Załącznik nr 1 do SWZ – Opis przedmiotu zamówienia- po zmianie z dnia 06.08.2021 r.

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu sieciowego

I. Przedmiot zamówienia

Przedmiotem zamówienia jest

1. dostawa sprzętu sieciowego wraz z oprogramowaniem oraz usługa wdrożenia Systemu,
2. usługa wsparcia technicznego,
3. dostawa voucherów na szkolenia dla administratorów systemu z data ważności nie krócej niż 6 miesięcy od dnia wdrożenia Systemu.

II. Terminy

Zamówienie będzie realizowane w następujących terminach:

1. dostawa sprzętu sieciowego wraz z oprogramowaniem oraz wdrożenie systemu - do 3 miesięcy, liczone od daty zawarcia Umowy,
2. usługa wsparcia technicznego - 36 miesięcy, liczone od dnia wdrożenia systemu,
3. dostawa voucherów dla administratorów systemu – do 3 miesięcy, liczone od daty zawarcia Umowy.

III. Wymagania dotyczące urządzeń

	Wymagania wspólne dla wszystkich urządzeń firewall. (Wymagania minimalne)
1	1. Muszą to być specjalizowane urządzenia sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako klaster wysokiej dostępności (HA) w trybach Active/Standby oraz Active/Active. 2. Specjalizowane urządzenia sieciowe i towarzyszące oprogramowanie musi być dostarczone i wspierane przez jednego producenta. Producent oferowanego rozwiązania musi być obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders przynajmniej od 4 lat. 3. Urządzenia muszą umożliwiać działanie w następujących trybach pracy: a. rutera (tzn. w warstwie 3 modelu OSI), b. mostu (tzn. w warstwie 2 modelu OSI), c. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; Musi pracować w trybie przezroczystego łączenia interfejsów w pary.). d. w trybie pasywnego nasłuchu (sniffer/tap). System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu. 4. Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45 lub w co najmniej jeden port konsoli w standardzie USB oraz w co najmniej jeden dedykowany port zarządzający 10/100/1000 BASE-T. Wymagane jest dostarczenie wraz z oferowanymi urządzeniami odpowiednich kabli konsolowych, które umożliwiają podłączenie ich do komputera przez port USB 2.0 lub 3.0. Lub równoważny Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45 oraz w co najmniej jeden port konsoli w standardzie USB oraz w co najmniej jeden

dedykowany port zarządzający 10/100/1000 BASE-T. Razem z urządzeniem należy dostarczyć kabel konsolowy oraz kabel Ethernet.

5. Urządzenia firewall muszą posiadać budowę z odseparowanymi zasobami. Procesory zarządzające oraz pamięć (tzw. Management Plane) muszą być oddzielne od procesorów i pamięci przetwarzających ruch sieciowy (tzw. Data Plane). Lub równoważny Urządzenia firewall muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu od zasobów służących do zarządzania urządzeniem.
6. Nadmierne obciążenie ruchem sieciowym (Data Plane) urządzenia nie może blokować funkcjonowania części zarządzającej (Management Plane). Nie może powodować problemów z konfigurowaniem czy monitorowaniem urządzenia, dostępem do interfejsu GUI i CLI. Lub równoważny Urządzenia firewall muszą posiadać dedykowane zasoby procesora (CPU) do funkcji zarządzania urządzeniem lub możliwość ustawienia dedykowanego procesora do funkcji zarządzania urządzeniem.
7. Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN. Lub równoważne Urządzenia firewall muszą wspierać protokół Ethernet z obsługą VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.
8. Urządzenia firewall muszą wspierać protokół LACP.
9. Urządzenia firewall muszą zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
10. Urządzenia firewall muszą działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.
11. Polityka zabezpieczeń firewall musi uwzględniać
    a. adresy IP źródłowe i docelowe,
    b. protokoły i usługi sieciowe,
    c. aplikacje,
    d. kategorie URL,
    e. użytkowników aplikacji i grupy,
    f. reakcje zabezpieczeń,
    g. rejestrowanie zdarzeń
    h. strefa wejściowa i wyjściowa
12. Urządzenia firewall muszą automatycznie identyfikować aplikacje bez względu na numery portów (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Urządzenie musi wykrywać co najmniej 3000 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. Muszą pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia (bez użycia zewnętrznych narzędzi).
13. Urządzenia firewall muszą pozwalać na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.
14. Urządzenia firewall muszą zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.
15. Urządzenia firewall muszą być wyposażone w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy dostarczyć odpowiednie dla minimum 20 użytkowników.
16. Dostęp do urządzeń i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
17. Urządzenia firewall muszą umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż: baza lokalna, serwer Radius, serwer TACACS+, serwer AD, serwer LDAP. Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH a dla dostępu GUI za pomocą certyfikatów kryptograficznych.

18. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
    a. a) Active Directory,
    b. b) Terminal Services
19. Polityka kontroli dostępu (urządzeń firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości musi odbywać się również transparentnie.
20. Urządzenia firewall muszą umożliwiać synchronizację i wymianę danych o użytkownikach pomiędzy sobą z wykorzystaniem centralnego systemu zarządzania opisanego w dalszej części wymagań.
21. Urządzenia firewall muszą pozwalać na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL.
22. Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF i CSV. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu. Sposób realizacji możliwy jest również jako rozwiązanie równoważne przez dostarczenie dodatkowego, lokalnego systemu logowania który powinien mieć takie same możliwości w każdej lokalizacji objętej postępowaniem. Po odzyskaniu połączenia z punktem centralnym musi być możliwe zsynchronizowanie lokalnych logów i raportów z lokalnych systemów z centralnym systemem zarządzania. W przypadku rozwiązania z dodatkowym lokalnym systemem logowania w każdej lokalizacji, musi zostać zapewniony poziom redundancji zasilania i dysków, który umożliwi kontynuację pracy nawet w wypadku awarii jednego z tych komponentów. Lub równoważny Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV lub XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika na przestrzeni wskazanego zakresu czasu. Równoważnie dopuszczona jest realizacja za pomocą lokalnego systemu logowania, który zostanie zainstalowany w każdej lokalizacji objętej postępowaniem. W przypadku przerw w łączności WAN, po odzyskaniu połączenia z głównym systemem zarządzania (centralnym) musi być dokonywana synchronizacja lokalnych logów i raportów z systemem centralnym. W przypadku rozwiązania z dodatkowym lokalnym systemem logowania w każdej lokalizacji musi on posiadać te same wymagania serwisowe co centralny system zarządzania.
23. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
    a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
    b. API

    lub równoważny

    Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników.

    Musi istnieć możliwość dynamicznego przypisania użytkownika do grupy w odpowiedzi na wykryte przez firewall zdarzenia bezpieczeństwa powiązane z tym użytkownikiem.

    Musi istnieć możliwość zdefiniowania poziomu krytyczności zdarzenia bezpieczeństwa, które wyzwoli automatyczne przypisanie użytkownika do grupy.

    Musi istnieć możliwość przypisania użytkownika do takiej grupy również przez zewnętrzne narzędzia bezpieczeństwa celem umożliwienia integracji systemów bezpieczeństwa w obecnym i przyszłym posiadaniu Zamawiającego. Urządzenie musi realizować w/w integrację przez API.

    Do dynamicznej grupy użytkowników musi być dodawana nazwa użytkownika. Nie dopuszcza się, aby do takiej grupy dodawany był tylko adres IP.
24. Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESX i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można potem wykorzystywać w polityce bezpieczeństwa urządzeń.
25. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF dla IPv4 i IPv6.
26. Urządzenia firewall muszą obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
27. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa. Lub równoważne Urządzenia firewall muszą obsługiwać NAT64.
28. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi.
29. Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju.

