Załącznik nr 1 do umowy
znak sprawy: 20/DI/PN/2020

Szczegółowy opis przedmiotu zamówienia

I. Dostawa 2 urządzeń typu Firewall

Lp.	Wymagania minimalne
Architektura urządzenia	
1	Urządzenie musi stanowić dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań serwerowych bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia
2	Urządzenie musi pełnić rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall)
3	Urządzenie musi być wyposażone w co najmniej 8 portów 10 Gigabit Ethernet SFP
4	Urządzenie musi obsługiwać interfejsy VLAN (802.1Q) na interfejsach fizycznych – min. 1.000 sieci VLAN
5	Urządzenie musi być wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band
6	Urządzenie musi być wyposażone w port USB 2.0 lub nowszy
7	Urządzenie musi posiadać zasilacze redundantne umożliwiające zasilanie prądem przemiennym 230V
8	Urządzenie o wysokości maksymalnej 2U, przystosowane do montażu w szafie rack 19'' (wymagane jest dostarczenie niezbędnych elementów montażowych)
Parametry wydajnościowe	
9	Urządzenie musi posiadać przepustowość dla uruchomionych modułów firewall'a, kontroli aplikacji i systemu IPS na poziomie co najmniej 20 Gb/s dla pakietów o wielkości maksymalnie 1024 bajtów
10	Urządzenie musi obsługiwać min. 10.000 połączeń VPN (Gateway-to-Gateway IPsec) z maksymalną sumaryczną przepustowością 6 Gbps dla pakietów o wielkości maksymalnie 1024 bajtów
11	Wymagana liczba sesji (z kontrolą aplikacji) co najmniej 8.000.000 z możliwością zestawiania 150.000 nowych połączeń na sekundę
Funkcjonalność urządzenia	
12	Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
13	Urządzenie musi umożliwiać podział na niezależne logiczne instancje. Urządzenie musi posiadać możliwość uruchomienia minimum 5 w pełni funkcjonalnych logicznych instancji tzw. wirtualnych firewalli, tj. wirtualnych instancji w ramach jednego urządzenia fizycznego, pozwalających na niezależną konfigurację i separację.
14	Urządzenie musi posiadać możliwość uruchomienia urządzenia w trybie firewall'a L3 oraz w trybie transparentnym
15	Urządzenie musi obsługiwać routing statyczny i dynamiczny (co najmniej: RIP, OSPF, BGP)
16	Urządzenie musi posiadać możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory
17	Urządzenie musi obsługiwać funkcjonalność Network Address Translation (NAT) wraz z Port Address Translation (PAT)
18	Urządzenie musi zapewniać mechanizmy redundancji, w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby

19	Urządzenie musi zapewniać funkcjonalność tzw. Firewall'a Next-Generation w zakresie: – systemu automatycznego wykrywania i klasyfikacji aplikacji – systemu IPS – systemu antymalware
20	Urządzenie musi zapewniać możliwość dodatkowej rozbudowy funkcjonalności w zakresie systemu filtracji ruchu w oparciu o URL
21	Urządzenie musi posiadać funkcjonalność wykrywania aplikacji, zapewniającą: – możliwość klasyfikacji ruchu i wykrywania co najmniej 1500 aplikacji – możliwość definiowania sygnatur aplikacyjnych pozwalających na skonfigurowanie opisu dowolnej aplikacji i wykorzystania go do automatycznego wykrywania oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz raportach
22	Urządzenie musi posiadać funkcjonalność systemu IPS zapewniającego: – możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system) – możliwość wykrywania i blokowania szerokiej gamy zagrożeń, w tym: o złośliwe oprogramowanie o skanowanie sieci o ataki na usługę VoIP o próby przepełnienia bufora o ataki na aplikacje P2P o zagrożenia dnia zerowego – możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna) – możliwość inspekcji warstwy sieciowej i informacji zawartych w nagłówkach pakietów oraz również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego, włącznie z możliwością sprawdzania zawartości pakietu – możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń – wiele możliwości reakcji na zdarzenia w tym takie, jak: o tylko monitorowanie o blokowanie ruchu zawierającego zagrożenia o zapisywanie pakietów – możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji – możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie
23	Urządzenie musi posiadać funkcjonalność polegająca na wykrywaniu i śledzeniu transferu następujących kategorii plików w ruchu sieciowym: – pliki graficzne – pliki PDF – pliki wykonywalne – pliki multimedialne – pliki pakietu Office – pliki skompresowane

