Opis przedmiotu zamówienia

załącznik nr 6 do SIWZ

Przedmiotem jest stworzenie bezpiecznego punktu styku sieci z Internetem przy wykorzystaniu urządzeń typu firewall/UTM, dostawa i instalacja przełączników sieciowych oraz zasilaczy UPS.

II.1. Dostarczyć i skonfigurować dwa urządzeń typu firewall/UTM *(unified threat management)* działających w klastrze o parametrach pozwalających aktywnie korzystać z zasobów Internetu 300 użytkownikom. Urządzenia powinny działać w konfiguracji wysokiej dostępności (High Availabity), w trybie Active/Active lub Active/ Passive.

Szczegółowa charakterystyka urządzenia zabezpieczającego sieć przedstawia tabela:

Lp.	Parametr	Wymagania techniczne
1	Architektura systemu ochrony	System ochrony musi być zbudowany przy użyciu minimalnej ilości elementów ruchomych, krytycznych dla jego działania. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanych układów ASIC. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie).
2	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia.
3	Parametry fizyczne systemu	Nie mniej niż 6 portów Ethernet 10/100/1000 Base-TX. Obudowa ma mieć możliwość zamontowania w szafie 19”.
4	Funkcjonalności podstawowe i uzupełniające	System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych: ✓ kontrolę dostępu - zaporę ogniową klasy Stateful Inspection ✓ ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM, NNTP) ✓ poufność danych - IPSec VPN oraz SSL VPN ✓ ochronę przed atakami - Intrusion Prevention System [IPS/IDS]. oraz funkcjonalności uzupełniających: ✓ kontrolę treści i kategoryzację odwiedzanych stron WWW – ✓ Web\URL Filter ✓ kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) ✓ kontrolę pasma oraz ruchu [QoS, Traffic shaping] ✓ kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM, P2P, VoIP, Web-mail) ✓ zapobieganie przed wyciekiem informacji poufnej - DLP (Data Leak Prevention) ✓ SSL proxy z możliwością pełniej analizy szyfrowanej komunikacji dla wybranych protokołów
5	Zasada działania (tryby)	Urządzenie powinno dawać możliwość ustawienia jednego z dwóch trybów pracy: ✓ jako router/NAT (3.warstwa ISO-OSI) lub ✓ jako most /transparent bridge/ . Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu.

Opis przedmiotu zamówienia

załącznik nr 6 do SIWZ

Lp.	Parametr	Wymagania techniczne
6	Polityka bezpieczeństwa (firewall)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, domeny, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie, zarządzanie pasmem sieci (m.in. pasma gwarantowane i maksymalne, priorytety, oznaczenia DiffServ). Urządzenie powinno umożliwiać utworzenie nie mniej niż **6.000** polityk firewall'a
7	Wykrywanie ataków	Wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. Nie mniej niż 4000 sygnatur ataków. Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie Możliwość dodawania własnych sygnatur ataków Możliwość wykrywania anomalii protokołów i ruchu
8	Moduł antywirusowy	Antywirus powinien mieć możliwość transferu częściowo przeskanowanego plik do klienta w celu zapobiegnięcia przekroczenia dopuszczalnego czasu oczekiwania (timeout). Antywirus powinien przeprowadzać sprawdzanie danych zarówno po bazie sygnatur wirusów jak i heurystycznie.
9	Moduł antyspam	Zawarty moduł antyspamowy powinien pracować w obrębie protokołów SMTP, POP3 i IMAP Klasyfikacja wiadomości powinna bazować na wielu czynnikach, takich jak: sprawdzenie zdefiniowanych przez administratora adresów IP hostów, które brały udział w dostarczeniu wiadomości, sprawdzenie zdefiniowanych przez administratora adresów pocztowych, RBL, ORDBL Sprawdzenie treści pod kątem zadanych przez administratora słów kluczowych Oprócz powyższego mechanizm antyspamowy powinien umożliwiać skorzystanie z zewnętrznej, wieloczynnikowej bazy spamu.
10	Filtracja stron WWW	Moduł filtracji stron www powinien umożliwiać blokowanie stron w oparciu o: białe i czarne listy URL o zawarte w stronie słowa kluczowe dynamicznie definiowane przez producenta kategorie.
11	Translacja adresów	Statyczna i dynamiczna translacja adresów (NAT). Translacja NAPT. NAT traversal dla protokołów SIP i H323
12	Wirtualizacja i routing dynamiczny	Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne tabele routingu, polityki bezpieczeństwa i dostęp administracyjny. Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego. Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM.