30. Urządzenia firewall muszą obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL oraz TLS 1.2, TLS 1.3.
31. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa.
32. Wykonywanie operacji deszyfrowanie ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji ułatwiającej diagnostykę.
33. Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL.
34. Dla deszyfrowania ruchu TLS 1.3 wymagane jest wsparcie dla X25519, X448 oraz minimum dla zestawów protokołów: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384 oraz TLS_CHACHA20_POLY1305_SHA256.
35. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
36. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) i ustawiania dla aplikacji priorytetu oraz pasma.
37. Urządzenia firewall muszą umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. routing-based VPN).
38. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
39. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
40. Urządzenia firewall muszą zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tuneli SSH.
41. Urządzenia firewall muszą posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
42. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur albo powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.
43. Urządzenia firewall muszą posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu lub na konsoli zarządzającej.
44. Urządzenia firewall muszą posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół minimum: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż raz na dobę i pochodzić od tego samego producenta co firewall.
45. Urządzenia firewall muszą posiadać funkcję anty-spyware. Baza sygnatur musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.
46. Urządzenia firewall muszą posiadać funkcję filtrowania URL.
47. Funkcja filtrowania URL musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
48. Urządzenia firewall muszą umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „SandBox" plików wykonywalnych PE i DLL przechodzących przez firewall. Systemy sandbox, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików, adresów IP, DNS i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik. Oczekiwany interwał aktualizacji raz na dobę.
49. Urządzenia firewall muszą wykrywać i blokować zagrożenia DNS - wykrywający i blokujący ruch do domen uznanych za złośliwe musi być sterowany (przekierowanie) za pomocą funkcji DNS Sinkholing.
50. Urządzenia firewall muszą obsługiwać funkcję DNS proxy.
51. Urządzenia firewall muszą obsługiwać funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta musi być realizowana na bazie technologii SSL VPN oraz IPSec. Jeżeli oprogramowania klienta Remote Access VPN dla laptopów z systemem Windows wymaga licencji – należy dostarczyć licencję na maksymalną wydajność oraz maksymalną ilość dla oferowanego typu urządzeń.
52. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.
53. Dostarczane razem z urządzeniami subskrypcje, licencje, gwarancje producenta muszą być ważne przez okres 36 miesięcy.
54. Dla wszystkich urządzeń Firewall łącznie wymagane jest dostarczenie 18 szt. kompatybilnych wkładek światłowodowych SFP+ zgodnych ze standardem IEEE 802.3ae 10GBASE-SR.

2	Wymagania dodatkowe - urządzenia Centralne – 2 szt. (para HA) 1. Urządzenie będzie pracowało w trybie HA. 2. Urządzenie musi być wyposażone w minimum: a. 12 interfejsów 10/100/1000 Ethernet (RJ45) b. 8 interfejsów Ethernet (tzw. elastycznych) obsługujących tryb 1G/10G akceptujących odpowiednio wkładki SFP/SFP+. Interfejsy pracują w trybie 1Gbps lub 10Gbps w zależności od zainstalowanej wkładki. c. 4 interfejsy 40GE Ethernet (QSFP+). d. 1 dedykowany port HA, 10GE Ethernet (SPF+). 3. Urządzenie musi być wyposażone w dysk systemowy SSD minimum 220 GB potrzeby systemu operacyjnego i logów. Dysk musi mieć możliwość wymiany bez potrzeby rozkręcania urządzenia. Lub równoważne Urządzenie musi być wyposażone w przestrzeń na logi i system operacyjny w postaci innej niż obrotowy dysk twardy (HDD) o wielkości minimum 200 GB. Zamawiający wymaga, aby wymiana uszkodzonego urządzenia umożliwiała odesłanie urządzenia (RMA) bez nośnika danych (dysku). 4. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: a. Minimum 9 Gbps dla rozpoznawania i kontroli aplikacji, b. Minimum 5 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Anty-wirus, Anty-spyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia. c. Minimum 100 000 nowych sesji na sekundę. d. Minimum 3 000 000 równoległych sesji 5. Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia oraz odpowiednio większą instalację systemu zarządzania (dotyczy liczby zarządzanych firewalli logicznych) 6. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 10 000 reguł polityki bezpieczeństwa. 7. Urządzenia firewall muszą zabezpieczać działanie protokołu DNS poprzez procesowanie zapytań DNS w celu wykrywania i blokowania: zagrożeń, wycieku danych (exfiltracja), tunelowania DNS. Urządzenia muszą posiadać ciągły (on-line) dostęp do centralnego repozytorium zagrożeń DNS, który będzie wykorzystywany w procesie decyzyjnym funkcjonalności. 8. Urządzenia firewall dla zdalnego dostępu VPN muszą umożliwiać zaawansowane funkcjonalności: a. Realizacja VPN dla aplikacji HTML/HTML5 w trybie przeglądarkowym (tzw. Clientless VPN) b. Zestawianie zdalnego dostępu dla urządzeń mobilnych tzw. smart devices. Telefony/tablety bazujące na systemach operacyjnych: Apple iOS, Google Android. c. Dostępność oprogramowania klienckiego VPN dla urządzeń mobilnych z systemami: Apple iOS (10-13), Android (6-10), Win 10 UWP d. Dostępność oprogramowania klienta VPN dla stacji/laptopów z systemami: Windows 7-10, Ubuntu 14-20, CentOS 7-8, macOS 10.11-10.15. e. Możliwość zestawiania połączeń zdalnego dostępu VPN za pomocą IPv6 f. Sprawdzanie informacji o systemie operacyjnym, aktualizacji poprawek OS, aktualizacji oprogramowania antywirusowego itp. dla systemów Windows. g. Sprawdzanie obecności konta urządzenia w systemie katalogowym Windows AD dla systemów Windows. h. Możliwość pomijania tunelu zdalnego dostępu VPN dla specyficznych aplikacji, domeny DNS, aplikacji video. Dla podłączających się stacji/laptopów Windows i MacOS. i. Dodatkowa identyfikacja urządzeń użytkownika na bazie unikalnego identyfikatora innego niż adres IP (Windows – MachineGuid, Android – Android ID, iOS – UDID) pozwalająca na blokadę dostępu VPN dla wybranego urządzenia. Np. blokada dostępu VPN dla urządzenia zainfekowanego. 9. Urządzenie musi być wyposażone w minimum 2 zasilacze typu AC 230V pracujące redundantnie. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy

	urządzenia. 10. Urządzenie musi być przeznaczone do montażu w szafie Rack 19” z maksymalnym rozmiarem 3RU. Montaż 4 punktowy – przód + tył urządzenia.
3	Wymagania dodatkowe - urządzenia Średnie – 7 szt. 1. Urządzenie musi być wyposażone w minimum: a. 4 interfejsy 10/100/1000 Ethernet (RJ45) b. 4 interfejsy 1GE Ethernet w formie SFP c. 1 dedykowany port HA, 10/100/1000 Ethernet (RJ45). 2. Urządzenie musi być wyposażone w dysk systemowy SSD wielkości minimum 220 GB na potrzeby systemu operacyjnego i logów. Lub równoważne Urządzenie musi być wyposażone w przestrzeń na logi i system operacyjny w postaci innej niż obrotowy dysk twardy (HDD) o wielkości minimum 220 GB. Zamawiający wymaga, aby wymiana uszkodzonego urządzenia umożliwiała odesłanie urządzenia (RMA) bez nośnika danych (dysku). 3. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: a. Minimum 1,4 Gbps dla rozpoznawania i kontroli aplikacji, b. Minimum 0,8 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Anty-wirus, Anty-spyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia. c. Minimum 8 000 nowych sesji na sekundę. d. Minimum 110 000 równoległych sesji 4. Urządzenie musi obsługiwać nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia oraz odpowiednio większą instalację systemu zarządzania (dotyczy liczby zarządzanych firewalli logicznych) 5. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 1500 reguł polityki bezpieczeństwa 6. Urządzenie musi być wyposażone w minimum 1 zasilacz sieciowy AC 230V. 11. Urządzenie musi być przeznaczone do montażu w szafie Rack 19” z maksymalnym rozmiarem 2RU.
4	Wymagania dodatkowe - urządzenia Małe – 6 szt. 1. Urządzenie musi być wyposażone w minimum: a. 8 interfejsów 10/100/1000 Ethernet (RJ45) 2. Urządzenie musi być wyposażone w dysk systemowy SSD lub zasób dyskowy flash wielkości minimum 30 GB na potrzeby systemu operacyjnego i logów. Lub równoważne Urządzenie musi być wyposażone w przestrzeń na logi i system operacyjny w postaci innej niż obrotowy dysk twardy (HDD) o wielkości minimum 30 GB. Zamawiający wymaga, aby wymiana uszkodzonego urządzenia umożliwiała odesłanie urządzenia (RMA) bez nośnika danych (dysku). 3. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: a. Minimum 540 Mbps dla rozpoznawania i kontroli aplikacji, b. Minimum 320 Mbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Anty-wirus, Anty-spyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia.

