Załącznik nr 1

OPIS PRZEDMIOTU SZACOWNIA

Spis treści

I. WPROWADZENIE

Przedmiotem szacowania jest dostawa 30 urządzeń brzegowych klasy Next Generation Firewall - NGFW (dalej: „Urządzenia") wraz z ich wdrożeniem i uruchomieniem oraz realizacją usługi szkolenia (dalej: „Szkolenie") oraz wsparcia powdrożeniowego (dalej: „Usługa Wsparcia powdrożeniowego"), we wskazanych lokalizacjach.

Zamówienie jest finansowane w ramach Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności (dalej: „KPO"), Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo - Cyberbezpieczny Rząd

II. OPIS PRZEDMIOTU SZACOWANIA

1. Zakres Przedmiotu szacowania

Wykonanie Przedmiotu zamówienia obejmuje:

1.1. dostawę, wdrożenie (instalację oraz konfigurację) oraz uruchomienie Urządzeń, w tym instalację i konfigurację oprogramowania standardowego dostarczonego wraz z Urządzeniami;
1.2. realizację Szkolenia w zakresie zastosowanych rozwiązań;
1.3. świadczenie Usługi Wsparcia powdrożeniowego.

2. Realizacja Przedmiotu szacowania

2.1. Wykonawca dostarczy i zainstaluje Urządzenia, zgodnie ze specyfikacją wymagań technicznych, we wskazanych w tabeli 1 lokalizacjach, pod nadzorem i przy współpracy osób upoważnionych przez Zamawiającego (dalej: „**Osoby kontaktowe**") do przekazywania Wykonawcy wszelkich informacji niezbędnych do realizacji instalacji Urządzeń, uzgadniania kwestii technicznych, koordynowania przebiegu prac oraz sprawowania bieżącej kontroli nad ich wykonaniem.
2.2. Dostarczone Urządzenia muszą być fabrycznie nowe, oryginalnie zapakowane, nieuszkodzone, pochodzić z autoryzowanego kanału sprzedaży producenta, muszą reprezentować model bieżącej linii produktowej i być dopuszczone do obrotu i użytkowania na terenie Unii Europejskiej.
2.3. Zamawiający nie dopuszcza Urządzeń odnawianych (refabrykowanych), demonstracyjnych, czy powystawowych. Wymagana jest dostawa Urządzeń nieużywanych wraz z niezbędnym, kompletnym wyposażeniem producenta.
2.4. Zamawiający wymaga, aby dostarczane Urządzenia wraz z oprogramowaniem standardowym były sprawdzone w praktyce rynkowej. Oznacza to, że oprogramowanie standardowe (firmware Urządzeń), realizujące wszystkie wymagane funkcje, jak też same Urządzenia (jako typ/model) były wprowadzone do obrotu na terytorium Rzeczypospolitej Polskiej na co najmniej 6 miesięcy przed upływem terminu składania ofert.
2.5. Zamawiający wymaga, aby zaoferowane Urządzenia były serwisowane przez producenta lub autoryzowanego przedstawiciela serwisowego oraz nie były przewidziane do wycofania ze sprzedaży i wsparcia (ogłoszone tzw. Dokumenty

End-of-Sale lub End-of-Life lub równoważne) – na dzień składania ofert. Wykonawca przedstawi wraz z ofertą oświadczenie własne w w/w zakresie.

2.6. Zamawiający wymaga, aby Wykonawca posiadał autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nią związanych. Wykonawca przedstawi wraz z ofertą oświadczenie własne w w/w zakresie.

2.7. Producent każdego z Urządzeń musi posiadać certyfikat zgodności z normą ISO 9001:2015 lub równoważną oraz certyfikat ISO 14001:2015 lub równoważną, obejmujący przedstawicielstwo w Polsce w zakresie sprzedaży oraz serwisu Urządzeń.

2.8. Urządzenia muszą spełniać wszystkie wymogi dotyczące bezpieczeństwa oraz zużycia energii określone w obowiązującym prawie polskim. Wykonawca winien przedłożyć wraz z ofertą deklaracja zgodności CE dla oferowanych Urządzeń.

2.9. Urządzenia muszą być oznakowane w taki sposób, aby możliwa była ich identyfikacja oraz identyfikacja producenta.

2.10. Wykonawca odpowiada za wady prawne i fizyczne, ujawnione w Urządzeniach będących Przedmiotem zamówienia oraz ponosi z tego tytułu wszelkie zobowiązania. Jest odpowiedzialny względem Zamawiającego, jeżeli dostarczone Urządzenia:

2.10.1. stanowią własność osoby trzeciej albo jeżeli są obciążone prawem osoby trzeciej,

2.10.2. mają wadę zmniejszającą ich wartość lub użyteczność wynikającą z ich przeznaczenia, nie mają właściwości wymaganych przez Zamawiającego albo jeżeli dostarczono je w stanie niezupełnym.

