OPIS PRZEDMIOTU ZAMÓWIENIA – część I zamówienia

*Urządzenie typu **Firewall** do ochrony systemu poczty elektronicznej.*

Zawartość

1. CEL ZAMÓWIENIA 2
1.1. Przedmiot zamówienia 2
1.2. Warunki gwarancji i serwisu 14
1.3. Uwagi do przedmiotu zamówienia 15

1. CEL ZAMÓWIENIA

Celem zamówienia jest dostawa urządzenia, co poprawi środowisko pracy podsystemu archiwizacyjnego CPE.

1.1. Przedmiot zamówienia

Przedmiotem zamówienia jest:

1.1.1. Dostawa przez Wykonawcę Urządzenia do CPE,
1.1.2. Dostawa przez Wykonawcę oprogramowania do Urządzenia wraz z licencją, umożliwiającą w pełni korzystanie z modułów opisanych w niniejszym Opisie przedmiotu zamówienia przez okres min. 36 miesięcy.
1.1.3. Udzielenie Zamawiającemu licencji na oprogramowanie do Urządzenia.
1.1.4. Wsparcie techniczne w miejscu działania przez okres 5 dni roboczych po zgłoszeniu przez Zamawiającego instalacji Urządzenia, którego celem będzie implementacja Urządzenia do istniejącej infrastruktury,
1.1.5. Dostarczenie przez Wykonawcę Dokumentacji - technicznej, instrukcji obsługi, kart gwarancyjnych Urządzenia,
1.1.6. Udzielenie przez Wykonawcę gwarancji i zapewnienie serwisu gwarancyjnego przez okres co najmniej 36 miesięcy.
1.1.7. Poniższa tabela przedstawia wymagania **minimalne**, jakie muszą zostać spełnione przez oferowany sprzęt:

1.1.7.1. Firewall A–1 komplet

Poz.	Parametr	Wymagania Minimalne	Parametry oferowane
1.1.7.1.1.	Producent	Brak wymagań	
1.1.7.1.2.	Identyfikator Produktu	Brak wymagań	
1.1.7.1.3.	Przeznaczenie	FIREWALL / PROXY / UTM / WAF (Web Application Firewall)	
	Ineterfejsy:		
1.1.7.1.4.	Liczba interfejsów 10/100/1000 Base-T	8	
1.1.7.1.5.	Port konsolowy	1	
1.1.7.1.6.	Port USB	1	
1.1.7.1.7.	Konfigurowalne porty internal/external/DMZ	TAK	
	Wydajność:		
1.1.7.1.8.	Prepustowość firewall	3500 MBps	
1.1.7.1.9.	Liczba równoległych sesji	1000000	
1.1.7.1.10.	Liczba nowych sesji na sekundę	20000	
1.1.7.1.11.	Liczba obsługiwanych użytkowników	nieograniczona	
1.1.7.1.12.	Liczba wirtualnych routerów	2	
1.1.7.1.13.	Liczba VLAN (definiowanych w oparciu o standard IEEE802.1q)	512 interfejsów wirtualnych	
1.1.7.1.14.	Liczba tuneli IPSec VPN	200	
1.1.7.1.15.	Przepustowość IPS	1000 MBps	

1.1.7.1.16.	Przepustowość Anti-Virus	1000 MBps	
1.1.7.1.17.	Przepustowość UTM	600 Mbps	
1.1.7.1.18.	Przepustowość tunelu IPSec VPN	350 Mbps	
	Parametry użytkowe		
1.1.7.1.19.	Uwierzytelnianie użytkowników poprzez Active Directory, LDAP, Radius oraz lokalną bazę użytkowników	Musi być zapewnione	
1.1.7.1.20.	Automatyczne uwierzytelnianie użytkowników w oparciu o Single Sign On	Musi być zapewnione	
1.1.7.1.21.	Wsparcie dla uwierzytelnienia w środowisku Microsoft Windows	Musi być zapewnione	
1.1.7.1.22.	Wysoka dostępność	Rozwiązanie musi: ○ umożliwiać pracę w klastrze active – active oraz acitve – pasive; ○ ruch w klastrze HA pomiędzy urządzeniami musi być szyfrowany; ○ urządzenie ma wspierać automatyczną i ręczną synchronizację urządzeń w klastrze	
1.1.7.1.23.	Moduł Firewall	○ Rozwiązanie musi pozwalać na określenie nazw użytkowników, adresów źródłowych docelowych i podsieci jeko kryteriów przy tworzeniu reguł na firewall'u; ○ System musi zapewniać możliwość tworzenia reguł na	