	c. Minimum 4 000 nowych sesji na sekundę. d. Minimum 60 000 równoległych sesji 4. Urządzenie musi obsługiwać nie mniej niż 3 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia oraz odpowiednio większą instalację systemu zarządzania (dotyczy liczby zarządzanych firewalli logicznych) 5. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 500 reguł polityki bezpieczeństwa 6. Urządzenie musi być wyposażone w minimum 1 zasilacz sieciowy AC 230V. 7. Urządzenie musi być wykonane w wersji pasywnego chłodzenia (brak wentylatorów).

IV. Centralny System zarządzania

	Centralny system zarządzania – 1 szt.
1	1. Wraz z urządzeniami Firewall wymagane jest dostarczenie centralnego systemu zarządzania. 2. Wykreślono zapis. 3. Zamawiający dopuszcza budowę systemu w oparciu o kilka komponentów zarządzania oferowanych przez producenta firewalli i systemu zarządzania pod warunkiem, iż będą one pochodziły od jednego producenta i będą przez niego w całości serwisowane. Zamawiający wymaga, aby wymagania dotyczące liczby zarządzanych firewalli, pojemności przestrzeni dyskowej oraz możliwości rozbudowy były spełnione przez każdy z komponentów tworzących system zarządzania. Należy dostarczyć urządzenia sprzętowe a nie platformy VM. 4. System zarządzania, logowania i raportowania musi zostać dostarczony w postaci urządzenia dedykowanego sprzętowego. Maszyny wirtualne nie są akceptowane. 5. System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne: a. obsługa nie mniej niż 25 firewalli b. w przyszłości możliwość rozbudowy zarządzania do 400 urządzeń (jeżeli jest wymagana specjalna licencja na ilość urządzeń w chwili dostawy wymagana jest dla punktu a – 25 urządzeń i możliwość rozbudowy w przyszłości). c. zasób dyskowy RAID w rozmiarze co najmniej 16TB. d. zapewnienie możliwości rozbudowy przestrzeni RAID do rozmiaru co najmniej 48 TB lub więcej za pomocą dokupienia dodatkowych dysków bez potrzeby zakupu dodatkowych licencji lub subskrypcji. Zamawiający dopuszcza dostarczenie systemu, który nie będzie posiadał opcji rozbudowy, ale w momencie dostawy będzie posiadał przestrzeń RAID o rozmiarze co najmniej 48TB. e. Wymiana uszkodzonego urządzenia umożliwia odesłanie urządzenia (RMA) bez nośników danych (dysków). 6. System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z urządzeń firewall. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach. 7. System musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli. 8. System zarządzania, logowania i raportowania musi zapewniać narzędzia dla szybkiej i skutecznej analizy informacji w tym co najmniej a. umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych. b. tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego. c. zapisywanie stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.

	d. tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down” 9. System zarządzania, logowania i raportowania musi umożliwiać centralne zarządzanie wieloma firewallami w tym co najmniej: a. budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu. i. lokalnych (dla wybranych firewalli) ii. globalnych (dla grup firewalli). b. umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery lub logiczne grupy urządzeń umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów). 10. Pozwalać na tworzenie raportów na podstawie zbudowanych kontenerów lub grup urządzeń a. umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium. b. umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych. 11. System zarządzania, logowania i raportowania musi umożliwiać centralne narzędzia inwentaryzacji i audytu oraz zarządzania konfiguracjami w tym co najmniej musi: a. umożliwiać dystrybucję i zdalną instalację nowych wersji systemu b. umożliwiać tworzenie kopii zapasowych zarządzanych firewalli. c. umożliwiać dystrybucję i zdalną instalację aktualizacji sygnatur. d. umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia przed jej zatwierdzeniem. e. pozwalać na zapisywanie różnych wersji konfiguracji zarządzanych firewalli. f. umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone g. informować o zmianach konfiguracji systemu 12. System zarządzania, logowania i raportowania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń. 13. Urządzenie musi być wyposażone w minimum 2 zasilacze typu AC 230V pracujące redundantnie. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia. 14. Urządzenie musi być przeznaczone do montażu w szafie Rack 19” z maksymalnym rozmiarem 3RU. Montaż 4 punktowy – przód + tył urządzenia.