2.11. Dostawa Urządzeń nastąpi na koszt własny Wykonawcy, w sposób zapewniającym ich całość i nienaruszalność.

2.12. Wykonawca musi dostarczyć wszelkie elementy, które są niezbędne do prawidłowego funkcjonowania całości Urządzeń. W przypadku, gdy w trakcie realizacji Przedmiotu zamówienia okaże się, że brakuje jakiegokolwiek elementu, które spowoduje nieprawidłowe funkcjonowanie całości Przedmiotu zamówienia, Wykonawca dostarczy je na własny koszt.

2.13. Wymagania językowe i komunikacyjne:

2.13.1. językiem umownym oraz językiem komunikacji na każdym etapie realizacji zamówienia (dostawa, wdrożenie, szkolenia, serwis, obsługa gwarancyjna) jest język polski;

2.13.2. Wykonawca zapewni, że osoby wyznaczone do realizacji prac wdrożeniowych, kontaktów z Zamawiającym oraz świadczenia Usług Wsparcia powdrożeniowego oraz usług gwarancyjnych posługują się językiem polskim w stopniu umożliwiającym swobodną komunikację techniczną i biznesową, bez konieczności udziału tłumacza;

2.13.3. Wszelka dokumentacja wytworzona w ramach zamówienia, w tym dokumentacja powykonawcza musi zostać sporządzona w języku polskim.

2.14. O ile nie wskazano inaczej, wszelkie zapisy OPZ, zawierające parametry techniczne, należy odczytywać jako parametry minimalne.

3. Wdrożenie

3.1. Wykonawca zobowiązany jest do wykonania usług wdrożeniowych w lokalizacjach wskazanych przez Zamawiającego w tabeli nr 1 poniżej, w trybie „on-site".

Tabela nr 1.

Miasto	Ilość sztuk	Podmiot, adres instalacji Urządzeń	Tryb pracy (HA) – min. active-passive
Białystok	2	Regionalna Dyrekcja Ochrony Środowiska w Białymstoku ul. Dojlidy Fabryczne 23 15-554 Białystok	**TAK**
Bydgoszcz	2	Regionalna Dyrekcja Ochrony Środowiska w Bydgoszczy ul. Dworcowa 81 85-009 Bydgoszcz	**TAK**
Gdańsk	2	Regionalna Dyrekcja Ochrony Środowiska w Gdańsku ul. Chmielna 54/57 80-748 Gdańsk	**TAK**
Gorzów	2	Regionalna Dyrekcja Ochrony Środowiska w Gorzowie Wielkopolskim ul. Jagiellończyka 13 66-400 Gorzów Wielkopolski	**TAK**
Katowice	1	Regionalna Dyrekcja Ochrony Środowiska w Katowicach Plac Grunwaldzki 8-10 40-127 Katowice	**NIE**
Kielce	1	Regionalna Dyrekcja Ochrony Środowiska w Kielcach ul. Szymanowskiego 6 25-361 Kielce	**NIE**
Kraków	1	Regionalna Dyrekcja Ochrony Środowiska w Krakowie ul. Mogilska 25 31-542 Kraków	**NIE**
Lublin	2	Regionalna Dyrekcja Ochrony Środowiska w Lublinie ul. Bazylianówka 46 20-144 Lublin	**NIE**
Łódź	2	Regionalna Dyrekcja Ochrony Środowiska w Łodzi ul. Traugutta 25 90-113 Łódź	**TAK**
Olsztyn	2	Regionalna Dyrekcja Ochrony Środowiska w Olsztynie ul. Dworcowa 60 10-437 Olsztyn	**NIE**
Opole	2	Regionalna Dyrekcja Ochrony Środowiska w Opolu ul. Firmowa 1 45-594 Opole	**TAK**
Poznań	2	Regionalna Dyrekcja Ochrony Środowiska w Poznaniu ul. Kościuszki 57, 61-891 Poznań	**NIE**
Rzeszów	2	Regionalna Dyrekcja Ochrony Środowiska w Rzeszowie Al. Józefa Piłsudskiego 38 35-001 Rzeszów	**TAK**
Szczecin	1	Regionalna Dyrekcja Ochrony Środowiska w Szczecinie ul. Juliusza Słowackiego 2 71-434 Szczecin	**NIE**
Warszawa	4	Regionalna Dyrekcja Ochrony Środowiska w Warszawie ul. Henryka Sienkiewicza 3 00-015 Warszawa	**NIE**
Wrocław	2	Regionalna Dyrekcja Ochrony Środowiska we Wrocławiu ul. Jana Długosza 68 51-162 Wrocław	**TAK**

3.1. Zamawiający wymaga, aby prace „on-site" zostały wykonane w w/w lokalizacjach przez inżyniera (eksperta) posiadającego ważną i aktualną certyfikację producenta oferowanego rozwiązania NGFW w zakresie: montażu, instalacji, konfiguracji, testów działania infrastruktury, omówienia wprowadzonej konfiguracji, technologii bezpieczeństwa sieci oraz musi posiadać dostęp do bazy wiedzy tego producenta. Na żądanie Zamawiającego, Wykonawca przedłoży pisemne oświadczenie, które potwierdza, że inżynier wyznaczony do realizacji niniejszego zamówienia spełnia w/w wymagania.

