Znak: IA.272.2.3.2018 **Załącznik nr 1b do SIWZ**

OPIS PRZEDMIOTU ZAMÓWIENIA dla części II

„Dostawa kserokopiarek oraz systemu bezpieczeństwa firewall wraz z systemem raportowania”

do zadania pod nazwą:

„Zakup sprzętu informatycznego wraz z oprogramowaniem”

Przedmiotem zamówienia jest dostawa 2 szt. kserokopiarek oraz systemu bezpieczeństwa firewall wraz z systemem raportowania z pełnym wdrożeniem, który musi zapewniać wszystkie wymienione w opisie 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.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.

W ramach postępowania wymaganym jest dostarczenie i pełne wdrożenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.

KOLOROWE URZĄDZENIE WIELOFUNKCYJNE 2 szt.	
NAZWA PARAMETRU	**WYMAGANIA MINIMALNE**
Technologia druku	technologia laserowa, czterobębnowa
Format oryginału i kopii	A3-A6
Prędkość drukowania	min. 25 stron A4 / min. w kolorze i mono
Rozdzielczość drukowania	600x600 dpi
Czas wydruku pierwszej strony	kolorowej maks. 10 sek., czarno-białej maks. 7 sek.
Czas nagrzewania	maks. 20 sek. od włączenia zasilania
Kopiowanie wielokrotne	do 999 kopii
Pamięć RAM	min. 3 GB
Dysk HDD lub SSD	min. 32 GB
Zoom	25-400%
Panel operatora	Panel wyposażony w kolorowy ekran dotykowy LCD, opisy na panelu oraz komunikaty na ekranie w języku polskim, panel z regulowanym położeniem w min. 2 pozycjach. Integracja z aplikacjami zewnętrznymi poprzez ekran dotykowy urządzenia.
Dupleks	automatyczny, obsługa papieru 80-250 g/m^2
Podajnik dokumentów	Dwustronny, pojemność tacy podającej min. 50 ark. 80 g/m^2
Podajniki papieru	- podajnik automatyczny min. 2 x 500 ark., 80-300 g/m^2 (w tym min. jeden obsługujący papier formatu A3); - taca boczna na min. 150 ark. A6-A3, 60-300 g/m^2
Podstawa	Dedykowana podstawa producenta urządzenia z katalogu dostępnych fabrycznie opcji, zamykana, na kółkach.
Pamięć drukarki	Współdzielona z kopiarką (dotyczy pamięci RAM i HDD)
Emulacje	PCL 6, Post Script Level 3
Interfejsy	USB 2.0, Ethernet 10/100/1000 Mb
Funkcje skanowania	skanowanie do PC, do e-mail, do FTP, TWAIN (sieciowy), do pamięci przenośnej USB, WIA, SMB, do skrzynki dokumentów
Rozdzielczość skanowania	600 dpi
Prędkość skanowania	kolor: min. 40 str. w rozdzielczości min. 300 dpi/A4 na minutę
Typy plików	PDF, PDF/A, PDF szyfrowany, PDF kompresowany, JPEG, TIFF, XPS
Kompresja i szyfrowanie plików PDF	w standardzie
Możliwość rozbudowy	- finiszer z tacą odbiorczą na min. 4000 ark. i min. 3-pozycyjnym zszywaczem na min. 50 ark. A4 80 g/m^2 - standardowy faks analogowy i funkcja PC-faks, - podajnik papieru na min. 3000 ark. A4 (80 g/m^2), 60-300 g/m^2
Materiały eksploatacyjne jako wyposażenie standardowe (dostarczone w komplecie w ramach oferowanej ceny jednostkowej).	Tonery: w ilości, która zapewni wydrukowanie minimum 12 000 stron kolorowych A4 (zgodnie z ISO 19798) Bębny: w ilości, która zapewni wydrukowanie minimum 200 000 stron kolorowych A4. Dostarczone materiały muszą być nowe i nieużywane, oraz wyprodukowane przez producenta oferowanych urządzeń.
Gwarancja	36 miesięcy.

SYSTEM BEZPIECZEŃSTWA FIREWALL WRAZ Z SYSTEMEM RAPORTOWANIA	
NAZWA PARAMETRU	**WYMAGANIA MINIMALNE**
System musi wspierać IPv4 oraz IPv6 w zakresie:	Firewall. Ochrony w warstwie aplikacji. Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego 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. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie:	1. System realizujący funkcję Firewall musi dysponować minimum: - 20 portami Gigabit Ethernet RJ-45. - 2 gniazdami SFP 1 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30 000 nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 7.4 Gbps dla pakietów 512 B. 3. Przepustowość Stateful Firewall: nie mniej niż 4.4 Gbps dla pakietów 64 B. 4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps. 5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 4 Gbps. 6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 1.9 Gbps. 7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps. 8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 190 Mbps.
Funkcje Systemu Bezpieczeństwa:	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być

	zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. Analiza ruchu szyfrowanego protokołem SSH.
Polityki Firewall	System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW. 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. 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. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: - Wsparcie dla IKE v1 oraz v2. - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). - Obsługa 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. - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. - Mechanizm „Split tunneling” dla połączeń Client-to-Site.

	2. 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
Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: - Routingu statycznego. - Policy Based Routingu. - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Kontrola Antywirusowa	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

	2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. 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 avoidance. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania
Uwierzytelnianie użytkowników w ramach sesji	1. 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. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
Logowanie	1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania). W ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy programowej. 2. 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. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
Zarządzanie	1. 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. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: - ICSA lub EAL4 dla funkcji Firewall. - ICSA lub NSS Labs dla funkcji IPS. - ICSA dla funkcji IPSec VPN. - ICSA dla funkcji SSL VPN.
System raportowania i logowania	
Interfejsy, Dysk	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 500 GB.
System raportowania i logowania	1. System musi być w stanie przyjmować minimum 1 GB logów na dzień. 2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.
Logowanie	1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: a. Listę najczęściej wykrywanych ataków.

	b. Listę najbardziej aktywnych użytkowników. c. Listę najczęściej wykorzystywanych aplikacji. d. Listę najczęściej odwiedzanych stron www. e. Listę krajów , do których nawiązywane są połączenia. f. Listę najczęściej wykorzystywanych polityk Firewall. g. Informacje o realizowanych połączeniach IPSec. 4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. 6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
W zakresie raportowania system musi zapewniać	1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów. 4. Możliwość spolszczenia raportów. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
W zakresie korelacji zdarzeń system musi zapewniać	1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System powinien korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: - Malware, - Aplikacje sieciowe, - Email, - IPS, - Traffic, - Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
Zarządzanie	1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. 2. System musi umożliwiać zdefiniowanie co najmniej 8

	administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
GWARANCJA, SERWIS	
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje na czas 36miesiecy upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. - Kontrola Aplikacji, - IPS, - Antywirus, - Antyspam, - Web Filtering.
Rozszerzone wsparcie serwisowe AHB/SOS	1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w **Następnym Dniu Roboczym** od momentu potwierdzenia zasadności zgłoszenia przesłanego na maila, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres **36 miesięcy.** 2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5.