		firewall'u w oparciu adres MAC; o Rozwiązanie musi umożliwiać określenie przepustowości łącza dla konkretnej aplikacji np.: Skype; o Rozwiązanie musi wspierać protokoły routingu: RIP1, RIP2, OSPF, BGP4; o Rozwiązanie musi wspierać konfigurację routingu statycznego i dynamicznego z poziomu wiersza poleceń zgodnego z CISCO; o Rozwiązanie musi obsługiwać translacje adresów PAT, NAT	
1.1.7.1.24.	Moduł Antywirus	Musi wspierać: o skanowanie protokołow: SMTP, POP3, IMAP, FTP, http, HTTPS; Skanowanie ruchu HTTP w oparciu o nazwę użytkownika, adres źródłowy i docelowy lub adres URL w notacji wyrażenia regularnego; o musi pracować jako SMTP Proxy; o musi dla ruchu POP3 i IMAP musi usuwać zawirusowany załącznik i przesłać odpowiednią informację do odbiorcy i administratora	
1.1.7.1.25.	Moduł Antyspam	Musi wspierać protokoły: o SMTP (z możliwością włączania/wyłączania skanowania dla autoryzowanego ruchu), POP3, IMAP, współpracować z bazą RBL, umożliwiać tworzenie białych i czarnych list adresów IP i e-mail; o zapewniać wykrywanie spamu niezależnie od stosowanego języka; o blokować spam w postaci plików graficznych np. tekst osadzony w obrazku; o oferować moduł kwarantanny z możliwością samoobsługi przez użytkowników (zwalnianie wiadomości)	
1.1.7.1.26.	Moduł filtrowania www	Musi umożliwiać: o blokowanie wysyłania treści poprzez http i HTTPS, blokadę stron HTTPS;	

		○ blokowanie anonimowego Proxy poprzez HTTP i HTTPS; ○ definiowanie polityk dostępu do internetu w oparciu o harmonogramy; ○ musi zawierać lokalną bazę kategorii stron (nie powinno wysyłać zapytań do zewnętrznych baz danych); ○ musi zawierać przynajmniej 50 kategorii stron WWW i umożliwiać tworzenie własnych kategorii	
1.1.7.1.27.	Moduł kontroli aplikacji	Musi identyfikować: ○ aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania, rozpoznawać przynajmniej 2000 aplikacji ○ musi umożliwiać blokowanie aplikacji, które pozwalają na transfer plików(np. P2P), komunikatorów internetowych (np.: Gadu-Gadu, Skype), Proxy uruchamianych przez przeglądarki internetowe, streaming media (np.: radio internetowe, Youtube, Vimeo)	
1.1.7.1.28.	Moduł IPS	Musi posiadać: ○ bazę sygnatur (minimum 3000 sygnatur); ○ umożliwiać tworzenie własnych sygnatur IPS; ○ automatycznie pobierać aktualizacje; ○ umożliwiać włączanie / wyłączanie poszczególnych sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów; ○ generować alerty w przypadku ataku	
1.1.7.1.29.	VPN	Musi wspierać: ○ połączenia VPN IPSec (Net-to-Net, Host-to-Host, Client-to-Site), L2TP i PPTP, ○ algorytmy szyfrowania DES, 3Des, AES; ○ lokalne i zewnętrzne centrum certyfikacji; ○ obsługiwać ogólnodostępnych klientów IPSec VPN; ○ zapewniać wbudowany moduł SSL VPN; ○ oferować możliwość skanowania antywirusowego	

		i antyspamowego tuneli VPN (IPSec/L2TP/PPTP); o oferować VPN failover	
1.1.7.1.30.	Zarządzanie	Musi umożliwiać: o tworzenie kont administracyjnych o różnych uprawnieniach; o automatyczne wylogowanie administratora po określonym czasie bezczynności; o definiowanie polityk hasłowych dla administratorów; o wspierać zarządzanie poprzez bezpieczne kanały komunikacji – HTTPS, SSH, konsolę; o wspierać SNMP v1, SNMP v2, SNMP v3; o monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM Obciążenie interfejsów sieciowych); o przechowywanie przynajmniej dwóch wersji firmware; o umożliwiać automatyczne wykonywanie kopii zapasowej konfiguracji systemu.	
1.1.7.1.31.	Logowanie i raportowanie	System musi: o umożliwiać składowanie i archiwizację logów, gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL, VPN wykorzystywanych aplikacjach sieciowych, wykrytych atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych o powiązać powyższe zdarzenia z nazwami użytkowników; o zapewniać monitoring ryzyka związanego z działanie aplikacji sieciowych uruchamianych przez użytkowników np. : klasyfikując ryzyka wg skali; o zapewnić generowanie raportów na zgodność z normami: HIPAA, SOX, PCI; o export zgromadzonych logów do zewnętrznych systemów składowania danych; o umożliwiać wysyłanie raportów na pocztę	