3.2. Wykonawca zapewni obecność wykwalifikowanego inżyniera, o którym mowa w pkt 3.1, podczas instalacji i uruchomienia Urządzeń, przez **co najmniej 2 dni robocze,** w łącznym wymiarze **nie mniejszym niż 12 godzin roboczych** w każdej lokalizacji, o której mowa w tabeli 1. Nie dopuszcza się realizacji w/w prac wykonywanych zdalnie.

3.3. W ramach realizacji Przedmiotu zamówienia, Wykonawca zobowiązany jest do wykonania co najmniej następujących prac wdrożeniowych:

Etap I: Instalacja fizyczna i inicjalizacja:

3.3.1. Fizyczna instalacja Urządzeń w lokalizacjach wymienionych w Tabeli nr 1. Instalacja nastąpi w miejscu wskazanym przez osoby wyznaczone przez Zamawiającego. *(Uwaga: Lista osób kontaktowych zostanie przekazana Wykonawcy niezwłocznie po podpisaniu Umowy).*
Uruchomienie Urządzeń na wersjach trialowych oprogramowania.

Etap II: Analiza i migracja konfiguracji (na podstawie danych przekazanych przez Osoby kontaktowe we wskazanych lokalizacjach):

3.3.2. Opracowanie konfiguracji docelowej na podstawie dostarczonych danych:
- Osoby kontaktowe we wskazanych lokalizacjach dostarczą Wykonawcy pliki konfiguracyjne (zrzuty konfiguracji) z obecnie wykorzystywanych urządzeń;
- Wykonawca zobowiązany jest do przeanalizowania dostarczonych plików oraz przygotowania konfiguracji nowych Urządzeń (tzw. migracja reguł), uwzględniając specyfikę każdej lokalizacji;
- przeprowadzenie analizy i optymalizacji obecnych polityk bezpieczeństwa przez Wykonawcę pod kątem usunięcia reguł zbędnych lub niebezpiecznych (tzw. rule cleaning) oraz dostosowanie ich do aktualnych standardów bezpieczeństwa i możliwości nowego systemu NGFW.

3.3.3. Proces przenoszenia reguł i polityk musi odbywać się w ścisłym porozumieniu i konsultacji z Osobami kontaktowymi we wskazanych lokalizacjach.

Etap III: Konfiguracja sieciowa i bezpieczeństwa:

3.3.4. Konfiguracja interfejsów sieciowych, routingu oraz translacji adresów (NAT) zgodnie z planem adresacji uzgodnionym z Osobami kontaktowymi we wskazanych lokalizacjach.

3.3.5. Konfiguracja mechanizmów wysokiej dostępności (HA – High Availability) w trybie active-passive (lub innym wymaganym), adekwatnie do wymogów danej lokalizacji.
3.3.6. Konfiguracja polityk bezpieczeństwa wraz z uruchomieniem zaawansowanych funkcji ochrony NGFW: Intrusion Prevention System (IPS), Anti-Virus, Anti-Malware, Anti-Spyware oraz filtrowanie URL.
3.3.7. Integracja Urządzeń z usługą katalogową (AD/LDAP) w celu identyfikacji użytkowników w regułach dostępu.
3.3.8. Uruchomienie logowania ruchu sieciowego i zdarzeń systemowych (zgodnie z polityką retencji logów dla każdej lokalizacji).

Etap IV: Konfiguracja połączeń VPN:

3.3.9. Odtworzenie i uruchomienie tuneli IPsec VPN (Site-to-Site) na podstawie analizy konfiguracji poprzednich urządzeń (zgodnie z pkt 3.3.4).
3.3.10. Konfiguracja i uruchomienie usług dostępu zdalnego VPN typu "Remote Access" (SSL VPN / IPsec) dla użytkowników końcowych.
3.3.11. Przeprowadzenie testów wydajnościowych i funkcjonalnych, w tym uruchomienie minimum 10 jednocześnie aktywnych połączeń VPN "Remote Access", w celu weryfikacji stabilności rozwiązania.

