1. **Załącznik nr 1 do umowy – Szczegółowy opis wymagań.**

2. **Urządzenia zabezpieczeń sieci (Firewall z IPS)**

3. **Zamawiający wymaga dostarczenia dwóch urządzeń zabezpieczeń sieci (Firewall z IPS) oraz pojedynczego modułu raportowania i korelacji logów współpracującego z dostarczonymi w przetargu urządzeniami.**

1. Montaż w szafie 19” rack. System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''.
2. System zabezpieczeń musi być dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
3. System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
4. Parametry wydajności urządzenia:
    1) Obsługa nie mniej niż 1 miliona jednoczesnych połączeń i 20 000 nowych połączeń na sekundę.
    2) Przepustowość:
        a) nie mniejsza niż 2 Gb/s dla ruchu nieszyfrowanego,
        b) nie mniejsza niż 500 Mb/s dla IPsec VPN (AES256).
5. Urządzenie zabezpieczeń musi być wyposażone w co najmniej 8 portów GbE RJ45 (w tym co najmniej 2 dedykowane porty WAN) oraz port USB z możliwością obsługi modemów 3G/4G). *Zamawiający dopuści rozwiązanie nie obsługujące modemów 3G/4G przez USB, pod warunkiem dostarczenia urządzenia zabezpieczeń sieci z urządzeniem zewnętrznym oferującym takie wsparcie przez interfejs typu Ethernet o ile liczba wszystkich interfejsów urządzenia zabezpieczeń sieci będzie większa niż wymagane 8.*
6. Urządzenie zabezpieczeń musi obsługiwać redundancje połączeń WAN w trybie co najmniej:
    1) Automatycznego przełączanie na sprawne łącze WAN, przy czym musi istnieć również możliwość używania jako łącza zapasowego modemu podłączonego przez wbudowany port USB.
    2) Loadbalancing (rozkładanie obciążenia) na łącza WAN (fizyczne porty WAN oraz port USB z możliwością obsługi modemów 3G/4G.
7. System zabezpieczeń musi działać w trybie co najmniej:
    1) Routera (tzn. w warstwie 3 modelu OSI).
    2) Transparentnym, przy czym tryb przezroczysty musi umożliwiać wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu (tzn. w warstwie 2 modelu OSI).
8. System musi obsługiwać statyczną i dynamiczna translacja adresów (NAT). Translacja NAPT.
9. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, domeny, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasmo gwarantowane i maksymalne, priorytety, oznaczenia DiffServ). *Zamawiający dopuści również rozwiązanie realizujące zarządzanie mechanizmem QoS w tym dedykowaną politykę odrębne od reszty polityk bezpieczeństwa i NAT.*
10. Urządzenie musi umożliwiać wykrywanie i blokowanie technik i ataków (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. Możliwość wykrywania anomalii protokołów i ruchu.
11. System musi zapewniać obsługę:

1) Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego.
2) Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM.

12. Wymaga się, aby urządzenie w zakresie połączeń VPN realizowało co najmniej:
    1) Tworzenie połączeń w topologii Site-to-site oraz Client-to-site, Hub & Spoke (gwiazdy).
    2) klient VPN własnej produkcji.
    3) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
    4) Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu. Przy czym *Zamawiający dopuszcza rozwiązanie, które nie wspiera konfiguracji tuneli IPSec typ site-to-site typu policy-based, ale nie ogranicza możliwości zestawiania tuneli z rządzeniami pracującymi w obu trybach.*
    5) (interface based VPN).
    6) Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth.
13. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
    1) haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia
    2) haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
    3) haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych
4. Rozwiązanie musi umożliwiać budowę logowania Single Sign On w środowisku Active Directory bez dodatkowych opłat licencyjnych.
14. System musi posiadać możliwość konfiguracji poprzez terminal i linię komend oraz konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą:
    1) haseł statycznych,
    2) haseł dynamicznych (RADIUS).