		elektroniczną; ○ generować reporty w formatach PDF i HTML; ○ wspierać wiele serwerów syslog (przynajmniej 2 serwery syslog) ○ zbierać logi z urządzeń UTM, Proxy i innych zgodnych z syslog; ○ statystyki muszą zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym;	
1.1.7.1.32.	Gwarancja	36 miesięcy	
	Hardware	-	-
1.1.7.1.33.	Obudowa, montaż	Obudowa oraz elementy do montażu w standardowej szefie RACK 19” max. wysokość urządzenia w szafie może wynieść 2U	
1.1.7.1.34.	Zasilanie (zmienne 230V / 50Hz)	Jeden zasilacz	
1.1.7.1.35.	Pamięć DRAM (zainstalowana)	2 GB	
1.1.7.1.36.	Dysk twardy (do celów logowania i raportowania)	120 GB	

1.1.7.2. Firewall B –1 komplet

Poz.	Parametr	Wymagania Minimalne	Parametry oferowane
1.1.7.2.1.	Producent	Brak wymagań	
1.1.7.2.2.	Identyfikator Produktu	Brak wymagań	
1.1.7.2.3.	Przeznaczenie	FIREWALL / PROXY / UTM	
	Ineterfejsy:		
1.1.7.2.4.	Liczba interfejsów 10/100/1000 Base-T	6	

1.1.7.2.5.	Port konsolowy	1	
1.1.7.2.6.	Port USB	1	
1.1.7.2.7.	Konfigurowalne porty internal/external/DMZ	TAK	
	Wydajność:		
1.1.7.2.8.	Prepustowość firewall	1500 MBps	
1.1.7.2.9.	Liczba równoległych sesji	300000	
1.1.7.2.10.	Liczba nowych sesji na sekundę	8000	
1.1.7.2.11.	Liczba obsługiwanych użytkowników	nieograniczona	
1.1.7.2.12.	Liczba wirtualnych routerów	2	
1.1.7.2.13.	Liczba VLAN (definiowanych w oparciu o standard IEEE802.1q)	512 interfejsów wirtualnych	
1.1.7.2.14.	Liczba tuneli IPSec VPN	100	
1.1.7.2.15.	Przepustowość IPS	300 MBps	
1.1.7.2.16.	Przepustowość Anti-Virus	300 MBps	
1.1.7.2.17.	Przepustowość UTM	200 Mbps	
1.1.7.2.18.	Przepustowość tunelu IPSec VPN	200 Mbps	
	Parametry użytkowe		
1.1.7.2.19.	Uwierzytelnianie użytkowników poprzez Active Directory, LDAP, Radius oraz lokalną	Musi być zapewnione	

	bazę użytkowników		
1.1.7.2.20.	Automatyczne uwierzytelnianie użytkowników w oparciu o Single Sign On	Musi być zapewnione	
1.1.7.2.21.	Wsparcie dla uwierzytelnienia w środowisku Microsoft Windows	Musi być zapewnione	
1.1.7.2.22.	Moduł Firewall	○ Rozwiązanie musi pozwalać na określenie nazw użytkowników, adresów źródłowych docelowych i podsieci jeko kryteriów przy tworzeniu reguł na firewall'u; ○ System musi zapewniać możliwość tworzenia reguł na firewall'u w oparciu adres MAC; ○ Rozwiązanie musi umożliwiać określenie przepustowości łącza dla konkretnej aplikacji np.: Skype; ○ Rozwiązanie musi wspierać protokoły routingu: RIP1, RIP2, OSPF, BGP4; ○ Rozwiązanie musi wspierać konfigurację routingu statycznego i dynamicznego z poziomu wiersza poleceń zgodnego z CISCO; ○ Rozwiązanie musi obsługiwać translacje adresów PAT, NAT	
1.1.7.2.23.	Moduł filtrowania www	Musi umożliwiać: ○ blokowanie wysyłania treści poprzez http i HTTPS, blokadę stron HTTPS; ○ blokowanie anonimowego Proxy poprzez HTTP i HTTPS; ○ definiowanie polityk dostępu do internetu w oparciu o harmonogramy; ○ musi zawierać lokalną bazę kategorii stron (nie	