Etap V: Przekazanie wiedzy i zakończenie prac

3.3.12. Omówienie, przygotowanie i przekazanie Osobom kontaktowym we wskazanych lokalizacjach procedury zgłaszania problemów do serwisu producenta.
3.3.13. Omówienie wdrożonej konfiguracji, w tym przeprowadzenie instruktażu z obsługi Urządzeń z wykorzystaniem GUI.
3.3.14. Przekazanie wszystkich haseł do Urządzeń.
3.3.15. Wykonanie kopii bezpieczeństwa konfiguracji zainstalowanych Urządzeń.
3.3.16. Po dokonaniu odbioru końcowego Urządzeń - przeprowadzenie rejestracji w serwisie producenta oraz aktywacja wszystkich wymaganych licencji.
3.3.17. Aktualizacja oprogramowania systemowego (firmware) do najnowszej wersji rekomendowanej przez producenta (wersja stabilna).

3.4. Wykonawca w ramach wdrożenia dostarczy niezbędne okablowanie i wkładki (transceivery) oraz wszelkie elementy konieczne do prawidłowego wykonania Przedmiotu zamówienia.
3.5. Wykonawca umożliwi Osobom kontaktowym we wskazanych lokalizacjach udział we wszystkich pracach prowadzonych w ramach realizacji Przedmiotu zamówienia (m.in. w czasie dostaw, instalacji, konfiguracji i testowania).
3.6. Dostęp do zasobów wskazanych lokalizacji musi być zgodny z obowiązującą u nich polityką bezpieczeństwa. Zamawiający udostępni procedury bezpieczeństwa Wykonawcy, którego oferta zostanie wybrana jako najkorzystniejsza, po podpisaniu Umowy.
3.7. Z uwagi na fakt, że prace będą realizowane na czynnych i użytkowanych obiektach, Wykonawca będzie zobowiązany do ścisłego współdziałania z Osobami kontaktowymi we wskazanych lokalizacjach podczas wykonywania prac,

w celu zminimalizowania ograniczeń i uciążliwości związanych z wykonywanymi pracami.

3.8. Poszczególne prace mogą być realizowane etapowo, tak, aby zachować ciągłość świadczenia usług przez wskazane lokalizacje oraz zapewnić bezpieczeństwo przebywających w obiekcie pracowników.

3.9. Wszelkie uszkodzenia infrastruktury ogólnej na obiektach wskazanych lokalizacji przez Wykonawcę podczas prowadzenia prac instalacyjnych obciążają jego samego i muszą być usunięte w ramach nieodpłatnego usunięcia szkód, niezwłocznie po ich stwierdzeniu.

3.10. Zamawiający wymaga, aby Wykonawca, po dokonaniu uruchomienia Urządzeń, przekazał niezbędne informacje do administrowania zainstalowanymi Urządzeniami oraz zastosowaną konfigurację dla każdej lokalizacji – w ramach wymaganej dokumentacji powykonawczej, o której mowa w pkt 5 poniżej.

4. Testy

4.1. W ramach Przedmiotu zamówienia muszą zostać przeprowadzone testy, których celem jest weryfikacja przez Zamawiającego, czy wszystkie prace wykonane w trakcie realizacji Przedmiotu zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi.

4.2. Testy będą przeprowadzane przez Wykonawcę, przy współudziale Osób kontaktowych we wskazanych lokalizacjach.

4.3. Pozytywne zakończenie testów wraz z usunięciem wskazanych wad jest niezbędne, aby dokonać odbioru częściowego Urządzeń w każdej ze wskazanych lokalizacji.

4.4. Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami.

4.5. W przypadku zidentyfikowania błędów lub wad, Wykonawca jest zobowiązany do ich poprawy przed odbiorem częściowym Urządzeń w danej lokalizacji.

5. Dokumentacja powykonawcza

5.1. Warunkiem dokonania odbioru częściowego Urządzeń dla każdej lokalizacji jest dostarczenie kompletnej dokumentacji powykonawczej.

5.2. Dokumentacja powykonawcza będzie obejmowała w szczególności:

5.2.1. opisy wszelkich cech, funkcjonalności i właściwości, pozwalające na poprawną, z punktu widzenia technicznego, eksploatację Urządzeń;

5.2.2. pełną charakterystykę licencjonowania Urządzeń;

5.2.3. zestaw danych konfiguracyjnych wdrożonych przez Wykonawcę, w tym obejmujących dane konfiguracyjne zainstalowanego oprogramowania dla Urządzeń.

5.3. Dokumentacja powykonawcza musi zostać napisana i dostarczona w języku polskim oraz udokumentowana w postaci elektronicznej w jednym z wymienionych formatów: PDF, RTF, DOC (DOCX), ODF (umożliwiających kopiowanie, modyfikowanie i wydruk treści dokumentu), opatrzona kwalifikowanym podpisem

elektronicznym i przekazana Zamawiającemu na nośniku danych elektronicznych oraz za pośrednictwem poczty elektronicznej na adresy, o których mowa w Umowie.