V. Wymagania dotyczące Dostawy i Usługi wdrożenia Systemu

W ramach dostawy Sprzętu usługi wdrożenia Systemu:

1. Wykonawca dostarczy urządzenia w następujących lokalizacjach:
   1) TDT - Transportowy Dozór Techniczny: ul. Puławska 125, 02-707 Warszawa,
   2) OT 1 - Oddział Terenowy TDT w Warszawie: ul. Puławska 125, 02-707 Warszawa,
   3) OT 2 - Oddział Terenowy TDT w Lublinie: Al. Witosa 1, 20-315 Lublin,
   4) OT 3 - Oddział Terenowy TDT w Krakowie: ul. Pocieszka 5, 31-408 Kraków,
   5) OT 4 - Oddział Terenowy w Katowicach: ul. Cedrowa 8, 40-181 Katowice,
   6) OT 5 - Oddział Terenowy TDT w Gdańsku: ul. Kętrzyńskiego 24 B, 80-376 Gdańsk,

7) OT 6 - Oddział terenowy TDT we Wrocławiu: ul. Solskiego 5, 52-401 Wrocław,
8) OT 7 - Oddział Terenowy TDT w Poznaniu: ul. Grunwaldzka 391, 60-173 Poznań,
9) OT 8 - Oddział Terenowy TDT w Szczecinie ul. Firlika 20, 71-673 Szczecin,
10) Zespół Inspektorów TDT w Białymstoku ul. Cieszyńska 3A, 15-371 Białystok,
11) Zespół Inspektorów TDT w Łodzi ul. Gdańska 136, 90-536 Łódź,
12) Zespół Inspektorów TDT w Kielcach, ul. Piotrkowska 12, 25-510 Kielce,
13) Zespół inspektorów w Rzeszowie ul. K.K. Baczyńskiego 1 35-210 Rzeszów,
14) Zespół Inspektorów TDT w Olsztynie ul. Szarych Szeregów 7, 10-079 Olsztyn,
15) Zespół Inspektorów TDT w Bydgoszczy ul. Zygmunta Augusta 14, 85-082 Bydgoszcz,

2. Rodzaje dostarczanych urządzeń do w/w lokalizacji będą uzgodnione z Zamawiającym.
3. Wszystkie oferowane urządzenia (wraz z zainstalowanym na nich Oprogramowaniem) muszą pochodzić od jednego producenta.
4. Dostarczane urządzenia muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed dniem dostawy, w oryginalnych opakowaniach transportowych producenta. Zamawiający dopuszcza rozpakowanie urządzeń przez Wykonawcę w celu przeprowadzenia przez Wykonawcę testu sprawności Routerów i wykonania ich konfiguracji wstępnej. Po dostarczeniu urządzeń do miejsca ich instalacji i wykonaniu prac instalacyjnych Wykonawca jest zobowiązany do usunięcia opakowań transportowych na własny koszt.
5. Każde z dostarczonych urządzeń, musi mieć zainstalowane rekomendowane do stosowania przez producentów Urządzeń wersje Oprogramowania. Ww. Oprogramowanie w dostarczonej wersji musi posiadać wsparcie techniczne producenta dostarczanych urządzeń.
6. Wszystkie urządzenia, w ramach całego zamówienia będą wyposażone w tą samą (identyczną) wersję Oprogramowania.
7. Każde z dostarczonych urządzeń, musi pochodzić z oficjalnego kanału dystrybucyjnego producenta, zapewniającego w szczególności realizację uprawnień gwarancyjnych.
8. Każde z urządzeń, zostanie dostarczone ze wszystkimi niezbędnymi elementami do zainstalowania w szafie rack 19”
9. Dostarczone Urządzenia w dniu złożenia oferty nie będą znajdować się na liście sprzętu przeznaczonego do wycofania z produkcji lub sprzedaży na terenie Polski.
10. Wykonawca uruchomi i przeprowadzi:
    1) instalację urządzenia w szafach telekomunikacyjnych, oraz dołączy urządzenia do wskazanych urządzeń produkcyjnych sieci,
    2) konfigurację urządzeń oraz systemu zarządzania
    3) konfigurację trybu wysokiej dostępności urządzeń
    4) konfigurację filtracji ruchu przychodzącego i wychodzącego
    5) konfigurację tuneli IPSEC pomiędzy centralą a wszystkimi oddziałami i zespołami Zamawiającego wymienionych.
    6) konfigurację min. trzech tuneli VPN dla pracowników Zamawiającego.
    7) konfigurację serwisu IPS.