		powinno wysyłać zapytań do zewnętrznych baz danych); ○ musi zawierać przynajmniej 50 kategorii stron WWW i umożliwiać tworzenie własnych kategorii	
1.1.7.2.24.	Moduł IPS	Musi posiadać: ○ bazę sygnatur (minimum 3000 sygnatur); ○ umożliwiać tworzenie własnych sygnatur IPS; ○ automatycznie pobierać aktualizacje; ○ umożliwiać włączanie / wyłączanie poszczególnych sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów; ○ generować alerty w przypadku ataku	
1.1.7.2.25.	VPN	Musi wspierać: ○ połączenia VPN IPSec (Net-to-Net, Host-to-Host, Client-to-Site), L2TP i PPTP, ○ algorytmy szyfrowania DES, 3Des, AES; ○ lokalne i zewnętrzne centrum certyfikacji; ○ obsługiwać ogólnodostępnych klientów IPSec VPN; ○ zapewniać wbudowany moduł SSL VPN; ○ oferować możliwość skanowania antywirusowego i antyspamowego tuneli VPN (IPSec/L2TP/PPTP); ○ oferować VPN failover	
1.1.7.2.26.	Zarządzanie	Musi umożliwiać: ○ tworzenie kont administracyjnych o różnych uprawnieniach; ○ automatyczne wylogowanie administratora po określonym czasie bezczynności; ○ definiowanie polityk hasłowych dla administratorów; ○ wspierać zarządzanie poprzez bezpieczne kanały komunikacji – HTTPS, SSH, konsolę; ○ wspierać SNMP v1, SNMP v2, SNMP v3; ○ monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM Obciążenie interfejsów sieciowych);	

		○ przechowywanie przynajmniej dwóch wersji firmware; ○ umożliwiać automatyczne wykonywanie kopii zapasowej konfiguracji systemu.	
1.1.7.2.27.	Logowanie i raportowanie	System musi: ○ umożliwiać składowanie i archiwizację logów, gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL, VPN wykorzystywanych aplikacjach sieciowych, wykrytych atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych ○ powiązać powyższe zdarzenia z nazwami użytkowników; ○ zapewniać monitoring ryzyka związanego z działanie aplikacji sieciowych uruchamianych przez użytkowników np. : klasyfikując ryzyka wg skali; ○ zapewnić generowanie raportów na zgodność z normami: HIPAA, SOX, PCI; ○ export zgromadzonych logów do zewnętrznych systemów składowania danych; ○ umożliwiać wysyłanie raportów na pocztę elektroniczną; ○ generować reporty w formatach PDF i HTML; ○ wspierać wiele serwerów syslog (przynajmniej 2 serwery syslog) ○ zbierać logi z urządzeń UTM, Proxy i innych zgodnych z syslog; ○ statystyki muszą zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym;	
1.1.7.2.28.	Gwarancja	36 miesięcy	
	Hardware	-	-
1.1.7.2.29.	Obudowa, montaż	Obudowa oraz elementy do montażu w standardowej szefie RACK 19” max. wysokość urządzenia w szafie może wynieść 2U	

1.1.7.2.30.	Zasilanie (zmienne 230V / 50Hz)	Jeden zasilacz	
1.1.7.2.31.	Pamięć DRAM (zainstalowana)	1 GB	
1.1.7.2.32.	Dysk twardy (do celów logowania i raportowania)	120 GB	

1.2. Warunki gwarancji i serwisu

Poniższa tabela zawiera minimalne wymagania stawiana warunkom gwarancji i serwisu urządzenia