5.4. Wykonawca ponosi odpowiedzialność za wszelkie braki w dostarczonej dokumentacji powykonawczej.

6. Minimalne parametry i funkcjonalności Urządzeń

6.1. Architektura systemu

6.1.1. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, umożliwiającej rozbudowę do dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności co najmniej Active-Passive.

6.1.2. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparentny.

6.2. Specyfikacja sprzętowa

6.2.1. Metalowa obudowa przeznaczona do montażu w szafie serwerowej (standard rack 19 cali, wysokość 1U).

6.2.2. Wymagane jest wbudowane, redundantne zasilanie.

6.2.3. Urządzenie musi być wyposażone w lokalny dysk o pojemności minimum 200 GB SSD do celów logowania i raportowania.

6.3. Typy interfejsów i parametry wydajności

6.3.1. Urządzenie musi dysponować minimum 8 interfejsami miedzianymi Ethernet o przepustowości co najmniej 2,5 Gb/s.

6.3.2. Urządzenie musi dysponować minimum 2 interfejsami optycznymi 1 GbE (SFP).

6.3.3. Urządzenie musi posiadać wbudowane lub udostępniać możliwość rozbudowy o co najmniej 2 porty 25 GbE SFP28.

6.3.4. Urządzenie musi mieć możliwość tworzenia minimum 128 interfejsów wirtualnych (VLAN) w oparciu o standard 802.1Q.

6.3.5. Urządzenie musi zapewnić:

- Minimalna liczba nowych połączeń na sekundę na poziomie: 30 000.
- Minimalna liczba jednoczesnych połączeń: 600 000.
- Minimalna przepustowość Firewall (dla pakietów UDP): 10 Gbps.
- Minimalna przepustowość IPS: 5,0 Gbps.
- Minimalna przepustowość Threat Protection (z włączonym antywirusem, IPS i kontrolą aplikacji): 1,3 Gbps.
- Minimalna przepustowość IPSec VPN (AES-256): 2,5 Gbps.

6.4. Zarządzanie i utrzymanie

6.4.1. Urządzenie musi być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH.

6.4.2. Urządzenie musi mieć wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej ping oraz narzędzia do przechwytywania pakietów i wyświetlania otwartych połączeń sieciowych.
6.4.3. Urządzenie musi mieć możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych Urządzenia (brak dostępu, tylko odczyt, pełen zapis/odczyt).
6.4.4. Urządzenie musi mieć możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów.
6.4.5. Urządzenie musi mieć mechanizm informowania o aktualizacjach oprogramowania systemowego oraz możliwość przechowywania przynajmniej dwóch wersji firmware.
6.4.6. Urządzenie musi mieć wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji (w tym automatycznych: codziennie, tygodniowo, miesięcznie).
6.4.7. Urządzenie musi mieć wsparcie dla protokołów SNMP v1, v2 i v3 oraz automatyczne powiadamianie przez SMTP lub SNMP.

6.5. Zapora sieciowa, konfiguracja sieciowa oraz routing

6.5.1. Urządzenie musi posiadać możliwość działania w oparciu o mechanizm Stateful Deep Packet Inspection.
6.5.2. Urządzenie musi posiadać możliwość budowania reguł zapory sieciowej w oparciu o obiekty takie jak host, sieć, interfejs, harmonogram, port, protokół, użytkownik, grupa użytkowników.
6.5.3. Urządzenie musi posiadać możliwość definiowania polityk NAT wraz z IP masquerading.
6.5.4. Urządzenie musi zapewniać ochronę przed atakami DoS, DDoS (flood protection) oraz skanowaniem portów (portscan blocking).
6.5.5. Urządzenie musi posiadać możliwość blokowania ruchu na podstawie kraju pochodzenia (geolokalizacja, IP).
6.5.6. Urządzenie musi posiadać możliwość obsługi routingu statycznego oraz protokołów routingu dynamicznego (RIP, OSPF, BGP).
6.5.7. Urządzenie musi posiadać funkcjonalność SD-WAN z analizą stanu łącza w czasie rzeczywistym (monitorowanie opóźnienia, jitter, utraty pakietów) i dynamicznym wyborem najkorzystniejszego łącza.
6.5.8. Urządzenie musi posiadać możliwość rozkładania ruchu pomiędzy wieloma interfejsami WAN w oparciu o wagi i automatyczne przełączanie w przypadku awarii (failover).
6.5.9. Urządzenie musi posiadać możliwość obsługi modemu USB LTE jako łącza zapasowego.

6.6. Ochrona antywirusowa

6.6.1. Urządzenie ma umożliwiać zastosowanie z co najmniej jednego skanera antywirusowego dostarczonego przez firmy trzecie.
6.6.2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany wraz z urządzeniem.

