Nowy, aktualny na dzień 25.10.2019 r.

Szczegółowy Opis Przedmiotu Zamówienia

Dostawa sieciowych urządzeń zabezpieczających oraz przeprowadzenie instruktażu z niezbędnych konfiguracji w ramach realizacji projektu „Poprawa komunikacji pomiędzy Regionalną Dyrekcją Ochrony Środowiska w Lublinie a społeczeństwem poprzez narzędzia informatyczne – e – drzwi do ochrony środowiska" RPLU.02.01.00-06-0023/16.

SIECIOWE URZĄDZENIA ZABEZPIECZAJACE (6 sztuk)

1. Wymaga się aby oferowany sprzęt informatyczny spełniał wszystkie parametry określone w poniższej tabeli oraz:
   1) był fabrycznie nowy i nieużywany,
   2) nie był prototypem,
   3) pochodził z bieżącej oferty producenta,
   4) był wyprodukowany nie wcześniej niż w 2019 roku,
   5) był oznakowany symbolem CE,
   6) pochodził z legalnego źródła,
   7) pochodził z oficjalnego kanału sprzedaży producenta na teren Polski (wymagane przedstawienie oświadczenie Producenta oferowanego urządzenia na wezwanie Zamawiającego).
   8) był objęty standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i oprogramowania, świadczonych przez sieć serwisową producenta na terenie Polski.
2. Zamawiający zastrzega sobie prawo do żądania potwierdzenia źródła pochodzenia zamawianego sprzętu w postaci oświadczenia producenta (na etapie realizacji Umowy).
3. Oferowany sprzęt komputerowy musi być dostarczony Zamawiającemu w oryginalnych opakowaniach fabrycznych.
4. Wykonawca musi przedstawić nazwę producenta i model oferowanego sprzętu komputerowego.
5. Zamawiający wymaga dostarczenia sprzętu we wskazane miejsce.
6. Cały sprzęt musi posiadać kompletne okablowanie niezbędne do uruchomienia i instalacji wszystkich urządzeń wchodzących w skład zamówienia.
7. Nie dopuszcza się zastosowania sprzętu nie współpracującego ze sobą.
8. Dla urządzeń wraz z wyspecyfikowanym oprogramowaniem standardowym, Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego na czas

wynikający z zasad licencjonowania określonych przez producenta danego rodzaju oprogramowania, a jeśli ten nie jest ograniczony czasowo – na czas nieoznaczony, tj. nieograniczony w czasie.

9. Na wezwanie Zamawiającego, Wykonawca dostarczy:
   • oświadczania producenta lub autoryzowanego dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (adres strony internetowej serwisu i numer infolinii telefonicznej),
   • Certyfikat ISO 9001 podmiotu serwisującego,
   • oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań,
   • w przypadku udzielanego instruktarzu, od prowadzącego instruktarz - certyfikat powiązany z dostarczonymi urządzeniami.
10. Zamawiający wymaga aby dostarczone urządzenia obsłużyły istniejącą strukturę sieciową oraz strefę DMZ, a także realizowały zabezpieczenia IDS/IPS, Antywirus, Web Filtering, Anyspam. Zamawiający będąc użytkownikiem sprzętu firmy Fortinet, zabezpieczającego połączenia brzegowe sieci, wymaga aby dostarczone urządzenia były z nim w pełni kompatybilne. Wdrożenie urządzeń polegać ma na zastąpieniu istniejących rozwiązań sieciowych, we wszystkich lokalizacjach Zamawiającego nowymi urządzeniami odpowiednio skonfigurowanymi, z zachowaniem istniejących parametrów sieciowych oraz odpowiednim zabezpieczeniu sieci. Uruchomione rozwiązanie umożliwiać ma obsługę redundancji połączenia z siecią Internet przy użyciu drugiego łącza bez ponoszenia dodatkowych kosztów na sprzęt albo licencje i oprogramowanie. Zamawiający wymaga wykonania rejestracji urządzeń oraz dostarczonych serwisów na stronach producenta (w porozumieniu z przedstawicielem Zamawiającego) oraz przekazania niezbędnych danych dostępowych Zamawiającemu.
11. Zamawiający wymaga aby oferowane urządzenia brzegowe sieci typ I oraz typ II pochodziły od jednego producenta.
12. Jeśli dostarczone urządzenia różnią się jedynie parametrami wydajności, a firmware oraz systemy bezpieczeństwa w nich zaimplementowane są zbieżne, to Zamawiający dopuszcza przeprowadzenie instruktarzu dla jednego z dostarczonych urządzeń.