24	Urządzenie musi posiadać możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: – HTTP – SMTP – FTP – IMAP – POP3
25	Urządzenie musi posiadać wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i umożliwiać: – sprawdzenie reputacji plików w systemie globalnym – sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze) – statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu
	Zarzadzanie
26	Zarządzanie musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli
27	Wraz z urządzeniami musi zostać dostarczona dedykowana platforma zarządzająca w formie maszyny fizycznej (pozwalająca na przechowywanie 10 GB logów dziennie przez okres 24 miesięcy) lub maszyny wirtualnej (Virtual Appliances for Vmware – środowisko wirtualizacyjne posiadane przez Zamawiającego)
28	Platforma zarządzająca musi: - umożliwiać centralne budowanie i dystrybucję polityk bezpieczeństwa, aktualizację oprogramowania i sygnatur oraz funkcje audytu i backupu konfiguracji - zapewniać interfejs, który może zostać dostosowany do wymagań użytkownika, w szczególności administrator posiada możliwość definiowania widoków (dashboard), które spełniają jego indywidualne kryteria - umożliwiać agregację i przechowywanie wszystkich zdarzeń historycznych (za okres 24 miesięcy, szacunkowa ilość logów dziennie 10 GB) oraz centralne monitorowanie i analizę działającą w czasie rzeczywistym - umożliwiać logowanie wszystkich czynności wykonywanych przez administratora - umożliwiać generowanie raportów włączając w to raporty predefiniowane oraz możliwość kompletnego dostosowania raportów do wymagań użytkownika - pozwalać na informowanie o zagrożeniach poprzez: wysłanie e-maila, trapa SNMP, przesłanie informacji do serwera Syslog
	Dodatkowe wymagania
29	Oferowane urządzenie w dniu składania ofert nie może być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży
30	Wraz z urządzeniem należy dostarczyć: - niezbędne okablowanie do podłączenia firewalli do sieci elektrycznej i LAN - sześć modułów optycznych 10GBASE-SR pochodzących z oferty producenta urządzenia

II. Dostawa 2 przełączników

Lp.	Wymagania minimalne
Architektura urządzenia	
1	Urządzenie musi pełnić rolę przełącznika warstwy 3
2	Urządzenie musi być wyposażone w co najmniej: - 24 porty 10/100/1000 BaseT RJ-45 - 8 porów 1/10G SFP/SFP+
3	Urządzenie musi mieć możliwość stackowania z zapewnieniem następujących funkcjonalności: – 6 urządzeń w stosie, – Zarządzanie poprzez jeden adres IP, – Możliwość tworzenia połączeń cross-stack Link Aggregation zgodnie z IEEE 802.3ad
4	Zasilanie i chłodzenie: – Redundantne i wymienne moduły wentylatorów – Dwa redundantne zasilacze 230V AC
5	Urządzenie o wysokości 1U, przystosowane do montażu w szafie rack 19'' (wymagane jest dostarczenie niezbędnych elementów montażowych)
Parametry wydajnościowe	
6	Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów. Przepustowość przełącznika (switching capacity): 200 Gb/s (bez podłączenia do stosu).
7	Pamięć: – Bufor pakietów – 16MB – DRAM – 8GB – Flash – 16 GB
8	Pozostałe parametry minimalne: – 1000 aktywnych sieci VLAN – 30000 adresów MAC – 8000 tras IPv4 – 4000 tras IPv6 – Ilość wpisów w listach kontroli dostępu Security ACL – 5000 – ilość wpisów w listach kontroli dostępu QoS ACL – 5000 – 1000 interfejsów SVI L3 – 128 interfejsów L3 – 128 połączeń zagregowanych typu „port channel"

Funkcjonalność urządzenia	
9	Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: – IEEE 802.1w Rapid Spanning Tree – Per-VLAN Rapid Spanning Tree (PVRST+) – IEEE 802.1s Multi-Instance Spanning Tree
10	Mechanizmy związane z bezpieczeństwem sieci: – Obsługa funkcji : Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, – Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+ – Obsługa list kontroli dostępu (ACL)
11	Mechanizmy związane z zapewnieniem jakości usług w sieci: – Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi – Implementacja algorytmu Shaped Round Robin dla obsługi kolejek – Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP źródłowy/docelowy port TCP – Kontrola sztormów dla ruchu broadcast/multicast/unicast
12	Obsługa protokołów i mechanizmów routingu: – Routing statyczny dla IPv4 i IPv6 – Routing dynamiczny – RIP, OSPF, IS-IS i BGP dla IPv4 i IPv6 – Policy-based routing (PBR)
13	Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
Zarządzanie	
14	Funkcje zarządzania: – Port konsoli – Dedykowany port Ethernet do zarządzania out-of-band – Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją – Obsługa protokołów SNMPv3, SSHv2, https, syslog – Port USB umożliwiający podłączenie zewnętrznego nośnika danych
Dodatkowe wymagania	
15	Oferowane urządzenie w dniu składania ofert nie może być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży
16	Wyposażenie urządzenia – zasilacz redundantny o mocy identycznej jak zasilacz podstawowy – moduł do łączenia w stos wraz z kablem stakującym o długości 50 cm – dwa moduły optyczne SFP/SFP+ 10GBASE-LR pochodzące z oferty producenta przełącznika – dwa moduły optyczne SFP/SFP+ 10GBASE-SR pochodzące z oferty producenta przełącznika