Lp.	Parametr	Wymagania techniczne
13	Połączenia VPN	Wymagane nie mniej niż: Tworzenie połączeń w topologii Site-to-Site oraz Client-to-Site Dostawca musi udostępniać klienta VPN własnej produkcji realizującego następujące mechanizmy ochrony końcówki: • firewall • antywirus • web filtering • antyspam Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN) Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
14	Uwierzytelnianie użytkowników	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych Rozwiązanie powinno umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych.
15	Wydajność	Obsługa nie mniej niż **500.000** jednoczesnych połączeń i **15.000** nowych połączeń na sekundę Przepływność nie mniejsza niż **5 Gbps** dla ruchu nieszyfrowanego i **2,5 Gbps** dla VPN (3DES). Obsługa nie mniej niż **2.000** jednoczesnych tuneli VPN
16	Funkcjonalność zapewniająca niezawodność	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive
17	Konfiguracja i zarządzanie	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: haseł statycznych haseł dynamicznych (RADIUS, RSA SecureID) System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB. Jednocześnie, dla systemu urządzenie powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.
18	Raportowanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym: Zbieranie logów z urządzeń bezpieczeństwa Generowanie raportów Skanowanie podatności stacji w sieci Zdalną kwarantannę dla modułu antywirusowego

Lp.	Parametr	Wymagania techniczne
19	Serwis oraz aktualizacje	1. Dostawca zobowiązany jest: 1) udzielić Zamawiającemu stałych bezterminowych licencji na użytkowanie zainstalowanego oprogramowania (systemu operacyjnego) 2) dokonywać bezpłatnych aktualizacji (upgradów) oprogramowania w okresie trwania gwarancji 3) udzielić Zamawiającemu gwarancji i rękojmi jakości na dostarczony sprzęt (wraz z zainstalowanym oprogramowaniem) na okres minimum 3 lat, licząc od daty zakończenia i odbioru. 2. Oferowany sprzęt wraz z zainstalowanym oprogramowaniem, musi pochodzić z legalnego źródła tj. być zakupiony w autoryzowanym kanale sprzedaży producenta na terenie Polski oraz być objęty pakietem usług gwarancyjnych zawartych w cenie dostawy urządzeń i świadczonych przez sieć serwisową producenta na terenie Polski
20	Certyfikaty	Potwierdzeniem wysokiej skuteczności systemów bezpieczeństwa są posiadane przez producenta certyfikaty. Producent musi posiadać następujące certyfikaty: ISO 9001, UTM NSS Approved, EAL4+, ICSA Labs dla funkcji: Firewall, IPSec, SSL, Network IPS, Antywirus.
21	Wyposażenie dodatkowe	Redundatny zasilacz

1. Instalacja i konfiguracja systemu powinna być przeprowadzona przez osoby posiadające odpowiednie kwalifikacje i doświadczenie tj. najwyższy stopień certyfikacji producenta oferowanych urządzeń,

2. Przeprowadzenie szkolenia w zakresie konfiguracji i obsługi dostarczonego urządzenia firewall/UTM (w zakresie podstawowym i rozszerzonym – min. 2 dni szkolenia po 8 godzin) oraz z zakresu obsługi i konfiguracji urządzenia analizującego logi, dla min. 2 osób (przedstawicieli Zamawiającego). Szkolenie musi zostać przeprowadzone przez osobę posiadającą stosowe uprawnienia producenta urządzeń.

