wysłania do sandboxa producenta (w chmurze lub lokalnego) plików przesyłanych przez niego – funkcja ta musi być realizowana co najmniej dla plików wykonywalnych. Zamawiający dopuszcza by odbywało się to poprzez dedykowany mechanizm wbudowany w urządzenie lub przez jeden z wymaganych silników detekcyjnych przy czym funkcja ta musi mieć możliwość wskazania/wykluczania z filtrowania specyficznego ruchu sieciowego na podstawie zarówno kierunku transmisji (ruch wchodzący/wychodzący ze wskazanej strefy bezpieczeństwa), adresu źródłowego IP jak i adresu

docelowego IP jak i rozpoznania aplikacji lub zdefiniowanych serwisów, np. poprzez numer portu, protokół transportowy.
Dopuszcza się zarówno realizację sandboxa w postaci chmury producenta jak i rozwiązania lokalnego. W tym drugim przypadku wymagane jest dostarczenie opisu współpracy proponowanej integracji z dostarczanym komponentem bezpieczeństwa
Bez względu na użyte rozwiązanie, wymaga się wydajności zapewniającej jednoczesną analizę minimum 20 plików/próbek w tzw. VM Sandboxing (rozumiana jako realizacja funkcjonalności sandbox polegająca na wykorzystaniu instancji maszyn wirtualnych z określonymi systemami operacyjnymi i zestawem zainstalowanych aplikacji do zdetonowania/uruchomienia, a następnie analizy podejrzanego pliku pod kątem jego potencjalnie negatywnego wpływu na komputery klienckie lub serwery).

26. Zarządzanie urządzeniami wchodzącymi w skład zestawu zabezpieczającego (w tym zarządzanie regułami/politykami bezpieczeństwa) musi odbywać się z linii poleceń (CLI) i graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). Zamawiający dopuszcza możliwość realizacji wyżej wymienionych funkcjonalności za pośrednictwem dodatkowych urządzeń (komponentu zarządczego) pod warunkiem, że urządzenia te zostaną dostarczone w ramach przedmiotu zamówienia i że będą funkcjonowały z zachowaniem wymogów, o których mowa w części: Specyfikacja komponentu zarządczego, w pkt 5. System musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach a w szczególności musi mieć zdefiniowane w systemie co najmniej dwa konta typu:
    a) Administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu,
    b) Operator, który ma możliwość tylko odczytu konfiguracji.
27. Komponent zabezpieczający musi umożliwiać uwierzytelnianie administratorów za pomocą co najmniej dwóch z następujących metod:
    a) bazy lokalnej,
    b) RADIUS lub TACACS+ (lub z pomocą protokołu kompatybilnego z tymi protokołami).
    c) serwera LDAP,
28. Praca na urządzeniach musi odbywać się na konfiguracji tymczasowej, a nie aktywnej. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. commit) i są zapisywane automatycznie na urządzeniu, bez wykonywania dodatkowych czynności przez administratora/operatora. Zamawiający wymaga, aby przed zatwierdzaniem zmian na urządzeniu była możliwość przejrzenia zmian, które zostały wykonane na konfiguracji tymczasowej w stosunku do wersji aktywnej. Sposób prezentacji zmian powinien dać administratorowi pełną wiedzę o wprowadzanych zmianach. Ponadto funkcja ta musi umożliwiać sprawdzenie konfiguracji tymczasowej przed jej zatwierdzeniem jako aktywnej konfiguracji urządzenia. Funkcja musi być dostępna co najmniej w interfejsie GUI, zamawiający dopuszcza także możliwość realizacji wspomnianej funkcjonalności za pośrednictwem dodatkowych urządzeń (np. komponentu zarządczego) pod warunkiem, że urządzenia te zostaną dostarczone w ramach przedmiotu zamówienia i że będą funkcjonowały za zachowaniem wymogów, o których mowa w części: Specyfikacja komponentu zarządczego, w pkt. 5.
29. Komponent zabezpieczający musi zapewniać automatyczne zapisanie minimum 20 poprzednich wersji konfiguracji w przestrzeni dyskowej urządzenia i musi istnieć możliwość przywrócenia konfiguracji z określonego dnia, w którym były dokonywane zmiany, tzn. po każdym zapisie konfiguracji na urządzeniu powinna być automatycznie zapisywana konfiguracja, a podczas wyboru konfiguracji musi być widoczna data zapisania konfiguracji. Zamawiający wymaga funkcjonalności odtworzenia konfiguracji urządzenia z każdej dowolnie wybranej wersji zapisanej konfiguracji.
30. Funkcja automatycznego zapisu minimum 20 poprzednich wersji konfiguracji może być również realizowana z wykorzystaniem komponentu zarządczego w uzupełnieniu komponentu zabezpieczającego zastrzegając, że komponent zarządczy musi być zaoferowany zgodnie z pkt 5. Specyfikacji komponentu zarządczego, z jednoczesną koniecznością spełnienia wymagania 11. wymagań dotyczących Systemu.
    Zamawiający wymaga funkcjonalności odtworzenia konfiguracji urządzenia z każdej dowolnie wybranej wersji zapisanej konfiguracji.

31. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest, aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. w innych systemach wirtualnych.
32. Komponent zabezpieczający musi zapewniać interfejs API (JSON, REST, XML lub inny) będący integralną częścią urządzenia, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
33. Komponent zabezpieczający musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG z wyłączeniem serwerów pośredniczących.
34. Zamawiający wymaga dostarczenia funkcjonalności polegającej na deszyfracji połączeń SSL/TLS, następnie przesłania (w trybie transparentnym lub L3) rozszyfrowanego ruchu do analizy przez zewnętrzne systemy bezpieczeństwa (np. WAF/IPS/ZEEK/AV/Anty-Spyware) (service chaining) - w tym systemy wbudowane w komponent zabezpieczający (IPS/AV/Anty-Spyware) w zależności od umiejscowienia – na NGFW komponentu zabezpieczającego lub elemencie dodatkowym). Rozszyfrowany ruch zbadany przez zewnętrzne systemy bezpieczeństwa zostaje przekazany z powrotem do zaszyfrowania do urządzenia, które wykonało deszyfrowanie, w celu ponownego zaszyfrowania (funkcjonalność nazywana dalej inspekcją SSL/TLS).
    Funkcjonalność ta może zostać spełniona przez Wykonawcę przy pomocy dwóch alternatywnych rozwiązań.
    Rozwiązanie pierwsze bazuje na NGFW komponentu zabezpieczającego, gdzie NGFW jest urządzeniem w którym wykonywane jest deszyfrowanie SSL/TLS i ponowne zaszyfrowanie.
    Drugie rozwiązanie pełniące funkcjonalność inspekcji SSL/TLS bazuje na elemencie dodatkowym (które rozszyfrowuje i ponownie zaszyfrowuje ruch) współpracującym z NGFW komponentu zabezpieczającego, przy czym rozwiązanie to musi być dostarczone z niezbędnymi licencjami i gwarancją zgodną z długością wsparcia komponentu zabezpieczającego. W tym drugim rozwiązaniu wymagane jest dostarczenie opisu współpracy proponowanej integracji z dostarczanymi funkcjami bezpieczeństwa (IPS/AV/Anty-Spyware).
    Bez względu na użyte rozwiązanie, wymaga się wydajności minimum 10 Gbps przepustowości dla inspekcji SSL/TLS (ang. SSL Inspection Throughput) oraz obsługę 20 wirtualnych instancji (analogicznie do NGFW).
35. Zamawiający dopuszcza, aby wymagane funkcjonalności komponentu zabezpieczającego (z wyjątkiem funkcji wykrywania aplikacji, obsługi IPS, AV i NAT) zostały zrealizowane poprzez dostarczenie urządzenia albo zespołu urządzeń wraz z odpowiednim oprogramowaniem (zwanych dalej łącznie elementem dodatkowym) pod warunkiem, że spełnione zostaną łącznie niżej określone wymagania:
    a) stosowanie elementu dodatkowego jest możliwe tylko przy zapewnieniu jego wysokiej dostępności. Oznacza to, że zamawiający dopuszcza dostarczenie takiego komponentu jako dedykowanego rozwiązania (urządzenie/urządzenia z dedykowanym dla niego oprogramowaniem serwisowane w całości przez jednego producenta), z pełną redundancją sprzętową i spełnieniem wymagań dotyczących zasilania urządzenia analogicznie jak dla urządzeń Next Generation Firewall (NGFW).
    b) element dodatkowy musi być zaoferowany z pełnym wsparciem producenta co oznacza wymóg zaoferowania wszystkich pakietów funkcjonalnych i serwisowych dostępnych dla danego rozwiązania w zakresie wymaganej funkcjonalności; zatem w przypadku rozwiązania realizującego funkcję inspekcji SSL/TLS, wsparcie musi obejmować zarówno urządzenie, jak i pakiety oprogramowania uruchamiane w ramach tego urządzenia oraz zapewniać wszystkie aktualizacje oprogramowania i posiadać wsparcie na czas wymagany w zamówieniu.
    c) element dodatkowy musi spełniać wymagania zdefiniowane dla całego Systemu;
    d) dla ewentualnych urządzeń w funkcji Inspekcji SSL/TLS, wymaganych jest co najmniej 8 interfejsów 10Gbps i wkładki o przepustowości 10 Gbps (transmisja na odległość min. 10km)
    e) jeżeli opis współpracy proponowanej integracji z dostarczanymi funkcjami bezpieczeństwa (IPS/AV/Anty-Spyware) wymaga dodatkowych interfejsów po stronie komponentu zabezpieczającego (firewalla) to należy je przewidzieć jako dodatkowe – ponad wymagane w niniejszej specyfikacji, dotyczy to także sytuacji kiedy należałoby dostosować infrastrukturę zamawiającego wtedy należy dostarczyć urządzenia takie jak (przełączniki i routery) ale tak aby