8) konfigurację serwisu URL filtering.
9) konfigurację serwisu anty-malware
10) konfigurację z usługami katalogowymi
11) konfigurację z istniejącymi systemami bezpieczeństwa Zamawiającego
12) przeprowadzi test całości rozwiązania.

11. Wykonawca będzie zobowiązany do przeniesienia logów systemowych z aktualnie użytkowanych urządzeń firmy PALO ALTO NETWORKS tj. PA-3020, PA-500 i PA-200 oraz centralnego sytemu zarządzania PAN-PRA-25 do nowych urządzeń lub zachowanie tych logów w miejscu wyznaczonym przez Zamawiającego. Lub równoważne Wykonawca będzie zobowiązany do przeniesienia logów systemowych z aktualnie użytkowanych urządzeń firmy PALOALTONETWORKS tj. PA-3020, PA-500 i PA-200 w miejsce (do zasobu dyskowego) wyznaczonego przez Zamawiającego.
12. Wykonawca zobowiązany jest zachować polityki bezpieczeństwa wdrożone w aktualnych rozwiązaniach i przenieść je do nowych urządzeń w uzgodnieniu z Zamawiającym. Lub równoważne Wykonawca w ramach wdrożenia urządzeń firewall przeniesie obecne polityki z eksploatowanego aktualnie przez Zamawiającego klastra firewalli Palo Alto Networks oraz urządzeń oddziałowych. Proces wdrażania firewalli nie może spowodować przerwy dłuższej niż 60 minut. Wdrożenie musi się odbyć w przerwie serwisowej, której datę i godzinę wskaże Zamawiający na etapie uzgodnień z Wykonawca. Szczegółową konfiguracje obecnych reguł i polityk w obecnie używanych przez Zamawiającego firewallach Palo Alto, Zamawiajacy przekaże Wykonawcy wyłonionego w ranach niniejszego postępowania na etapie realizacji wdrożenia.
13. Wykonawca zobowiązany jest do przekazania Zamawiającemu dokumentacji technicznej powdrożeniowej zgodnie z wymaganiami określonymi w punkcie VI niniejszego OPZ.

VI. Wymagania - Dokumentacja techniczna (powdrożeniowa)

1. Dokumentacja musi zawierać szczegółowy opis techniczny zaimplementowanego rozwiązania wraz z konfiguracja urządzeń bezpieczeństwa i opisem uruchomionych funkcjonalności.
2. Dokumentacja techniczna będzie stanowiła dokument na podstawie którego będzie możliwe odbudowanie architektury zaimplementowanego rozwiązania bezpieczeństwa.
3. Szczegółowa konfiguracja urządzeń bezpieczeństwa przedstawiona zostanie w osobnych załącznikach.
4. Dokumentacja techniczna będzie zawierała:
   1) przedstawienie ogólnej architektury systemu bezpieczeństwa
   2) wykorzystywane elementy bezpieczeństwa,
   3) ogólna architektura wdrożenia,
   4) wykorzystywane mechanizmy sieciowe, bezpieczeństwa i redundancji
   5) przedstawienie szczegółowej architektury z konfiguracją funkcjonalności:
      a. sieciowych (adresacja IP; warstwy L2, L3 modelu ISO/OSI; trybami pracy urządzeń itp.),
      b. bezpieczeństwa (reguły bezpieczeństwa, funkcje IPS, antymalware itp.)

c. redundancji (sposób pracy, komunikacja pomiędzy elementami klastra, zarządzenia i monitorowanie klastra urządzeń)

6) przedstawienie metod oraz sposobów zarządzania i monitorowania rozwiązania bezpieczeństwa

7) załączniki z pełną konfiguracją urządzeń bezpieczeństwa.