6.6.3. Dostarczony skaner antywirusowy musi pochodzić od europejskiego producenta.
6.6.4. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
6.6.5. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

6.7. Ochrona antyspam

6.7.1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
6.7.2. Ochrona antyspam ma działać w oparciu o:
- białe/czarne listy,
- DNS RBL,
- Skaner heurystyczny.

6.7.3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
6.7.4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin

6.8. Filtr dostępu do stron www

6.8.1. Urządzenie ma posiadać wbudowany filtr URL.
6.8.2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
6.8.3. Administrator ma mieć możliwość dodawania własnych kategorii URL.
6.8.4. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
- blokowanie dostępu do adresu URL,
- zezwolenie na dostęp do adresu URL,
- blokowanie dostępu do adresu URL oraz wyświetlenie strony
- HTML zdefiniowanej przez administratora.

6.8.5. Administrator ma mieć możliwość skonfigurowania różnych stron z komunikatem o zablokowaniu strony.
6.8.6. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
6.8.7. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
6.8.8. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
6.8.9. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
6.8.10. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

6.9. Autoryzacja użytkowników

6.9.1. Urządzenie musi posiadać wbudowaną lokalną bazę użytkowników (minimum 100 kont).
6.9.2. Urządzenie ma umożliwiać integracje z Active Directory, RADIUS i LDAP oraz uwierzytelnianie w trybie Single Sign On (SSO).
6.9.3. Urządzenie ma umożliwiać uwierzytelnianie przez wbudowany Captive Portal.
6.9.4. Urządzenie musi posiadać wbudowany moduł 2FA (TOTP) dla tuneli VPN, portalu uwierzytelniania oraz interfejsów administracyjnych (Web GUI, SSH).

6.10. Podstawowe opcje VPN

6.10.1. Urządzenie musi posiadać funkcjonalność koncentratora VPN dla połączeń Site-to-site (IPSec) oraz Client-to-site (IPSec, SSL VPN).
6.10.2. Urządzenie musi posiadać funkcjonalność ZTNA (Zero Trust Network Access) dla klienta SSL VPN, umożliwiająca weryfikację stanu hosta przed zestawieniem tunelu (m.in. weryfikacja AV, domeny, firewalla systemowego).
6.10.3. Producent urządzenia ma umożliwiać pobranie klienta VPN.

6.11. Ochrona sieci

6.11.1. Urządzenie musi zapewnić dodatkowy moduł ochrony klasy IPS z bazą minimum 1000 sygnatur, z możliwością dodawania własnych sygnatur i automatyczną aktualizacją.
6.11.2. Urządzenie musi zapewnić ochronę i kontrolę Web poprzez filtrowanie treści jako Transparent Web Proxy dla HTTP i HTTPS, z inspekcją TLS 1.3, skanowaniem antywirusowym w czasie rzeczywistym i filtrowaniem na podstawie MIME.
6.11.3. ochronę i kontrolę aplikacji poprzez identyfikacja aplikacji niezależnie od portu i protokołu, kontrola mikroaplikacji (np. w mediach społecznościowych), z automatyczną aktualizacją sygnatur.

6.12. Logowanie i raportowanie

6.12.1. Urządzenie musi zapewnić możliwość gromadzenia, składowania i archiwizacji logów dotyczących zdarzeń sieciowych (Web, FTP, VPN, aplikacje, ataki, wirusy) z możliwością powiązania ich z nazwami użytkowników.
6.12.2. Urządzenie musi zapewnić możliwość przeglądania archiwalnych logów z użyciem filtrów oraz eksport do zewnętrznych systemów (np. SIEM).
6.12.3. Urządzenie musi zapewnić możliwość generowania raportów w formacie HTML i CSV oraz wysyłanie logów do serwerów syslog.
6.12.4. Urządzenie musi zapewnić możliwość podglądu wykorzystania łącza w czasie rzeczywistym w oparciu o użytkownika/adres IP, z możliwością anonimizacji danych.

6.13. Gwarancja i serwis

6.13.1. Do każdego dostarczonego w ramach Umowy Urządzenia Zamawiający wymaga dostarczenia standardowej gwarancji i wsparcia producenta, której bieg liczony będzie od daty podpisania Protokołu odbioru częściowego bez

uwag (dla każdej lokalizacji osobno) – po dostarczeniu i uruchomieniu Urządzeń we wskazanych lokalizacjach. Wykonawca zobowiązany jest do przekazania Zamawiającemu kart gwarancyjnych producenta lub autoryzowanego przedstawiciela producenta jednoznacznie identyfikujących każde Urządzenie (stanowi to warunek odbioru końcowego Urządzeń).