III. Zakres prac wdrożeniowych

W ramach przygotowania do wdrożenia Sprzedawca:

1. Przeprowadzi analizę konfiguracji posiadanych przez Kupującego urządzeń: Palo Alto Networks, Cisco ASR, Cisco ASA, Cisco Nexus, Juniper SRX, w zakresie niezbędnym do przygotowania projektu technicznego.
2. Opracuje projekt techniczny, który musi zawierać m.in.:
    1) Opis techniczny i funkcjonalny dostarczonych urządzeń.
    2) Specyfikację parametrów fizycznych i środowiskowych, tj.: wagę, rozmiar, parametry zasilania, emitowane ciepło.
    3) Opis zastosowania najlepszych praktyk producenta urządzeń w ramach wdrażanej konfiguracji.
    4) Koncepcję podłączenia dostarczanych urządzeń do istniejącej infrastruktury Kupującego – schemat podłączenia fizycznego i logicznego. Dostarczone urządzenia mają zastąpić użytkowane przez Kupującego urządzenia Cisco ASA5585-SSP-20 (klaster).
    5) Zakres prac i zmian konfiguracyjnych.
    6) Opis sposobu migracji dotychczasowej konfiguracji na nowe urządzenia.
    7) Procedurę i harmonogram przełączenia sieci na dostarczone urządzenia z uwzględnieniem wymogu prowadzenia prac w dniu ustawowo wolnym od pracy lub w nocy ze względu, że prace wykonywane będą na produkcyjnie działającej infrastrukturze. **Kupujący dopuszcza przerwę techniczną w działaniu infrastruktury IT (powodującą niedostępność usług IT) wynoszącą 1 godzinę, w czasie którego Wykonawca dokona przełączenia ruchu sieciowego na dostarczone urządzenia.**

   Kupujący w terminie 3 dni od otrzymania projektu technicznego dokona jego akceptacji lub zgłosi uwagi. Warunkiem rozpoczęcia prac wdrożeniowych jest zaakceptowanie przez Kupującego projektu technicznego.

W ramach wdrożenia firewalli Sprzedawca zgodnie z zaakceptowanym projektem technicznym:

1. Zainstaluje dostarczane urządzenia w szafach RACK, podłączy do sieci: elektrycznej i LAN, skonfiguruje zarządzanie urządzeniami.
2. Dostosuje konfigurację istniejących urządzeń, aby umożliwić podłączenie dostarczonych urządzeń.
3. Wykona konfigurację urządzeń właściwą dla docelowego środowiska, obejmującą migrację konfiguracji z posiadanych przez Kupującego firewalli Cisco ASA 5585 na dostarczane urządzenia.
4. Skonfiguruje mechanizmy ochrony typu IPS oraz antymalware.
5. Wykona przełączenie ruchu sieciowego na dostarczone urządzenia.
6. Wykona testy akceptacyjne (plan testów Sprzedawca przedstawi Kupującemu do akceptacji).
7. Wykonana dokumentację powykonawczą i procedury eksploatacyjne.
8. Przeprowadzi warsztaty, min. 2 dni po 5 godzin, na których Sprzedawca przeszkoli Kupującego z podstawowej obsługi wdrożonych urządzań.
9. Dostarczy jeden voucher na autoryzowane szkolenie z zakresu podstawowej konfiguracji dostarczonych firewalli. Szkolenie musi trwać co najmniej 3 dni, być prowadzone w języku polskim w ośrodku szkoleniowym na terenie Warszawy. Sprzedawca dostarczy Kupującemu voucher ważny do 31.12.2021 r.