I. URZĄDZENIE BRZEGOWE SIECI TYP 1 - (1 sztuka)

L.p	*Nazwa parametru*	*Opis parametru (wymagany, minimalny parametr)*
1	*2*	*3*
1.	Wymagania ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym pochodzącymi od producenta dostarczonego sprzętu. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System musi wspierać IPv4 oraz IPv6 w zakresie: – firewall, – ochrony w warstwie aplikacji, – protokołów routingu dynamicznego.
2.	Obudowa	Przystosowana do instalacji w standardowej szafie RACK 19” rozwiązanie może zajmować maksymalnie 1U.
3.	Redundancja monitoring i wykrywanie awarii	– system pełniący funkcje Firewall, IPSec, Kontrola Aplikacji oraz IPS musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall, – zaimplementowane: monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych, – możliwość monitoringu stanu realizowanych połączeń VPN.
4.	Interfejsy fizyczne oraz wirtualne	– min. 5 portów Gigabit Ethernet RJ-45. – wbudowany port konsoli szeregowej – gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB – W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
5.	Parametry wydajnościowe	– w zakresie Firewall’a obsługa min. 1.3 miliona jednoczesnych połączeń oraz min. 30 tys. nowych połączeń na sekundę, – min. 4 Gbps przepustowości Firewall, – min. 900 Mbps przepustowości Firewall z włączoną funkcją Kontroli Aplikacji, – wydajność min. 75 Mbps przy szyfrowaniu IPSec VPN (dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256), – wydajność min. 300 Mbps przy skanowaniu ruchu w celu

		ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS), – wydajność min. 150 Mbps przy skanowaniu ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus, – wydajność systemu min. 125 Mbps w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 125 Mbps
6.	Bezpieczeństwo	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: – kontrola dostępu - zapora ogniowa klasy Stateful Inspection, – kontrola aplikacji, – poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN, – ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS, – ochrona przed atakami - Intrusion Prevention System, – kontrola stron WWW, – kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, – zarządzanie pasmem (QoS, Traffic shaping), – mechanizmy ochrony przed wyciekiem poufnej informacji (DLP), – dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site, – analiza ruchu szyfrowanego protokołem SSL.
7.	Polityki, Firewall	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: - translację jeden do jeden oraz jeden do wielu. - dedykowany ALG (Application Level Gateway) dla protokołu SIP. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
8.	Połączenia VPN	System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: – wsparcie dla IKE v1 oraz v2, – obsługę szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM), – obsługę protokołu Diffie-Hellman grup 19 i 20, – wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE, – tworzenie połączeń typu Site-to-Site oraz Client-to-Site,

		– monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności, – możliwość wyboru tunelu przez protokoły dynamicznego routingu (np. OSPF) oraz routingu statycznego, – obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth, – mechanizm „Split tunneling" dla połączeń Client-to-Site. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: – pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0, – pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
9.	Obsługa routingu i łączy WAN	– routingu statycznego, – Policy Based Routingu, – rotokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
10.	Zarządzanie pasmem	– możliwość określenia maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu, – możliwość określania pasma dla poszczególnych aplikacji, – możliwość zarządzania pasmem dla wybranych kategorii URL.
11.	Kontrola Antywirusowa	– silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach, – system musi umożliwiać skanowanie formatów archiwów, w tym co najmniej: zip, RAR, – system realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń – ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur, – baza sygnatur ataków powinna zawierać minimum 500 wpisów, – system musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS, – system powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach, – mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym.
12.	Kontrola aplikacji	– funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. – baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z

		harmonogramem definiowanym przez administratora. – aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. – baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P, Botnet. – administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur
13.	Kontrola WWW	– moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. – w ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. – filtr WWW musi dostarczać kategorii stron zabronionych prawem, takich jak hazard. – administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL oraz definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
14.	Uwierzytelnianie użytkowników w ramach sesji	– system Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu, • haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, • haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. – musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego, – rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory
15.	Zarządzanie	– elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania, – komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów, – powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego, – system musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow, – system musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia

		dokumentację, – system musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
16.	Logowanie	– system musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej, – w ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania, – logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu, – musi istnieć możliwość logowania do serwera SYSLOG.
17.	Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: – ICSA lub EAL4 dla funkcji Firewall – ICSA lub NSS Labs dla funkcji IPS – ICSA dla funkcji IPSec VPN – ICSA dla funkcji SSL VPN
18.	Licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrolę Aplikacji, IPS, Antywirus, Antyspam, Web Filtering przez okres minimum 24 miesięcy
19.	Zasilanie	System musi być wyposażony w zasilanie AC.
20.	Warunki gwarancji	– gwarancja producenta na okres …….. miesięcy *(liczba miesięcy do wstawienia z oferty - min. 24 miesięcy),* realizowana w następnym dniu roboczym po zgłoszeniu awarii, – możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta, – wymagane dołączenie do oferty oświadczenia, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta, – zapewnienie wsparcia technicznego w okresie trwania gwarancji, – możliwość aktualizacji wewnętrznego oprogramowania urządzenia w okresie gwarancji,
21.	Instruktaż z konfiguracji oraz obsługi	Wymaga się aby instruktarz przeprowadzony był w formie warsztatów przy wykorzystaniu dostarczonych urządzeń bądź ich równoważnych odpowiedników. Celem ma być zdobycie umiejętności praktycznych potrzebnych do samodzielnej administracji tymi urządzeniami oraz zapoznanie z najczęściej spotykanymi zagrożeniami i tworzeniem, a także

		zarządzaniem polityką bezpieczeństwa na styku sieci lokalnej z Internetem, integracją urządzeń z domeną AD oraz zaawansowanymi opcjami routingu. Instruktarz ma być przeprowadzony w oparciu o najnowszy firmware urządzeń. Od prowadzącego instruktarz wymaga się posiadania certyfikatu wydanego przez producenta urządzeń. Tematyka instruktarzu powinna obejmować: – omówienie wstępnej konfiguracji urządzeń: • tryby pracy NAT/Transparent • konfiguracja sieci i routingu • system Dashboard i moduły systemu • administracja urządzeniem (WWW, CLI) – politykę zapory sieciowej: • koncepcja firewall • tworzenie obiektów dla reguł firewall • translacja adresów NAT i Virtual IP • Internet Service Database – inspekcję ruchu SSL i metody dystrybucji certyfikatów, – omówienie trybów pracy urządzenia – Proxy i Flow, – logowanie i powiadomienia, – konfigurację funkcji ochronnych (profile bezpieczeństwa): • ochrona antywirusowa • filtrowanie antyspamowe • system IPS / DoS Policy • kontrola ruchu WWW / blokowanie URL / DNS Filter • kontrola aplikacji • reputacja klienta • Data Leakage Prevention (DLP) • Web Application Firewall (WAF) – optymalizację ruchu sieciowego (kształtowanie pasma), – konfigurację połączeń SSL VPN, – konserwację i bieżąca obsługa systemu, – wirtualizację w obrębie urządzenia - wykorzystanie trybów pracy NAT / Transparent – zaawansowaną konfiguracja sieci i routingu: • routing dynamiczny, • tworzenie sieci VLAN, • pojęcie Policy Routingu, • SD-WAN -Load Balancing oraz redundancja łącz Internetowych, – uwierzytelnianie użytkowników: • integracja z usługami katalogowymi, • tworzenie reguł firewall w oparciu o grupy użytkowników • konta użytkowników gości – wirtualne sieci prywatne - VPN: • IPSec VPN site-to-site, client-to-site, • VXLAN, • ADVPN, – diagnostykę i rozwiązywanie problemów. Minimalna ilość godzin przeznaczonych na instruktaż - 32 godz. zegarowe.

22.	Wsparcie wdrożeniowe	Zamawiający wymaga od Wykonawcy wsparcia przy wdrożeniu urządzeń do struktury informatycznej Zamawiającego obejmującego: – wykonanie audytu obecnej topologii sieci oraz użytych mechanizmów sieciowych pod kątem wybrania optymalnej topologii docelowej, – analizy utylizacji używanych obecnie łącz oraz przepływu danych w sieci pod kątem wykorzystania przez poszczególne usługi, – przygotowania koncepcji wdrożenia firewalla uwzględniając aspekt współpracy/integracji z systemami i urządzeniami (typu przełączniki, Active Directory) Wykonane czynności muszą zostać przeprowadzone w siedzibie Zamawiającego przez osoby posiadające certyfikacje techniczne. Czas poświęcony na zrealizowanie wsparcia - min. 5 godz. zegarowych.

