**Opis Przedmiotu Zamówienia (OPZ)**

Przedmiotem Zamówienia jest dostawa i wdrożenie urządzeń firewall, m.in. w zakresie dostawy sprzętu i oprogramowania wraz z montażem, konfiguracją, integracją z infrastrukturą teleinformatyczną ZAMAWIAJĄCEGO oraz opracowania dokumentacji.

Opis parametrów technicznych sprzętu i oprogramowania został szczegółowo określony w opisie technicznym. Oferent jest zobowiązany dołączyć do oferty karty katalogowe oferowanych rozwiązań potwierdzające spełnienie wymagań Zamawiającego.

Sprzęt i oprogramowanie oferowane w ramach postępowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na rynek polski i musi być objęty serwisem oraz wsparciem technicznym przez okres 60 miesięcy od daty dostawy.

Dostarczony sprzęt musi być nowy i nieużywany we wcześniejszych projektach (nie dopuszcza się zastosowania urządzeń tzw. „*Refurbished”*.

Dostarczony sprzęt i oprogramowanie Wykonawca skonfiguruje w uzgodnieniu i zgodnie z wytycznymi Zamawiającego oraz będzie świadczył pełne wsparcie techniczne przez cały okres gwarancji obejmujące awarie, bieżące zmiany konfiguracji, aktualizację urządzeń itp. w trybie 8 godzin 5 dni w tygodniu z czasem reakcji na zgłoszenie do 4 godzin.

Wykonawca dostarczy wszystkie niezbędne licencje w ramach postępowania tak aby opisane niżej funkcjonalności były spełnione.

**Opis Techniczny:**

1. **Urządzenia klasy „Next-Generation Firewalls” z zaawansowanymi rozwiązaniami bezpieczeństwa i zarządzaniem. 1 komplet – 2 sztuki pracujące w klastrze w trybie „HA”.**
2. **Minimalne wymagania dla urządzeń NG firewall.**
3. Muszą to być specjalizowane urządzenia sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako para wysokiej dostępności (HA) w trybach Active/Standby, Active/Active.
4. Całość sprzętu i oprogramowania musi być dostarczona i zapewniać wsparcie serwisowe przez jednego i tego samego producenta.
5. Urządzenia muszą umożliwiać działanie w następujących trybach pracy:
	1. routera (tzn. w warstwie 3 modelu ISO OSI),
	2. mostu (tzn. w warstwie 2 modelu ISO OSI),
	3. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; Musi pracować w trybie przezroczystego łączenia interfejsów w pary) w trybie pasywnego nasłuchu (tzw. sniffer/tap).

System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.

1. Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45, w co najmniej jeden dedykowany port zarządzający realizowany jako port Ethernet 10/100/1000 lub jako port SFP z wkładką 1000BASE-T.
2. Urządzenia muszą być wyposażone w minimum 2 zasilacze AC 230V pracujące redundantnie.
3. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia tzw. “hot-plug”.
4. Urządzenia firewall muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu (tzw. data plane) od zasobów służących do zarządzania urządzeniem (tzw. management plane). Akceptowana jest separacja logiczna zasobów realizowana za pomocą przypisania dedykowanej ilości rdzeni zasobów procesorów (tzw. CPU cores) do obu z funkcji lub alternatywnie za pomocą oddzielnych dedykowanych procesorów (tzw. CPU) dla każdej z funkcji.
5. 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 min. 4000 znaczników VLAN.
6. Urządzenia firewall muszą wspierać protokół LACP.
7. 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).
8. 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.
9. Polityka zabezpieczeń firewall musi uwzględniać
	1. adresy IP źródłowe i docelowe,
	2. protokoły i usługi sieciowe,
	3. aplikacje,
	4. kategorie URL,
	5. użytkowników aplikacji i grupy,
	6. reakcje zabezpieczeń,
	7. logowanie zdarzeń (początek i koniec sesji)
	8. strefa wejściowa i wyjściowa
10. 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 3300 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz z aplikacjami przemysłowymi (tzw. ICS/OT) np. DNP3, Modbus.