VII. Wymagania - Usługa wsparcia technicznego świadczona przez Wykonawcę

1. W ramach realizacji zamówienia wymagane jest świadczenie usługi wsparcia technicznego przez Wykonawcę.
2. Wsparcie musi być świadczone przez okres 36 miesięcy od dnia wdrożenia systemu (w wymiarze do 8 godzin miesięcznie).
3. Usługa musi zawierać wsparcie techniczne świadczone on-site przez Wykonawcę.
4. Wsparcie techniczne będzie polegać w szczególności na:
   1) wsparciu w instalacji oprogramowania, tj. poprawek oprogramowania, najnowszych komercyjnie dostępnych wersji oprogramowania,
   2) zapewnieniu dostępu do narzędzi konfiguracyjnych i dokumentacji technicznej oprogramowania i urządzeń (o ile nie zapewnia tego producent).
   3) obsługa incydentów bezpieczeństwa.

VIII. Wymagania – Gwarancja Wykonawcy

1. Niezależnie od gwarancji producenta Urządzeń Wykonawca udzieli własnej gwarancji jakości na wszystkie zainstalowane Urządzenia.
2. Termin gwarancji – co najmniej 36 miesięcy od daty podpisania protokołu wdrożenia Systemu bez zastrzeżeń.
3. W ramach gwarancji Wykonawca zapewnia:
   1) bezawaryjne funkcjonowanie Sprzętu,
   2) naprawy Sprzętu:
      a. w miejscu jego lokalizacji (do końca pierwszego dnia roboczego po dniu zgłoszenia awarii),
         a jeżeli naprawa w miejscu jego lokalizacji okaże się niemożliwa
      b. w serwisie Wykonawcy lub producenta pod warunkiem zapewnienia Urządzenia tymczasowego (zwane dalej rozwiązanie tymczasowe) trwającego nie dłużej niż 30 dni liczone od końca pierwszego dnia roboczego po dniu zgłoszenia awarii. W przypadku zastosowania rozwiązania tymczasowego, Wykonawca dostarczy naprawione urządzenie w ciągu nie dłużej niż 30 dni od dnia zastosowania rozwiązania tymczasowego.
   3) wymianę Sprzętu (w przypadku braku możliwości dokonania jego naprawy) na fabrycznie nowy, wolny od wad, o takich samych lub lepszych parametrach techniczno-eksploatacyjnych i funkcjonalnych.
4. Pozostałe wymagania dotyczące gwarancji w tym sposób wykonywania serwisu gwarancyjnego określa Umowa która jest równocześnie dokumentem stanowiąym oświadczenie gwarancyjne Wykonawcy.

IX. Wymagania - Szkolenia

1. Wykonawca zapewni Zamawiającemu oficjalne/autoryzowane szkolenia producenta dla administratorów (w formie voucherów szkoleniowych) w zakresie każdego rodzaju oferowanego urządzenia. Szkoleniem należy objąć 4 osoby w wymiarze nie krótszym niż 80 godzin zegarowych dla każdej z osób.
2. Szkolenia zostaną zrealizowane przez autoryzowany przez producenta dostarczanych Urządzeń podmiot szkoleniowy.
3. Wykonawca zapewni certyfikaty dla uczestników, potwierdzające odbycie szkolenia.
4. Szkolenia zostaną przeprowadzone w języku polskim.
5. Czas ważności voucherów nie może być krótszy niż 6 miesięcy od dnia wdrożenia Systemu. Przekazanie voucherów musi nastąpić nie później niż wdrożenie Systemu.