Załącznik Nr 1 do SIWZ

Punkt	Opis	
1	**Firewall**	
1.1	**Funkcjonalność Firewall**	
1.1.1	Firewall musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2)	
1.1.2	Firewall musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF i BGP	
1.1.3	Firewall musi obsługiwać policy based routing	
1.1.4	Firewall musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPoE) na zewnętrznym interfejsie	
1.1.5	Firewall musi obsługiwać DHCP v6 na zewnętrznym interfejsie	
1.1.6	Firewall musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP), jako bridge (transpartentmode) lub z tym samym adresem IP na wszystkich portach.	
1.1.7	Firewall musi mieć możliwość obsługi wielu łączy zewnętrznych z opcją balansowania ruchu.	
1.1.8	Firewall musi mieć możliwość obsługi łącza zapasowego typu LTE	
1.1.9	Firewall musi obsługiwać Dynamic DNS	
1.1.10	Firewall musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1	
1.1.11	Firewall musi obsługiwać translację portów: PAT	
1.1.12	Firewall musi obsługiwać IPSec NAT traversal	
1.1.13	Firewall musi obsługiwać mechanizm policy-based NAT	
1.1.14	Firewall musi obsługiwać VLAN 802.1Q	
1.1.15	Firewall musi zapewniać ochronę przed atakami stosującymi techniki unikania wykrycia, np. fragmentacja pakietów	
1.1.16	Firewall musi obsługiwać pracę jako serwer DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.	
1.1.17	Firewall musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP	
1.1.18	Firewall musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.	
1.1.19	Firewall musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID oraz wewnętrznej bazy użytkowników.	
1.1.20	Firewall musi umożliwiać transparentne uwierzytelnianie użytkowników przez Active Directory.	
1.1.21	Urządzenie musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z Microsoft Terminal Services i CitrixXenApp	
1.1.22	Urządzenie nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.	
1.1.23	Firewall musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji	
1.1.24	Firewall musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.	
1.1.25	Firewall musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: http, https, ftp, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP	
1.1.26	Firewall musi zapewniać ochronę z wykorzystaniem mechanizmów IPS	
1.1.27	Firewall musi zapewniać ochronę antywirusową dla obsługiwanych protokołów	
1.1.28	Firewall musi zapewniać możliwość filtrowania URL	
1.1.29	Firewall musi zapewniać inspekcję ruchu szyfrowanego https	
1.1.30	Firewall musi zapewniać ochronę przed niechcianą pocztą (AntySPAM)	
1.1.31	Firewall musi zapewniać rozpoznawanie aplikacji w oparciu o analizę ruchu sieciowego a nie wyłącznie nr portu.	
1.1.32	Urządzenie musi mieć możliwość filtrowania treści według typu MIME	
1.1.33	Urządzenie musi umożliwiać sterowanie przepustowością w oparciu o	

	następujące parametry: użytkownik, grupa, protokół, polityka, interfejs sieciowy, adres IP, sieć VLAN, aplikacja i kategoria aplikacji	
1.1.34	Firewall musi udostępniać mechanizmy limitowania dostępu do sieci użytkownikom w oparciu o kwoty czasowe lub transferu danych.	
1.1.35	Firewall musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site	
1.1.36	Zamawiający wymaga dostarczenia sprzętu - dwa urządzenia NGFW pracujących jako klaster w trybie Active-Active lub Active-Passive , wraz z wymienionym osprzętem, montażem w siedzibie Zamawiającego w Warszawie (wskazane miejsce montażu i współpraca z działem IT) i instalacją niezbędnego oprogramowania, skonfigurowaniem, testami i uruchomieniem z minimalnymi skutkami na działanie innych systemów zamawiającego	
1.2	**Wydajność firewall**	
1.2.1	Firewall musi zapewnić obsługę na poziomie minimalnym: **33Gbps**dla pracy w trybie firewall, **4.5 Gbps** dla pracy w trybie UTM (z włączonymi mechanizmami AV i IPS)	
1.2.2	Firewall musi obsługiwać **8 000 000** jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną **135 tyś.** nowych połączeń na sekundę	
1.2.3	Ilość obsługiwanych sieci VLAN: min **700**	
1.2.4	Minimalna ilość portów 10/100/1000 BaseT: **8**	
2	**VPN**	
2.1	**Funkcje VPN**	
2.1.1	Urządzenie musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz TLS	
2.1.2	Urządzenie musi w zakresie IPSec site-to-site VPN współpracować z rozwiązaniami innych producentów	
2.1.3	Rozwiązanie musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256	
2.1.4	Rozwiązanie musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-SharedKey, 3rd Party Cert.	
2.1.5	Wsparcie dla Dead Peer Detection (DPD)	
2.1.6	Urządzenie musi obsługiwać IKEv1 i IKEv2	
2.1.7	Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman do wymiany kluczy przez email i web	
2.1.8	Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego) z podtrzymaniem zestawionych połączeń TCP	
2.1.9	Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu	
2.1.10	Urządzenie musi obsługiwać statyczne i dynamiczne (routowane) połączenia VPN do dostawców chmury obliczeniowej (AWS i MS Azzure)	
2.1.11	Urządzenie musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP.	
2.1.12	Połączenia client-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android	
2.1.13	Urządzenie ma zapewnia funkcję portalu dostępowego chronionego przez szyfrowanie https (TLS)	
2.2	**Wydajność VPN**	
2.2.1	Przepustowość IPSec VPN nie mniejsza niż **7,5 GBps**	
2.2.2	Obsługa nie mniej niż: **700** tuneli IPSec site-to-site	
2.2.3	Obsługa nie mniej niż: **700** tuneli client-to-site	
3	**Filtrowanie zawartości URL**	
3.1	Urządzenie musi umożliwiać filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji	
3.2	Funkcjonalność filtrowania zawartości powinna dawać możliwość filtrowania stron według minimalnie 80 kategorii	
3.3	Rozwiązanie musi pozwalać na tworzenie białych list (white lists) wyjątków dla filtrowania zawartości	