Urządzenia muszą pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia (bez użycia zewnętrznych narzędzi).

1. Urządzenia firewall muszą pozwalać na blokowanie transmisji plików wybranego typu, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .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.
2. Urządzenia firewall muszą być zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji lub pobierania dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.
3. 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 przewidzieć odpowiednie licencje dla minimum 30 administratorów na wszystkie oferowane urządzenia.
4. 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.
5. Urządzenia firewall muszą umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż: baza lokalna, serwer Radius, serwer TACACS+, serwer AD/LDAP. Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH.
6. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie min. z systemami:
	1. Microsoft Active Directory,
	2. Microsoft Exchange
	3. Terminal Services
	4. Syslog
	5. Cisco ISE
7. 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.
8. 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, połączeniach VPN.
9. 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 i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.
10. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
	1. reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
	2. API
11. Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESXi i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można następnie wykorzystywać w polityce bezpieczeństwa urządzeń.
12. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.
13. 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.
14. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
15. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami informacji o NAT.
16. Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju. Konieczna jest obsługa Syslog za pomocą transportu UDP, TCP, SSL oraz obsługa formatów IETF oraz BSD.
17. Urządzenia firewall muszą obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
18. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji - rozdzielny od polityk bezpieczeństwa.
19. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS który nie ma zostać odszyfrowany, ale poddany sprawdzeniu czy certyfikat serwera nie wygasł oraz sprawdzeniu czy certyfikat nie pochodzi od zaufanego wystawcy. W takim przypadku urządzenie musi umożliwiać blokadę takiej sesji użytkownika.
20. Wykonywanie operacji deszyfrowanie ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji. Musi zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.
21. Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL (w przypadku, gdy jest wymagane jego dostarczenie) albo możliwość wykorzystania własnej utworzonej na urządzeniu listy URL które mają podlegać deszyfracji albo być z niej wykluczone (tzw. wyjątek).
22. Urządzenie firewall musi posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
23. 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, TLS\_CHACHA20\_POLY1305\_SHA256.
24. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości sesji w odniesieniu do źródłowego lub docelowego adresu IP.
25. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) dla aplikacji i użytkowników.
26. 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).
27. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
28. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
29. Urządzenia firewall muszą zapewniać inspekcję komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu blokowania tuneli SSH.
30. Urządzenia firewall muszą obsługiwać funkcję DNS proxy.
31. 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 klienckim Windows wymaga licencji – należy dostarczyć licencję na maksymalną wydajność oraz maksymalną ilość dla oferowanego typu urządzeń.
32. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.
33. Dostarczane razem z urządzeniami subskrypcje, licencje, gwarancje muszą funkcjonować min. **60** miesięcy.
34. W przypadku potrzeby wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby dyski zostały wymontowane z urządzenia i pozostały w jego siedzibie w celu bezpiecznej utylizacji.
35. **Wymagania dodatkowe dla urządzeń NG Firewall.**

Należy dostarczyć 2 szt. urządzeń, które będą pracowały jako 1 para w układzie HA.

Razem z urządzeniami muszą zostać dostarczone następujące typy i ilości modułów połączeniowych. Ilość dla zestawu 2 urządzeń głównych:

1. Do HA:4 szt. SFP+ 10GE wariant SR
2. Do LAN**:** 4 szt. SFP+ 10GE wariant SR

Każde z urządzeń musi (poza wymaganiami wspólnymi), spełniać dodatkowo wymagania:

1. Urządzenie musi być wyposażone w minimum:
	1. minimum 4 porty Ethernet RJ45 wspierających 100Mbps/1GE;
	2. minimum 4 porty Ethernet RJ45 wspierających 5G/2.5G/1GE/100Mbps;
	3. minimum 4 porty Ethernet RJ45 wspierających 5G/2.5G/1GE/100Mbps z zasilaniem PoE z budżetem 150W mocy oraz możliwością udostępnienia na porcie 50W mocy;
	4. minimum 2 portów Ethernet SFP (akceptujących moduły 1GE SFP)
	5. minimum 8 portów Ethernet SFP+ (akceptujących moduły 10GE SFP+ oraz 1GE SFP)
	6. minimum 1 port dla celów połączenia urządzeń w HA: minimum 1x 10GE SFP+ (lub szybszy) oraz minimum 2x 1GE (SFP lub RJ45) (lub szybszy). Porty te muszą być traktowane jako dodatkowe względem wymaganych powyżej. Nie dopuszcza się liczenia jako HA, portów wymaganych wcześniej.
2. Musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 200 GB na potrzeby systemu operacyjnego i logów.
3. W przypadku procedury wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby zasób dyskowy zostały wymontowany z urządzenia i pozostał w jego siedzibie w celu bezpiecznej utylizacji.
4. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
	1. Minimum 9 Gbps dla rozpoznawania i kontroli aplikacji,
	2. Minimum 5 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Antywirus, Antyspyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia.
	3. Minimum 6.5 Gbps wydajności IPSec VPN.
	4. Minimum 130 000 nowych sesji na sekundę.
	5. Minimum 1.3M równoległych sesji
	6. Minimum 1500 tuneli klienckich VPN
	7. Minimum 2500 sąsiedztw IKE (IPSec)
5. 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.
6. Musi umożliwiać zdefiniowanie nie mniej niż 1500 reguł polityk bezpieczeństwa oraz min. 3000 reguł NAT.
7. 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.
8. Urządzenie musi być przeznaczone do montażu w szafie Rack 19”.
9. Urządzenie musi posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
10. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur oraz powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.
11. Urządzenie musi posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.
12. Urządzenie musi 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 przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny (nie rzadziej niż raz na 48h) i pochodzić od tego samego producenta co firewall.
13. Urządzenie musi 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.
14. Urządzenie musi posiadać funkcję filtrowania URL.
15. Urządzenie musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (a nie tylko filtrującego) ruch w politykach bezpieczeństwa.
16. 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.
17. Wymagane jest posiadanie oddzielnych kategorii URL dla zagrożeń typu malware, phishing, C2C oraz dla ostatnio zarejestrowanych domen.
18. Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania kategorii URL.
19. Urządzenie musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sandbox” plików różnych typów (Windows Portable Executable (m.in. exe, dll), MacOS (MachO, DMG, PKG), Linux ELF, pdf, MS Office, JAR, APK, JS, VBS, PowerShell Script, HTA) w celu ochrony przed zagrożeniami typu „zero-day”. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. Interwał aktualizacyjny to maksymalnie 2 godziny
20. Administrator musi mieć możliwość konfiguracji jakiego rodzaju typy plików z listy wspieranych przez funkcję Sandbox zostaną wysłane do skanowania przez „Sandbox”.
21. Musi istnieć możliwość wysyłania plików do systemu Sandbox w chmurze obliczeniowej producenta oraz do fizycznych (lokalnych) urządzeń Sandbox gdyby takie zostały zainstalowane w przyszłości w infrastrukturze Zamawiającego.
22. Urządzenie musi wykrywać i blokować zagrożenia DNS w ruchu przechodzącym przez urządzenie bez potrzeby rekonfiguracji serwera DNS i bez potrzeby ustawiania firewall jako serwera DNS. Wykrywający i blokujący ruch do domen uznanych za złośliwe musi być sterowany (przekierowanie) za pomocą funkcji DNS Sinkholing.
23. Urządzenie musi zapewniać ochronę DNS, co najmniej w zakresie:
	1. wykrywanie domen dynamicznych Dynamic DNS;
	2. wykrywanie zapytań do domen złośliwych;
	3. wykrywanie domen generowanych przez algorytmy DGA;
	4. wykrywanie tunelowania złośliwej komunikacji w protokole DNS;
	5. wykrywanie DNS Exfiltration or DNS Inflitration;
24. **Zarządzanie urządzeniami firewall**
25. Wraz z urządzeniami Firewall konieczne jest dostarczenie centralnego systemu zarządzania tego samego producenta co wyżej opisane urządzenia firewall.
26. 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 platformy VM (tzw. VM Appliance).
27. System zarządzania, logowania i raportowania musi zostać dostarczony w postaci urządzenia dedykowanego VM – tzw. Virtual Appliance.( zgodność z Hyper-V i Vmware, instalacja w środowisku wirtualizacji Zamawiającego).
28. System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne:
	1. obsługa nie mniej niż 20 klastrów firewalli, z możliwością rozbudowy w przyszłości do 100.
	2. obsługa przestrzeni dyskowej minimum 20TB.
29. 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, połączeniach vpn itp.
30. System musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli.
31. System zarządzania, logowania i raportowania musi zapewniać narzędzia dla szybkiej i skutecznej analizy informacji w tym co najmniej:
	1. umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych,
	2. tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego,
	3. 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,
	4. tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down”.
32. System zarządzania, logowania i raportowania musi umożliwiać centralne zarządzanie wieloma firewallami w tym co najmniej:
	1. budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu,
		1. lokalnych (dla wybranych firewalli),
		2. globalnych (dla grup firewalli),
	2. 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).
33. Pozwalać na tworzenie raportów na podstawie zbudowanych kontenerów lub grup urządzeń:
	1. umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium,
	2. umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych.
34. System zarządzania, logowania i raportowania musi udostępniać centralne narzędzia inwentaryzacji i audytu oraz możliwość zarządzania konfiguracjami, w tym co najmniej:
	1. umożliwiać dystrybucję i zdalną instalację nowych wersji systemu,
	2. umożliwiać tworzenie kopii zapasowych zarządzanych firewalli,
	3. umożliwiać dystrybucję i zdalną instalację aktualizacji sygnatur,
	4. umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia przed jej zatwierdzeniem,
	5. pozwalać na zapisywanie różnych wersji konfiguracji zarządzanych firewalli,
	6. umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak, aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone,
	7. informować o zmianach konfiguracji systemu.
35. System zarządzania, logowania i raportowania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń.
36. **Warunki gwarancji i wdrożenia**