nie będą wpływały na parametry wydajnościowe komponentu zabezpieczającego oraz komponentu dodatkowego i były zgodne z systemami zarządzania zamawiającego.
f) element dodatkowy musi mieć możliwość wysyłania zdarzeń do zewnętrznych serwerów SYSLOG.

36. Funkcja Inspekcji SSL/TLS musi posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania w szczególności do stron wrażliwych np. stron rządowych powiązanych z profilem zaufanym czy stron podmiotów medycznych.
37. Komponent zabezpieczający musi zapewniać realizację funkcjonalności zdalnych sesji VPN (ang. remote access VPN) dla użytkowników w zakresie opisanym poniżej:
    1) Komponent zabezpieczający musi obsługiwać funkcjonalność zdalnych sesji VPN umożliwiającą realizację zdalnych sesji VPN przez użytkowników z wykorzystaniem aplikacji klienckich instalowanych na stacjach roboczych (ang. desktop clients),
    2) Komponent zabezpieczający musi zapewniać realizację co najmniej 3000 jednoczesnych zdalnych sesji VPN.
    3) Zestawianie tuneli SSL VPN z wykorzystaniem klienta VPN dostarczonego przez producenta urządzenia NGFW dla co najmniej 3000 użytkowników.
    4) Jeżeli wykorzystanie funkcjonalności zdalnych sesji VPN zgodnie z wymaganiami Zamawiającego wymaga zakupu dodatkowych licencji, to należy je przewidzieć w ofercie w ramach wynagrodzenia Wykonawcy. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez Wykonawcę. Wyjątek stanowi wykorzystanie funkcjonalności pozwalającej na realizację zdalnych połączeń VPN ze stacji roboczych z systemami Windows i macOS w oparciu o aplikacje klienckie, która to funkcjonalność nie może być ograniczona czasowo i jeżeli wymaga ona licencji to muszą być one przewidzieć w ofercie w ramach wynagrodzenia Wykonawcy jako permanentne (bez ograniczenia czasowego).
    5) Komponent zabezpieczający musi zapewniać następujące funkcjonalności dla zdalnych sesji VPN:
        a) obsługę zdalnych sesji VPN z wykorzystaniem protokołu IPSec (ang. Internet Protocol Security) oraz protokołu SSL (ang. Secure Sockets Layer) co najmniej dla dostępu z wykorzystaniem aplikacji klienckich instalowanych na stacjach roboczych,
        b) tunelowanie całego ruchu pochodzącego od stacji klienckiej z wykorzystaniem połączenia VPN oraz tunelowanie jedynie ruchu kierowanego do wybranych adresów IP tzw. dzielone tunelowanie VPN (ang. split-tunneling),
        c) konfigurowanie polityk dostępu umożliwiających dostęp do określonych zasobów wskazywanych w postaci adresów IP i portów UDP/TCP,
        d) konfigurowanie polityk połączenia określających co najmniej statyczne pule adresów IP, z których przyznawane są użytkownikom adresy podczas nawiązywania połączenia oraz możliwość wskazywania adresu serwera DNS,
        e) zakończenie (przerwanie) przez administratora aktywnych zdalnych sesji VPN,
        f) uzyskanie przez administratora informacji o liczbie aktualnie zalogowanych użytkowników (aktywnych zdalnych sesji VPN).
    6) Komponent zabezpieczający musi zapewniać realizację połączeń VPN z wykorzystaniem klientów instalowanych na stacjach roboczych (ang. desktop clients). Aplikacje te muszą być kompatybilne z oferowanym urządzeniem i pochodzić od tego samego producenta lub być przez niego rekomendowane.
    7) Aplikacje klienckie instalowane na stacjach roboczych muszą być udostępnione przez Wykonawcę lub producenta i nie mogą wymagać dodatkowych licencji instalowanych na tych stacjach. Jeżeli dostęp do strony umożliwiającej pobranie oprogramowania wymaga autoryzacji Wykonawca zapewni do niej dostęp dla wskazanych pracowników Zamawiającego. W czasie trwania wsparcia technicznego Wykonawca musi zapewnić dostęp do aktualizacji i nowych wersji aplikacji klienckich i zapewnić dla niego wsparcie.
    8) Wymagane jest, aby aplikacje klienckie umożliwiały realizacje połączeń VPN z urządzeń pracujących pod kontrolą co najmniej następujących systemów operacyjnych: Windows, macOS.