URZĄDZENIE BRZEGOWE SIECI TYP 2 - (5 sztuk)

L.p	*Nazwa parametru*	*Opis parametru (wymagany, minimalny parametr)*
1	*2*	*3*
1.	Wymagania ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym pochodzącymi od producenta dostarczonego sprzętu. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System musi wspierać IPv4 oraz IPv6 w zakresie: – firewall, – ochrony w warstwie aplikacji, – protokołów routingu dynamicznego.
2.	Obudowa	Przystosowana do instalacji w standardowej szafie RACK 19” rozwiązanie może zajmować maksymalnie 1U.
3.	Redundancja monitoring i wykrywanie awarii	– system pełniący funkcje Firewall, IPSec, Kontrola Aplikacji oraz IPS musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall, – zaimplementowane: monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych, – możliwość monitoringu stanu realizowanych połączeń VPN.
4.	Interfejsy fizyczne oraz wirtualne	– min. 5 portów Gigabit Ethernet RJ-45. – wbudowany port konsoli szeregowej – gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB – W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 100 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
5.	Parametry wydajnościowe	– w zakresie Firewall’a obsługa min. 900 tys. jednoczesnych połączeń oraz min. 15 tys. nowych połączeń na sekundę, – min. 950 Mbps przepustowości Firewall, – min. 400 Mbps przepustowości Firewall z włączoną funkcją Kontroli Aplikacji, – wydajność min. 75 Mbps przy szyfrowaniu IPSec VPN (dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256), – wydajność min. 300 Mbps przy skanowaniu ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS),

		– wydajność min. 150 Mbps przy skanowaniu ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus, – wydajność systemu min. 125 Mbps w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 125 Mbps
6.	Bezpieczeństwo	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: – kontrola dostępu - zapora ogniowa klasy Stateful Inspection, – kontrola aplikacji, – poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN, – ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS, – ochrona przed atakami - Intrusion Prevention System, – kontrola stron WWW, – kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, – zarządzanie pasmem (QoS, Traffic shaping), – mechanizmy ochrony przed wyciekiem poufnej informacji (DLP), – dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site, – analiza ruchu szyfrowanego protokołem SSL.
7.	Polityki, Firewall	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: - translację jeden do jeden oraz jeden do wielu. - dedykowany ALG (Application Level Gateway) dla protokołu SIP. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
8.	Połączenia VPN	System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: – wsparcie dla IKE v1 oraz v2, – obsługę szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM), – obsługę protokołu Diffie-Hellman grup 19 i 20, – wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE, – tworzenie połączeń typu Site-to-Site oraz Client-to-Site, – monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności,

		– możliwość wyboru tunelu przez protokoły dynamicznego routingu (np. OSPF) oraz routingu statycznego, – obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth, – mechanizm „Split tunneling" dla połączeń Client-to-Site. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: – pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0, – pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
9.	Obsługa routingu i łączy WAN	– routingu statycznego, – Policy Based Routingu, – rotokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
10.	Zarządzanie pasmem	– możliwość określenia maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu, – możliwość określania pasma dla poszczególnych aplikacji, – możliwość zarządzania pasmem dla wybranych kategorii URL.
11.	Kontrola Antywirusowa	– silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach, – system musi umożliwiać skanowanie formatów archiwów, w tym co najmniej: zip, RAR, – system realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń – ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur, – baza sygnatur ataków powinna zawierać minimum 500 wpisów, – system musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS, – system powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach, – mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym.
12.	Kontrola aplikacji	– funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. – baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. – aplikacje chmurowe (co najmniej: Facebook, Google Docs,

		Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. – baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P, Botnet. – administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur
13.	Kontrola WWW	– moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. – w ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. – filtr WWW musi dostarczać kategorii stron zabronionych prawem, takich jak hazard. – administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL oraz definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
14.	Uwierzytelnianie użytkowników w ramach sesji	– system Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu, • haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, • haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. – musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego, – rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory
15.	Zarządzania	– elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania, – komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów, – powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego, – system musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow, – system musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację, – system musi mieć wbudowane narzędzia diagnostyczne,

		przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
16.	Logowanie	– system musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej, – w ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania, – logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu, – musi istnieć możliwość logowania do serwera SYSLOG.
17.	Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: – ICSA lub EAL4 dla funkcji Firewall – ICSA lub NSS Labs dla funkcji IPS – ICSA dla funkcji IPSec VPN – ICSA dla funkcji SSL VPN
18.	Licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrolę Aplikacji, IPS, Antywirus, Antyspam, Web Filtering przez okres minimum 12 miesięcy
19.	Zasilanie	System musi być wyposażony w zasilanie AC.
20.	Warunki gwarancji	– wymagane jest min. 12 miesięcy gwarancji producenta z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, – możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta, – wymagane dołączenie do oferty oświadczenia, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta, – zapewnienie wsparcia technicznego w okresie trwania gwarancji, – możliwość aktualizacji wewnętrznego oprogramowania urządzenia w okresie gwarancji,
21.	Instruktaż z konfiguracji oraz obsługi	Wymaga się aby instruktarz przeprowadzony był w formie warsztatów przy wykorzystaniu dostarczonych urządzeń bądź ich równoważnych odpowiedników. Celem ma być zdobycie umiejętności praktycznych potrzebnych do samodzielnej administracji tymi urządzeniami oraz zapoznanie z najczęściej spotykanymi zagrożeniami i tworzeniem, a także zarządzaniem polityką bezpieczeństwa na styku sieci lokalnej z Internetem, integracją urządzeń z domeną AD oraz zaawansowanymi opcjami routingu. Instruktarz ma być

		przeprowadzony w oparciu o najnowszy firmware urządzeń. Od prowadzącego instruktarz wymaga się posiadania certyfikatu wydanego przez producenta urządzeń. Tematyka instruktarzu powinna obejmować: – omówienie wstępnej konfiguracji urządzeń: • tryby pracy NAT/Transparent • konfiguracja sieci i routingu • system Dashboard i moduły systemu • administracja urządzeniem (WWW, CLI) – politykę zapory sieciowej: • koncepcja firewall • tworzenie obiektów dla reguł firewall • translacja adresów NAT i Virtual IP • Internet Service Database – inspekcję ruchu SSL i metody dystrybucji certyfikatów, – omówienie trybów pracy urządzenia – Proxy i Flow, – logowanie i powiadomienia, – konfigurację funkcji ochronnych (profile bezpieczeństwa): • ochrona antywirusowa • filtrowanie antyspamowe • system IPS / DoS Policy • kontrola ruchu WWW / blokowanie URL / DNS Filter • kontrola aplikacji • reputacja klienta • Data Leakage Prevention (DLP) • Web Application Firewall (WAF) – optymalizację ruchu sieciowego (kształtowanie pasma), – konfigurację połączeń SSL VPN, – konserwację i bieżąca obsługa systemu, – wirtualizację w obrębie urządzenia - wykorzystanie trybów pracy NAT / Transparent – zaawansowaną konfiguracja sieci i routingu: • routing dynamiczny, • tworzenie sieci VLAN, • pojęcie Policy Routingu, • SD-WAN -Load Balancing oraz redundancja łącz Internetowych, – uwierzytelnianie użytkowników: • integracja z usługami katalogowymi, • tworzenie reguł firewall w oparciu o grupy użytkowników • konta użytkowników gości – wirtualne sieci prywatne - VPN: • IPSec VPN site-to-site, client-to-site, • VXLAN, • ADVPN, – diagnostykę i rozwiązywanie problemów. Minimalna ilość godzin przeznaczonych na instruktaż - 32 godzin zegarowych.
22.	Wsparcie wdrożeniowe	Zamawiający wymaga od Wykonawcy wsparcia przy wdrożeniu urządzeń do struktury informatycznej Zamawiającego obejmującego:

		– wykonanie audytu obecnej topologii sieci oraz użytych mechanizmów sieciowych pod kątem wybrania optymalnej topologii docelowej, – analizy utylizacji używanych obecnie łącz oraz przepływu danych w sieci pod kątem wykorzystania przez poszczególne usługi, – przygotowania koncepcji wdrożenia firewalla uwzględniając aspekt współpracy/integracji z systemami i urządzeniami (typu przełączniki, Active Directory) Wykonane czynności muszą zostać przeprowadzone w siedzibie Zamawiającego przez osoby posiadające certyfikacje techniczne. Czas poświęcony na zrealizowanie wsparcia - min. 5 godz. zegarowych.