**Wszystkie wymagane, oferowane funkcjonalności muszą być dostępne lub/i licencjonowane i mieć gwarancje na okres minimum 60 miesięcy**.

W ramach Zamówienia, Wykonawca przeprowadzi pełną konfigurację i integrację elementów systemu z infrastrukturą Zamawiającego w konfiguracji uzgodnionej z Zamawiającym na etapie wdrożenia. Prace będą obejmowały swoim zakresem, fizyczną instalację urządzeń i oprogramowania będących przedmiotem postępowania (w miejscach wskazanych przez Zamawiającego), integrację z istniejącym systemem teleinformatycznym, konfigurację całego systemu zgodnie z wytycznymi Zamawiającego, konfiguracje dla integracji z środowiskami: infrastruktury sieciowej, wirtualizacji, systemowej oraz przeszkolenie wyznaczonych pracowników Zamawiającego w zakresie użytkowania i administrowania wdrożonego rozwiązania.

Zamawiający wymaga przeszkolenia 4 osób (Administratorów). Czas szkolenia min. 40 godzin szkoleniowych.

Zakres szkolenia musi obejmować praktyczne warsztaty w przygotowanym środowisku szkoleniowym.

Szkolenie musi być potwierdzone certyfikatem producenta dostarczonego sprzętu (szkolenie certyfikowane).

Ostateczne ustalenia z Zamawiającym dotyczące realizacji całego projektu zostaną opisane przez Wykonawcę w dokumencie projektowym, który będzie zawierał szczegóły konfiguracyjne. Dokument zostanie następnie uzgodniony z Zamawiającym.

Wykonawca po zakończeniu wdrożenia protokolarnie przekaże Zamawiającemu dokumentację powykonawczą konfiguracji dostarczonych i uruchomionych elementów systemu.

Ponadto Wykonawca będzie świadczył wsparcie merytoryczne przez okres 60 miesięcy w zakresie zmian konfiguracji, aktualizacji i rozwiązywania bieżących problemów i awarii.