9) Komponent zabezpieczający musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem kont lokalnych oraz z wykorzystaniem co najmniej protokołu LDAP poprzez odwołanie się do zewnętrznego serwera.
10) Przy uwierzytelnianiu użytkowników z wykorzystaniem protokołu LDAP musi być obsługiwana możliwość przypisania dla użytkownika dostępu do określonych zasobów (polityk dostępu) w oparciu o przynależność do grup LDAP do których użytkownik jest przypisany na serwerze LDAP
11) Komponent zabezpieczający musi zapewniać logowanie danych dotyczących połączeń zdalnych sesji VPN w zakresie co najmniej:
    a) nazwy lub identyfikatora użytkownika nawiązującego połączenie,
    b) adresu IP, z którego nawiązywane jest przez użytkownika połączenie,
    c) daty i godziny nawiązania i zakończenia połączenia,
    d) informacji o zakończonych niepowodzeniem próbach nawiązania sesji przez użytkownika (np. nieprawidłowa autoryzacja),
    e) przyznanego na czas trwania sesji adresu IP (w przypadku połączenia z wykorzystaniem aplikacji klienta).

III. Specyfikacja komponentu zarządczego

Komponent zarządczy musi umożliwiać centralne zarządzanie urządzeniami wchodzącymi w skład komponentu zabezpieczającego (w tym zarządzanie regułami/politykami bezpieczeństwa) przy pomocy graficznej konsoli WebGUI dostępnej przez przeglądarkę WWW. Musi umożliwiać zarządzanie wszystkimi urządzeniami NGFW wchodzącymi w skład zaoferowanego komponentu zabezpieczającego i jest wymagany tylko w przypadku gdy jest niezbędny do realizacji funkcji opisanych w punkcie II OPZ.

1. Komponent zarządczy musi być dostarczony w postaci dedykowanego urządzenia.
2. Komponent zarządczy musi pochodzić od tego samego producenta, co urządzenia NGFW wchodzące w skład komponentu zabezpieczającego.
3. Komponent zarządczy musi umożliwiać zarządzanie łącznie co najmniej 10 fizycznymi urządzeniami NGFW i co najmniej 40 firewallami wirtualnymi rozumianymi jako wirtualny firewalli/system/domena/kontekst z możliwością licencyjnej rozbudowy do 80.
4. Komponent zarządczy musi umożliwiać zdefiniowanie co najmniej 10 lokalnych kont administracyjnych z możliwością określenia praw dostępu.
5. Zamawiający dopuszcza możliwość zastąpienia WebGUI, wyłącznie w momencie, gdy:
    a) dostawca zapewni wszystkie niezbędne składniki do jego działania w trybie wysokiej dostępności HA (w celu wykluczenia pojedynczego punktu awarii),
    b) zapewni wszystkie niezbędne licencje i komponenty, przy czym licencje te muszą być nieodwołalne i nie mogą powodować powstania po stronie zamawiającego obowiązku wnoszenia dodatkowych opłat, wynagrodzenia, honorariów etc., Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez dostawcę.
    c) rozwiązanie to będzie umożliwiało dostęp dla co najmniej 10 osób jednocześnie,
    d) gwarancja i wsparcie na rozwiązanie zastępujące WebGUI musi trwać cały okres gwarancyjny komponentu zabezpieczającego,
6. Komponent zarządczy musi dawać możliwość pełnej konfiguracji urządzeń, ze wszystkimi ich funkcjami składowymi minimum takimi jak: zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium, dystrybucję i zdalną instalację nowych sygnatur oraz wersji oprogramowania systemowego oraz przechowywanie różnych wersji konfiguracji zarządzanych NGFW.
7. Komponent zarządczy musi być w stanie zarządzać wersjami baz sygnatur na urządzeniach NGWF oraz zdalnymi uaktualnieniami baz sygnatur.