5. System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB.
6. Jednocześnie, dla systemu bezpieczeństwa powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.
15. System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem centralnego zarządzania umożliwiającym:
    1) Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej.
    2) Wersjonowanie polityk w taki sposób aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości.
    3) Zarządzanie wersjami firmware'u na urządzeniach oraz zdalne uaktualnienia.
    4) Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia.
    5) Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM).
    6) Zapis i zdalne wykonywanie skryptów na urządzeniach.
16. System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym:
    1) Zbieranie logów z urządzeń bezpieczeństwa.
    2) Generowanie raportów.
    3) Skanowanie podatności stacji w sieci.
    4) Zdalną kwarantannę dla modułu antywirusowego.
17. System zabezpieczeń musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive oraz w trybie Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
18. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym. Dostawca musi na etapie odbioru sprzętu okazać zaświadczenie informujące o możliwości przyjęcia uszkodzonego urządzenia objętego serwisem do naprawy u dystrybutora na terenie polski. *Zamawiający dopuści również rozwiązanie, że serwis Dostawcy na etapie odbioru sprzętu okaże zaświadczenie informujące o możliwości przyjęcia uszkodzonego urządzenia objętego serwisem do naprawy na terenie Polski.*
19. Zasilanie z sieci 230V/50Hz.

20. System ochrony obsługuje w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych:
    1) kontrolę dostępu - zaporę ogniową klasy Stateful Inspection,
    2) poufność danych - IPSec VPN oraz SSL VPN,
    3) ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, SMTPS, POP3S, IMAPS, HTTPS),
    4) ochronę przed atakami - Intrusion Prevention System [IPS/IDS],
7. oraz funkcjonalności uzupełniających:
    5) kontrolę treści – Web Filter [WF],
    6) kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP, SMTPS, POP3S, IMAPS), *Zamawiający*
8. *dopuszcza rozwiązanie oferujące kontrolę AS na bazie usług reputacyjnych dostępnych w Internecie,*
    7) kontrolę pasma oraz ruchu [QoS i Traffic shaping],
    8) kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM oraz P2P),
    9) zapobieganie przed wyciekiem informacji poufnej DLP (Data Leak Preention),
    10) inspekcje SSL z możliwością pełniej analizy szyfrowanej komunikacji.
21. System zabezpieczeń musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w sieci Internet) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona AntiVirus i AntiSpyware), filtracja plików, danych i URL.
22. System zabezpieczeń musi identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się, co najmniej, poprzez sygnatury i analizę heurystyczną.
23. System zabezpieczeń musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
24. Co najmniej 36 miesięcy bezpłatnej gwarancji (części i robocizna) od daty obustronnego podpisania Końcowego Protokołu Zdawczo-Odbiorczego Dostawy, na miejscu u Zamawiającego.
25. Maksymalny czas usunięcia awarii do następnego dnia roboczego (poniedziałek-piątek) od dnia zgłoszenia lub w przypadku braku możliwości usunięcia awarii w w/w terminie podstawienie sprzętu zastępczego o parametrach technicznych niegorszych niż sprzęt oferowany.

26. Uszkodzony dysk: hdd/ssd (jeżeli występuje i nie jest integralną - nierozłączalną częścią urządzenia) pozostaje u Zamawiającego.
27. Zamawiający wymaga dostarczenia licencji dla modułów bezpieczeństwa (antywirus, wykrywanie włamań, kontrola aplikacji i webfiltering) na co najmniej 3 lata od daty obustronnego podpisania Końcowego Protokołu Zdawczo-Odbiorczego Dostawy. Urządzenie nie może być urządzeniem wycofanym ze sprzedaży lub nie posiadającym wsparcia producenta.
28. Zamawiający wraz z urządzeniami zabezpieczeń sieci wymaga dostarczenia modułu raportowania i korelacji logów w postaci maszyny wirtualnej (zgodnej z Hyper-V 2012R2/2016) lub urządzenia sprzętowego, umożliwiającego przetwarzanie logów z urządzeń bezpieczeństwa w ilości, co najmniej, 20GB dziennie oraz pozwalającego na przechowywanie co najmniej 10 TB danych. *Przy czym należy zaznaczyć, że Zamawiający nie wymaga dostarczenia serwera fizycznego na potrzeby wdrożenia modułu raportowania i korelacji logów w postaci maszyny wirtualnej. Moduł raportowani i korelacji logów musi pozwalać na obsługę co najmniej 20 urządzeń.*
29. Zamawiający wymaga dostępu do aktualizacji oprogramowania wewnętrznego (firmware) przez co najmniej 36 miesięcy od daty obustronnego podpisania Końcowego Protokołu Zdawczo-Odbiorczego Dostawy zarówno dla urządzenia zabezpieczeń sieci jak i modułu raportującego. Dostęp do aktualizacji oprogramowania wewnętrznego musi być realizowany co najmniej poprzez stronę internetową producenta dostarczonego urządzenia.