6.13.2. Standardowa gwarancja w okresie jej obowiązywania musi zapewniać dostęp do poprawek oprogramowania Urządzeń oraz wsparcia technicznego. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta Urządzeń lub autoryzowanego przedstawiciela producenta. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

6.13.3. Usługi serwisu i wsparcia technicznego muszą być świadczone przez producenta Urządzeń, lub autoryzowanego partnera serwisowego producenta - wymagane jest dostarczenie oświadczenia Wykonawcy potwierdzające, że serwis będzie realizowany przez producenta lub autoryzowanego partnera serwisowego producenta, które należy dołączyć do oferty;

6.13.4. Zgłoszenia serwisowe powinny być przyjmowane w języku polskim (telefonicznie lub poprzez e-mail lub dedykowany serwis www).

6.13.5. Zamawiający musi uzyskać dostęp do portalu producenta w celu pobierania aktualizacji oprogramowania, dokumentacji oraz uzyskania pomocy technicznej przez cały okres trwania licencji oprogramowania Urządzeń.

6.14. Dokumenty.

6.14.1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej Przedmiotem zamówienia (tzw. Produkty podwójnego zastosowania), Wykonawca winien posiadać 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 2004, Nr 229, poz. 2315 z późn. zm.) 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. Wykonawca złoży wraz z ofertą stosowne oświadczenie.

6.14.2. Wykonawca przedłoży z ofertą oświadczenie, że jest autoryzowany przez producenta Urządzeń w zakresie sprzedaży oferowanego rozwiązania na terenie Polski.

7. Szkolenie

7.1. Wymagania ogóle

7.1.1. Wykonawca zorganizuje i przeprowadzi dedykowane, dwudniowe Szkolenie w trybie online dla maksymalnie 20 osób wskazanych przez Zamawiającego.

7.1.2. Szkolenie musi być przeprowadzone na żywo przez instruktora, umożliwiając interakcję z uczestnikami oraz sesję Q&A.
7.1.3. Wykonawca zapewni stabilną platformę do szkolenia online, spełniającą wymogi bezpieczeństwa informacji i ochrony danych przy spotkaniach zdalnych, z możliwością udostępniania ekranu i pracy warsztatowej.
7.1.4. Wykonawca udostępni uczestnikom materiały szkoleniowe w języku polskim w formie elektronicznej oraz, jeśli to możliwe, środowisko demonstracyjne/laboratoryjne do ćwiczeń praktycznych.
7.1.5. Czas trwania: 2 dni robocze (minimum 12 godzin, przy czym godzina liczona jest jako 60 minut).
7.1.6. Strony ustalą termin Szkolenia, przy czym Wykonawca zaproponuje co najmniej dwa terminy do wyboru.
7.1.7. Zamawiający wymaga, aby Szkolenie zostało przeprowadzone przez eksperta/inżynier z oficjalnym certyfikatem producenta oferowanego rozwiązania NGFW na poziomie eksperckim. Wykonawca przedstawi Zamawiającemu kopię certyfikatu na 2 dni robocze przed planowanym terminem Szkolenia.

*7.2. **Zakres Szkolenia***

7.2.1. Szkolenie ma na celu przekazanie kompleksowej wiedzy teoretycznej i praktycznych umiejętności w zakresie administracji, konfiguracji i utrzymania zapór sieciowych nowej generacji (NGFW).
7.2.2. Program szkolenia musi obligatoryjnie obejmować następujące zagadnienia:
- Architektura proponowanego rozwiązania NGFW.
- Architektura proponowanego rozwiązania NGFW.
- Podstawowa konfiguracja urządzenia.
- Zarządzanie konfiguracją i tworzenie kopii zapasowych (backupy).
- Konfiguracja interfejsów sieciowych.
- Tworzenie i zarządzanie politykami bezpieczeństwa.
- Konfiguracja translacji adresów (NAT).
- Identyfikacja aplikacji (Application Identification) i jej wykorzystanie w politykach bezpieczeństwa.
- Konfiguracja mechanizmów ochrony (IPS, Antywirus, Anty-Spyware, Anty-Malware, filtrowanie URL).
- Deszyfracja ruchu szyfrowanego SSL – omówienie metod i konfiguracja.
- Identyfikacja użytkowników w sieci (User-ID), metody gromadzenia informacji o użytkownikach i wykorzystanie tożsamości w politykach.
- Konfiguracja bezpiecznego dostępu zdalnego dla użytkowników (np. SSL VPN, GlobalProtect).
- Konfiguracja tuneli VPN Site-to-Site (IPSec).
- Monitorowanie pracy urządzenia, analiza logów oraz tworzenie raportów.
- Konfiguracja klastra wysokiej dostępności (High Availability), w tym omówienie i konfiguracja trybów Active/Passive oraz Active/Active.
- Omówienie najlepszych praktyk konfiguracyjnych i optymalizacyjnych.