Warunki gwarancji i serwisu	Wymagane
Czas reakcji serwisu liczony od chwili zgłoszenia do chwili przystąpienia do usunięcia usterki – maksymalnie 48 h	TAK
Możliwość zgłaszania napraw 24h/dobę i przez 365 dni w roku, za pomocą faksu i drogą elektroniczną lub za pomocą połączenia telefonicznego przeznaczonego do zgłaszania awarii	TAK
Czas oczekiwania na usunięcie uszkodzenia w przypadku konieczności importu części	TAK, nie więcej niż 5 dni roboczych
Czas oczekiwania na usunięcie uszkodzenia nie wymagającego importu części zamiennych	TAK, nie więcej niż 3 dni robocze
Graniczny czas naprawy gwarancyjnej, po przekroczeniu, którego okres gwarancji przedłuża się o czas przerwy w eksploatacji	2 dni
Liczba napraw gwarancyjnych uprawniająca do wymiany podzespołu na nowe (z wyjątkiem uszkodzeń z winy użytkownika)	3 naprawy
Naprawy i konserwacja sprzętu w okresie gwarancji będą odbywać się w miejscu jego eksploatacji. Jeżeli zaistnieje konieczność naprawy poza siedzibą Zamawiającego, Wykonawca odbierze uszkodzony element i dostarczy go do Zamawiającego po zakończonej naprawie na własny koszt i ryzyko, a na okres naprawy dostarczy urządzenie zastępcze	TAK

o parametrach nie gorszych niż eksploatowane	

1.3. Uwagi do przedmiotu zamówienia

1.3.1. **Składana oferta musi odpowiadać warunkom nie gorszym niż określone poniżej Uwagi:**

1.3.1.1. Oferowane urządzenia muszą spełniać wszystkie parametry określone w niniejszym załączniku oraz być fabrycznie nowe. Wykonawca może zaoferować produkty o parametrach lepszych niż określone w niniejszym załączniku.

1.3.1.2. Wykonawca winien przedstawić nazwę producenta i model oferowanego sprzętu w poszczególnych jego rodzajach, a parametrami rzeczywistymi opisać oferowany sprzęt.

1.3.1.3. Zamawiający informuje, że obecnie eksploatuje następujące urządzenia: Microsoft Forefront TMG 2010 i Cyberoam 35 wi, i zgodnie z planem dostosowania sieci komputerowej do rosnących potrzeb zapewniania bezpieczeństwa w ruchu sieciowym, poprzez zdwojenie urządzeń do pracy w klastrze analogicznych urządzeń lub poprzez rozdzielenie sygnału na parę odpowiednich urządzeń filtrujących (do wyboru w dowolnym czasie przez Zamawiającego) oraz zapewnieniem działania obecnie działających mechanizmów dostępu zdalnego do poczty elektronicznej i szyfrowanych połączeń VPN, przy założeniu, że dysponuje określonym oprogramowaniem zarządzającym dołączonym do obecnie eksploatowanych urządzeń lub oprogramowaniem dołączonym do nowo dostarczanych urządzeń, zamierza zrealizować niniejsze zamówienie celem zastosowania urządzeń tożsamych co do modelu do obecnie eksploatowanych lub w pełni zgodnych z nimi dla osiągnięcia najlepszego efektu bezpieczeństwa. Opierając sie na informacjach od producenta urządzenia posiadanego przez Zamawiającego, Zamawiający dopuszcza ofertę polegającą na wymianie Microsoft Forefront TMG 2010, w trybie upgrade urządzenia wg promocyjnego programu cenowego określanego przez producenta, pod warunkiem, że Wykonawca nie będzie żądał zwrotu posiadanego już urządzenia. Ponadto, z informacji od producenta, wynika, że nie jest możliwe uzyskanie pełnego wsparcia technicznego w rozumieniu przedłużenia obecnego serwisu na wymieniony produkt eksploatowany przez Zamawiającego.

Powyższe upoważnia Zamawiającego, na podstawie art. 29 ust. 3 Pzp, do dokładnego określenia przedmiotu zamówienia przez podanie producenta i modelu urządzeń – w punkcie 1.3.1.3 wymagań zakresu technicznego, z uwagi na specyfikę przedmiotu zamówienia. Zamawiający informuje, że jeżeli Wykonawca zaproponuje rozwiązanie równoważne w zakresie utworzenia klastra firewalli z firewalla będącego przedmiotem zamówienia z obecnie eksploatowanym (Cyberoam 35wi) u Zamawiającego, które nie pozwoli na funkcjonowanie prawidłowe obu układów jako zmodernizowanych całości lub nie będzie możliwe zagwarantowanie serwisu technicznego dla Zamawiającego, w tym gwarancyjnego, producenta/ów i Wykonawcy/ów odnośnie już eksploatowanego firewalla

w czasie eksploatacji w związku z różnorodnością sprzętową i systemową, rozwiązanie oferowane będzie niezgodne z wymaganiem Zamawiającego.