IV. Szczegółowe warunki serwisu gwarancyjnego i wsparcia technicznego:

1. Urządzenia muszą być fabrycznie nowe i nieużywane wcześniej w żadnych innych projektach. Nie dopuszcza się urządzeń typu refubrished (zwróconych do producenta i później odsprzedawanych ponownie przez producenta).
2. Wszystkie karty oraz interfejsy dokładane do urządzeń muszą pochodzić od tego samego producenta sprzętu.
3. Sprzedawca zapewni bezpłatny serwis gwarancyjny w okresie obowiązywania gwarancji.
4. Serwis gwarancyjny musi być świadczony w oparciu o świadczenia gwarancyjne producenta sprzętu i zapewniać prawo do aktualizacji oprogramowania zainstalowanego na urządzeniach oraz baz sygnatur IPS. Sprzedawca zobowiązuje się do zapewnienia Kupującemu konta w serwisach internetowych producenta sprzętu, które umożliwi przeglądanie baz wiedzy, informacji o nowych wersjach oprogramowania systemowego, firmware, poprawkach/aktualizacjach, zaleceniach/rekomendacjach oraz pobierania wcześniej wymienionego oprogramowania.
5. Gwarancji podlegają stwierdzone w dostarczonych urządzeniach wady materiałowe i konstrukcyjne, a także niespełnianie deklarowanych przez producenta funkcji użytkowych.
6. Sprzedawca przystąpi do naprawy urządzeń nie później niż następnego dnia roboczego od zgłoszenia awarii.
7. Serwisowanie sprzętu odbywać się będzie w dni robocze w godzinach pracy Kupującego, tj. od godz. 8:15 do godz. 16:15.
8. Naprawa urządzeń odbywać się będzie w miejscu wskazanym przez Kupującego. Naprawa może odbyć się w serwisie, jeżeli Sprzedawca uzna to za konieczne, przy czym Sprzedawca transportuje uszkodzony sprzęt do serwisu, a po naprawie z serwisu, na własny koszt i ryzyko.
9. Po wykonaniu napraw urządzeń poza siedzibą Kupującego, Sprzedawca zobowiązuje się dokonać ponownej instalacji sprzętu w środowisku Kupującego.
10. **Termin naprawy urządzeń sieciowych wynosi maksymalnie 1 dzień roboczy od daty otrzymania zgłoszenia awarii przez Sprzedawcę.** Dla zgłoszeń po godz. 15:00 lub w dni ustawowo wolne od pracy, jako datę zgłoszenia przyjmuje się datę pierwszego dnia roboczego.
11. W przypadku gdy czas usunięcia awarii przekracza 2 dni robocze, Sprzedawca zobowiązuje się do dostarczenia sprzętu zastępczego o parametrach nie gorszych od sprzętu uszkodzonego oraz do jego instalacji.
12. Okres gwarancji zostanie przedłużony o łączną liczbę dni, podczas których sprzęt był wyłączony z eksploatacji z powodu naprawy w okresie objętym gwarancją, o ile nie dostarczono sprzętu zastępczego. Liczbę tę określa się jako liczbę dni, która upłynęła pomiędzy datą zgłoszenia awarii przez Kupującego, a datą naprawy lub dostarczenia naprawionego sprzętu przez Sprzedawcę.
13. W razie odrzucenia reklamacji przez Sprzedawcę, Kupujący może zlecić przeprowadzenie niezależnej ekspertyzy.
14. Jeżeli reklamacja Kupującego okaże się uzasadniona, koszty związane z przeprowadzeniem ekspertyzy ponosi Sprzedawca.
15. Podczas usuwania awarii urządzeń Sprzedawca zobowiązuje się przestrzegać wymagań wynikających m.in. z polityki bezpieczeństwa lub procedur stosowanych u Kupującego, z którymi Kupujący zapozna Sprzedawcę niezwłocznie po zawarciu umowy.
16. Uprawnienia wynikające z udzielonej gwarancji nie wyłączają możliwości dochodzenia przez Kupującego uprawnień z tytułu rękojmi za wady.
17. W ramach wsparcia technicznego Sprzedawca zapewni …. godzin *(liczba godzin zostanie określona na podstawie oferty Sprzedawcy)* wsparcia technicznego inżyniera/ów Sprzedawcy przez okres 12 miesięcy od daty odbioru przedmiotu umowy, obejmującą pomoc techniczną dotyczącą dostarczonych urządzeń. Wsparcie techniczne świadczone będzie w dni robocze w godzinach 8:00-16:00. W przypadku konieczności świadczenia wsparcia technicznego w godzinach 16:00-8:00 lub w dniach wolnych od pracy – termin zostanie uzgodniony ze Sprzedawcą z 3 dniowym wyprzedzeniem.