8. Graficzny interfejs musi być dostępny po protokole HTTPS przez przeglądarkę www z wykorzystaniem najnowszej wersji protokoły HTML bez wykorzystywania technologii java albo flash.
9. Komponent zarządczy musi pozwalać na obsługę co najmniej 50 logów na sekundę przy szacowanym przyroście dziennym nie mniejszym niż 1,5GB i przechowywać te logi przez okres minimum 5 lat.
10. Komponent zarządczy musi posiadać co najmniej cztery interfejsy 1 Gigabit Ethernet (minimum 2 SFP).

IV. Warsztaty szkoleniowe

1. Wykonawca po zakończeniu prac związanych z wdrożeniem i migracją zobowiązany jest przeprowadzić warsztaty szkoleniowe.
2. Wykonawca będzie zobowiązany przeprowadzić warsztaty szkoleniowe aktualizujące wiedzę administratorów w związku z zastosowanymi rozwiązaniami, dla co najmniej czterech administratorów systemu bezpieczeństwa u Zamawiającego.
3. Warsztaty muszą zostać przeprowadzone w formie ćwiczeń, czas ćwiczeń to minimum 6 godzin dziennie (maksymalnie 8 godzin). Zamawiający szacuje z własnego doświadczenia iż poniżej wskazany zakres oznacza iż warsztaty powinny trwać minimum 4 dni. Warsztaty powinny obejmować swoim zakresem wiedzy z obsługi urządzeń dotyczącą konfiguracji i zarządzania urządzeniami w tym także instalacje i przeprowadzanie aktualizacji urządzeń do najnowszego oprogramowania.
4. Zakres tematyczny warsztatów szkoleniowych:
   Architektura dostarczonego rozwiązania Next Generation Firewall, przegląd interfejsu administratora CLI i GUI, backup konfiguracji i innych elementów oraz ich przywracanie po awarii, aktualizacja firmware, oraz innych elementów systemu, konfiguracja klastra niezawodnościowego Active/Passive w trybie HA, zarządzanie urządzeniem z poziomu interfejsu „command line", zarządzanie licencjami, aktualizacja zarządzanych urządzeń, konfiguracja podstawowa urządzenia, konfiguracja sieci i routingu, tworzenie sieci VLAN na urządzeniach, konfiguracja routingu dynamicznego, policy routing, ustawienie odpowiedniego połączenia urządzenia i konfiguracja protokołu BGP dla zachowania redundancji połączeń, dwuskładnikowa autoryzacja, polityki bezpieczeństwa oraz translacja adresów w ramach konfiguracji urządzenia, identyfikacja aplikacji, wyjaśnienie działania, podstawy ochrony (Mechanizm IPS, AV, Anty-Spyware i inne), kategoryzacja stron Internetowych URL filtering, deszyfracja ruchu szyfrowanego SSL, identyfikacja użytkowników, konfiguracja połączeń VPN wraz z elementami systemu, monitorowanie urządzenia oraz tworzenie raportów, alertów, zarządzenie logami systemu urządzenia, monitorowanie ruchu na firewallu – ruch użytkowników, ruch aplikacji, analiza pakietów, przeprowadzanie diagnostyki urządzenia, przeprowadzenie użytkownika przez najczęściej pojawiające się problemy (tzw. Troubleshooting). Jeżeli rozwiązanie wymaga uruchomienia analizatora logów w formie osobnej instancji należy zapewnić szkolenie także z tego produktu.
5. Warsztaty szkoleniowe powinny zostać uzgodnione odnośnie daty z przedstawieniem minimum dwóch terminów szkoleń oraz rozpisanym planem na poszczególne dni w siedzibie zamawiającego, gdzie zamawiający udostępni miejsce na przeprowadzenie zajęć.