3.4	Baza zawartości URL powinna być dostępna on-line lub do ściągnięcia i zainstalowania lokalnie	
3.5	Funkcja powinna filtrować treści w wielu językach, w tym w języku polskim	
3.6	Filtrowanie musi obsługiwać również protokół https	
3.7	Urządzenie musi umożliwiać wyłączenie inspekcji https dla wybranych kategorii stron WWW	
3.8	System kategoryzacji stron musi posiadać kategorie: Proxy avoidance, Malicious sites, Phishing	
4	**Kontrola aplikacyjna**	
4.1	System kontroli aplikacyjnej musi rozpoznawać aplikacje oraz kategorie aplikacji	
4.2	Aplikacje muszą być rozpoznawana w oparciu o analizę ruchu a nie przez porty i protokoły	
4.3	Ilość rozpoznawanych aplikacji nie mniejsza niż 1800	
4.4	W ramach konkretnej aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe)	
4.5	Kontrola aplikacyjna musi rozpoznawać co najmniej aplikacje: Tor, Proxy service, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online	
5	**Antywirus**	
5.1	System musi mieć możliwość uruchomienia co najmniej 1 silnika skanera antywirusowego	
5.2	Aktualizacja plików sygnatur antywirusowych musi się odbywać automatycznie	
5.3	Aktualizacja plików sygnatur antywirusowych musi się odbywać nie rzadziej niż co 12 godzin.	
5.4	Antywirus musi mieć możliwość przeprowadzania kwarantanny e-mail.	
5.5	Wykrywanie i blokowanie spyware'u	
5.6	Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji	
5.7	Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS	
5.8	System musi zapewniać możliwość zablokowania zagrożenia ransomware uruchomionego na stacjach roboczych i serwerach.	
5.9	Przepustowość AV w urządzeniu nie mniejsza niż **4,5 Gbps**	
7	**IPS**	
7.1	Automatyczna aktualizacja sygnatur IPS	
7.2	IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy	
7.3	Automatyczne blokowanie znanych źródeł ataków	
7.4	System musi pozwalać na blokowanie ataków typu DoS i DDoS	
7.5	Przepustowość IPS w urządzeniu nie mniejsza niż **5,2 Gbps**	
8	**Antymalware**	
8.1	System musi zapewniać ochronę przed nieznanym złośliwym oprogramowaniem, na zasadzie analizy behawioralnej (sandbox).	
8.2	System musi pracować w trybie lokalnym lub z wykorzystaniem mechanizmów chmury (zlokalizowanej na terytorium Unii Europejskiej)	
8.3	Analizie muszą podlegać pliki ściągane przez http(s) i przesyłane pocztą elektroniczną.	
8.4	System musi zapewniać ogólne oszacowanie poziomu ryzyka dla analizowanych plików oraz udostępniać szczegółowe informacje o wykrytych działaniach niebezpiecznych.	
9	**Ochrona przed phishingiem**	
9.1	System musi zapewniać dedykowaną (poza ochroną przed SPAM'em) ochronę przed phishingiem	
9.2	System winien blokować możliwość dostępu do spreparowanych stron.	
9.3	System musi blokować dostęp niezależnie od użytego protokołu czy portu komunikacyjnego	