3. Warunki gwarancji i suportu na urządzenia firewall/UTM:
   - okres gwarancji na urządzenia min. 36 miesięcy
   - okres subskrypcji na poszczególne funkcjonalności firewall/UTM min.36 miesięcy
   - okres suportu na urządzenia 36 miesięcy
   - przyjmowanie zgłoszeń przez telefon, za pośrednictwem e-mail, www lub faxem.
   - maksymalny czas naprawy lub wymiany urządzeń - 14 dni roboczych od dnia powiadomienia o stwierdzonej usterce (wadzie).
   - dostęp do telefonicznego wsparcia technicznego w języku polskim w okresie trwania suportu.
   - bezpłatne udostępnianie aktualizacji oprogramowania urządzeń (firmware) do najnowszej dostępnej wersji (w okresie trwania gwarancji).

II.2. „Dostawa, instalacja i konfiguracja przełączników sieciowych i zasilaczy UPS".

Opis przedmiotu zamówienia

załącznik nr 6 do SIWZ

II.2.1. Przełącznik sieciowy HP 5120-48G EI (JE067A), 48 Portów 10/100/1000 Mb/s RJ-45 + 4 Porty 1000 SFP, lub równoważny - **sztuk 8.**

Opis Parametrów równoważności:

a) liczba poszczególnych portów,
b) liczba Vlanów,
c) wydajność,
d) obsługiwane protokoły i spełniane standardy,
e) możliwość zarządzania poprzez oprogramowanie 3Com Intelligent Management Center.

II.2.2. Przełącznik sieciowy HP 1810-24G (J9450A) - **2 sztuki** lub równoważny.

Opis Parametrów równoważności:

a) liczba poszczególnych portów,
b) wydajność,
c) obsługiwane protokoły i spełniane standardy,

II.2.3. Przełącznik sieciowy HP E4800-24G-SFP (JD009A) – **2 sztuki** (komplety) lub równoważny.

Opis Parametrów równoważności:

a) liczba poszczególnych portów,
b) liczba Vlanów,
c) wydajność,
d) obsługiwane protokoły i spełniane standardy,
e) możliwość zarządzania poprzez oprogramowanie 3Com Intelligent Management Center.

Wyposażenie dodatkowe:
a) Moduł 2 x 10 Gigabit Local Connection Module (JE051A)
b) Kabel CX4 - 50cm – **2 szt**.

II.2.4. Patchcord światłowodowy jednomodowy odpowiedni do zastosowanych modułów SFP (LC lub SC) z jednej strony oraz SC/APC z drugiej strony. Długość ok. 1m. – **razem 20 sztuk.**

II.2.5. Patchcord światłowodowy SC/APC – SC/APC simlex 2m – **10 szt.**

II.2.6. Para modułów SFP 1000 Mbps, Wave Division Multiplexing (WDM) – **14 par** – (**razem 28 sztuk modułów**):

- zasięg min - 20 km.
- moduły muszą poprawnie współpracować z przełącznikami firmy HP.

II.2.7. Zasilacz bezprzerwowy, UPS – **7 szt.**

- moc pozorna: min. 400 VA
- moc rzeczywista: min 250 Wat
- liczba i rodzaj gniazdek z utrzymaniem zasilania: min. 2 x IEC320 C13 (10A)
- typ gniazda wejściowego: IEC320 C14 (10A)
- min. pojemność akumulatora: 12v 7Ah

- min. czas podtrzymania dla obciążenia 200W: 8 min
- min. czas podtrzymania przy obciążeniu 50W: 50 min
- sygnalizacja wizualna na obudowie (diody, wyświetlacz itp.):
    - konieczna wymiana baterii,
    - praca z baterii,
    - praca z sieci zasilającej,
    - przeciążenia UPSa