8. Usługa Wsparcia powdrożeniowego

8.1. Usługa Wsparcia powdrożeniowego będzie realizowana w wskazanych w tabeli 1 lokalizacjach, na podstawie zgłoszeń (dalej: „**Zgłoszenie**") Osób kontaktowych.

8.2. Usługa Wsparcia powdrożeniowego ma na celu ustabilizowanie i optymalizację działania Urządzeń dostarczonych w ramach Przedmiotu zamówienia.

8.3. W ramach Usługi Wsparcia powdrożeniowego Osoby kontaktowe we wskazanych lokalizacjach mogą zlecić Wykonawcy wykonanie w szczególności:

8.3.1. aktualizacji oprogramowania firmware oraz software zgodnie z najnowszymi wytycznymi,

8.3.2. przeprowadzania koniecznych zmian w konfiguracji Urządzeń zgodnie z wymogami Zamawiającego,

8.3.3. strojenie polityk bezpieczeństwa,

8.3.4. konsultacje oraz wdrażanie możliwych usprawnień systemowych,

8.3.5. świadczenie doradztwa i wsparcia w pozostałych problemach związanych z Przedmiotem zamówienia, nieujętych w standardowej gwarancji producenta.

8.4. Wykonawca powinien informować na bieżąco Osoby kontaktowe o stwierdzonej przez niego konieczności zainstalowania poprawek, nowych wersji oraz nowych funkcjonalności dla Urządzeń, oprogramowania dostarczonego wraz z Urządzeniami – w oparciu o taką informację Osoby kontaktowe mogą przesłać Wykonawcy Zgłoszenie zlecając mu realizację zasygnalizowanych przez Wykonawcę działań.

8.5. Zamawiający wymaga, aby Wykonawca, w tym jego personel realizujący Usługi Wsparcia powdrożeniowego posiadał certyfikację producenta oferowanego rozwiązania NGFW, umożliwiającą rozwiązywanie problemów technicznych. Na żądanie Zamawiającego, Wykonawca przedstawi stosowne oświadczenie lub certyfikat w tym zakresie.

8.6. Szczegółowe warunki realizacji Usługi Wsparcia powdrożeniowego zostały opisane w § 7 Umowy.

9. DNSH (Do No Significant Harm)

Przedmiot zamówienia musi być zgodny z zasadą „niewyrządzania znaczącej szkody" (Do No Significant Harm – DNSH). Oznacza to, że Wykonawca musi zapewnić, że jego realizacja nie będzie miała znaczącego negatywnego wpływu na cele środowiskowe, takie jak ochrona klimatu, gospodarka o obiegu zamkniętym, zapobieganie zanieczyszczeniom oraz ochrona bioróżnorodności. Wszystkie wdrażane rozwiązania muszą zostać zaprojektowane w sposób minimalizujący negatywny wpływ na środowisko naturalne.

10. Ochrona danych osobowych

Z komentarzem [G1]: Od IOD

10.1. Wykonanie przedmiotu zamówienia przez Wykonawcę w zakresie określonym w ust. 1 pkt 1.1 oraz 1.3, nie wiąże się z koniecznością przetwarzania danych osobowych użytkowników infrastruktury informatycznej. W związku z powyższym Zamawiający nie przewiduje dodatkowego uregulowania zasad przetwarzania danych osobowych na gruncie przepisów o ochronie danych osobowych. W sytuacji, gdyby w toku realizacji zamówienia doszło do konieczności dostępu do danych osobowych lub ich przetwarzania, Wykonawca zobowiązany jest do niezwłocznego poinformowania o

tym fakcie Zamawiającego, wstrzymania się z wykonywaniem czynności skutkujących przetwarzaniem danych osobowych do czasu otrzymania pisemnej instrukcji Zamawiającego oraz do zachowania w poufności wszelkich danych, do których uzyskał dostęp.

10.2. Wykonanie przedmiotu zamówienia przez Wykonawcę, w zakresie określonym w ust. 1 pkt. 1.2. wiąże się z koniecznością przetwarzania danych osobowych, uczestników szkolenia. Zamawiający zobowiązuje się udostępnić Wykonawcy dane osobowe w zakresie imienia i nazwiska oraz służbowego adresu e-mail, a Wykonawca zobowiązuje się przetwarzać udostępnione dane wyłącznie w celu realizacji szkolenia, w szczególności w celu umożliwienia kontaktu organizacyjnego, przekazania materiałów szkoleniowych i przeprowadzeniem szkolenia oraz wystawienia imiennego zaświadczenia jego uczestnikom.

10.3. Strony zobowiązują się do zapewnienia ochrony udostępnianych danych osobowych w sposób gwarantujący ich poufność, integralność oraz dostępność, poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych, adekwatnych do charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób, których dane dotyczą.