9.4	Zablokowanie dostępu musi być odpowiednio notyfikowane użytkownikowi, którego dotyczy, niezależnie od logów i raportów	
9.5	System musi chronić przed nadużyciem protokołu DNS	
10	**Zarządzanie**	
10.1	Administracja urządzenia musi być możliwe poprzez graficzny interfejs zarządzania w czasie rzeczywistym.	
10.2	Urządzenie musi umożliwiać zarządzanie za pomocą linii poleceń poprzez port szeregowy lub poprzez SSH.	
10.3	Urządzenie musi umożliwiać zarządzanie za pomocą wbudowanego interfejsu WEB.	
10.4	Urządzenie może być zarządzane jednocześnie z wielu platform przez różnych administratorów.	
10.5	Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.	
10.6	Rozwiązanie musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online	
10.7	Rozwiązanie musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według harmonogramu	
10.8	System musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.	
10.9	Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.	
10.10	System ma posiadać metodę porównywania różnych wersji konfiguracji.	
10.11	Obsługa różnych ról administratorów.	
10.12	Umożliwia monitorowanie logów ruchu w czasie rzeczywistym.	
10.13	Urządzenie musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi (access pointy).	
10.14	System zarządzania musi zapewniać korelację zdarzeń dotyczących konkretnych komputerów pochodzących z systemów ochrony sieciowej i z chronionych komputerów	
10.15	Stacja zarządzająca 3 szt. G703GI-E5139R Rog strix G703GI i9-8950HK/64G/2x256PCIe+ SSD1TB HDD/Win10Pro; Stacja zarządzająca 1 szt. ;;	
10.16	Stacja zarządzająca 1szt AW17-7124 17 i9-8750H/32G/1x512 GB PCIe SSD+1TB HDD (min 7200 obr.)/Win10 Pro, GTX1070	
10.17	Stacja zarządzająca: 1 szt. ThinkPad X280 , Core I5 8gen lub wyższy, 12,5” FHD (1920 x 1080) IPS, 8 GB DDR4 2133 MHZ, 512GB SSD PCIe, wbudowany modem LTE Soundtouch 30	
11	**Dzienniki i raporty**	
11.1	Rozwiązanie musi umożliwiać zbieranie i przechowywanie dzienników i raportów.	
11.2	Rozwiązanie musi umożliwiać przesyłanie logów do co najmniej 2 serwerów dziennika	
11.3	Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.	
11.4	Rozwiązanie musi udostępniać narzędzie analizy całości ruchu	
11.5	Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa	
11.6	Rozwiązanie musi posiadać minimum 30 predefiniowanych typów raportów.	
11.7	Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie	
11.8	System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.	
11.9	System musi być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania tych sprawozdań pocztą e-mail.	
11.10	Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.	
11.11	System raportowania musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów i dzienników.	
11.12	System musi wspierać automatyczne wysyłanie wszystkich typów raportów pocztą elektroniczną.	
11.13	Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym	

	użytkownikom.	
11.14	System musi umożliwiać pseudo anonimizację użytkowników z prawem do de anonimizacji tylko dla wybranych administratorów	
11.15	System musi zapewniać wizualizację, opisującą w trybie graficznym stan przepustowości systemu.	
12	**Zasilanie**	
12.1	System musi być dostarczony wraz z dedykowanym systemem zasilania oraz niezbędnym okablowaniem zgodnym z systemem zasilania.	
13.	**Wsparcie**	
13.1	Pomoc techniczna oraz szkolenia z produktu powinny być dostępne w Polsce na terenie miasta stołecznego Warszawy.	
13.2	Zamawiający wymaga dostarczenia wszystkich niezbędnych licencji i subskrypcji na okres minimum 5 lat (60 miesięcy), w tym okresie bezpłatne wsparcie techniczne oraz wszelkie aktualizacje (łatki, poprawki, update oprogramowania i firmware-u oraz aktualizacje sygnatur dla wszystkich wymaganych funkcjonalności).	
13.3	Wdrożenie produktu powinno obejmować wszystkie niezbędne funkcjonalności podane powyżej dla prawidłowego funkcjonowania systemu bezpieczeństwa.	
13.4	System bezpieczeństwa powinien być objęty serwisem gwarancyjnym producenta przez okres subskrypcji o których mowa w 13.2, polegającym na naprawie lub wymianie urządzeń w przypadku ich wadliwości oraz uszkodzenia. W okresie gwarancji wymagane jest bezpłatne usuwanie awarii oraz bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii.	

Zamawiający wymaga, aby wykonawca przeprowadził w siedzibie zamawiającego szkolenia w zakresie konfiguracji i obsługi urządzeń dla 4 osób (2 szkolenia po 2 osoby). Minimalny czas szkolenia 8 godzin zajęć. Minimalny zakres szkolenia:

1) logowanie i monitoring zdarzeń,
2) konfiguracja polityk firewall-a,
3) lokalne uwierzytelnianie użytkowników,
4) tworzenie i monitoring VPN SSL, IPSec-VPN, operacje oparte na certyfikatach,
5) konfiguracja skanowania antywirusowego,
6) konfiguracja filtrów WWW, tworzenie polityk,
7) kontrola aplikacji,
8) konfiguracja Routingu w tym BGP i OSPF,
9) transparently tryb pracy,
10) wysoka dostępność (Klaster HA - High Availability),
11) Intrusion Prevention System - IPS,
12) diagnostyka i rozwiązywanie problemów,
13) zasoby systemowe - optymalizacja,
14) rozwiązywanie problemów sieciowych,
15) rozwiązywanie problemów: z uwierzytelnianiem użytkowników