



AT.ZP.271.26.2024 ZCH.RMN

Załącznik nr 1-2 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI II

Dostawa fabrycznie nowego sprzętu i oprogramowania oraz wdrożenie urządzenia sieciowego na potrzeby Domu Pomocy Społecznej „Leśna Oaza” w Słupsku

1) Zakup sprzętu do DPS „Leśna Oaza” w Słupsku

Pozycja 1	
Przedmiot zamówienia:	Zasilacz UPS +SNMP
Ilość:	1 sztuka
Okres gwarancji producenta:	24 m-ce
Parametry	
Obudowa	Tower +Rack
Topologia	Line-interactive
Moc pozorna	Minimum 3000 VA
Moc skuteczna	Minimum 2700 W
Napięcie wejściowe	0 - 300 V
Gniazda wyjściowe	Minimum IEC - 9 szt., RJ-45 (in/out)
Czas przełączania	do 7 ms
Średni czas ładowania	do 7 h
Interfejs komunikacyjny	USB, Karta SNMP do zdalnego zarządzania UPS-em przez sieć LAN
Dodatkowe wymagania	Automatyczna regulacja napięcia (AVR), Funkcja awaryjnego wyłączania zasilania EPO (Emergency Power Off)
Dołączone akcesoria	Kabel zasilający, Oprogramowanie, Zestaw montażowy, Kabel USB, Wtyczka EPO



Pozycja 2	
Przedmiot zamówienia:	Sprzętowe urządzenie sieciowe klasy UTM
Ilość:	1 sztuka
Okres gwarancji producenta:	24 m-ce
Parametry	
Przepustowość Firewall (1518 bajtów UDP)	Min. 4 Gbps
Przepustowość IPS	Min. 1 Gbps
Przepustowość ochrony	Min. 600 Mbps
Liczba jednoczesnych sesji	Min. 400 000
Nowe sesje na sekundę	Min. 30 000
Interfejsy	Min. 3 x Ethernet 100/1000 RJ45
Pamięć na logi	Min. Karta MicroSD lub pamięć wewnętrzna
Układ TPM	Tak

Wymagania/funkcjonalność

- Interfejs administracyjny urządzeń w języku polskim lub angielskim.
- Jednodniowe wdrożenie w ustalonym przez strony dniu, urządzenia w jednostce Zamawiającego przez przedstawiciela Wykonawcy posiadającego odpowiednią wiedzę.
- Jedna godzina zdalnego wsparcia po wdrożeniu, do wykorzystania w okresie 12 miesięcy od wdrożenia – łącznie 1 godzina.
- W okresie aktywnego serwisu podstawowego bezpłatna usługa wymiany urządzenia w razie awarii niemożliwej do usunięcia przez pomoc techniczną, otrzymanie sprawnego urządzenia w terminie maksymalnie 14 dni roboczych od dnia dostarczenia wadliwego urządzenia przez Dystrybutora na adres kontaktowy Producenta.
- Możliwość uruchomienia dla urządzeń zarządzania centralnego, bezpłatnie lub po wykupieniu dodatkowej opcji.
- Sprzęt musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w styczniu 2023 r., dostarczony w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Nie dopuszcza się zastosowania urządzeń tzw. „refurbished”.
- Gwarancja producenta min. 2 lata.
- Minimum 2 lata gwarancji na usługę wdrożenia od zakończenia wdrożenia.

9. Zarządzanie przez stronę www.
10. Serwisy podstawowe z aktualizacjami na min. 24 miesiące - nin. IDS/IPS, IPSec + SSL VPN, Antywirus, Filtr URL, Antyspam.
11. Bezpłatne zdalne wsparcie techniczne dystrybutora w języku polskim, przez min. okres ważności serwisu podstawowego, świadczone telefonicznie oraz drogą elektroniczną.
12. Min. 4 letni okres możliwego wsparcia i udostępnienia serwisów dla urządzeń od daty ich dostarczenia Zamawiającemu.

Obsługa sieci

1. Wsparcie dla protokołu IPv4 oraz IPv6 na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
2. Dla urządzeń możliwość konfiguracji min. 2x. WAN.

Zapora (Firewall)

1. Firewall klasy Stateful Inspection.
2. Translacja adresów NAT n:1, NAT 1:1 oraz PAT.
3. Ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej.
4. Tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów w Interface (GUI). Określanie parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
5. Budowanie reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
6. Filtrowanie na podstawie adresów MAC.
7. Edytor reguł firewall ma wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
8. Wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
9. Budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

Intrusion Prevention System (IPS)

1. System detekcji i prewencji włamań (IPS) zaimplementowany w jądrze systemu, wykrywa włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
2. Moduł IPS opracowany przez producenta urządzenia.
3. Tworzenie własnych sygnatur dla systemu IPS.
4. Moduł IPS nie tylko wykrywa, ale również usuwa szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
5. Inspekcja ruchu tunelowanego wewnątrz protokołu SSL, w zakresie analizy HTTPS, POP3S oraz SMTPS.
6. Konfiguracja jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
7. Ochronę przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
8. Automatyczna aktualizacja sygnatur kontekstowych.

Ochrona antywirusowa

1. Minimum jeden skaner antywirusowy dostarczany w ramach podstawowej licencji.
2. Określenie maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
3. Definiowanie treści komunikatu dla użytkownika o wykryciu infekcji.

Ochrona antyspam

Mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
Ochrona antyspam działa w oparciu o: białe/czarne listy, DNS RBL, Skaner heurystyczny.

Wirtualne sieci prywatne (vpn)

1. Tworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
2. Wspierane typy sieci VPN: IPSec VPN, SSL VPN.

Filtr dostępu do stron WWW a) Wbudowany filtr URL.

1. Filtr URL działający w oparciu o klasyfikację URL stron internetowych.
2. Dodawanie własnych kategorii URL.
3. Definiowanie akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru:
 - blokowanie dostępu do adresu URL, zezwolenie na dostęp do adresu URL,
 - blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
4. Filtr URL uwzględnia komunikację po protokole HTTPS.
5. Tworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

Uwierzytelnianie

W oparciu o lokalną bazę użytkowników (wewnętrzny LDAP), zewnętrzną bazę użytkowników (zewnętrzny LDAP), usługę katalogową Microsoft Active Directory.

Administracja łączami do internetu (ISP)

1. Wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
2. Przełączenie na łącznie zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
3. Monitorowanie dostępności łącza w oparciu o ICMP oraz TCP.

Administracja urządzeniem

1. Konfiguracja urządzenia z wykorzystaniem polskiego interfejsu graficznego.
2. Interfejs konfiguracyjny dostępny poprzez przeglądarkę internetową, a komunikacja poprzez zaszyfrowany protokół HTTPS.
3. Wskazanie do komunikacji innego portu niż 443 TCP.
4. Zarządzanie z poziomu konsoli (SSH)
5. Możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania.
6. Wbudowany webowy, graficzny interfejs administracyjny urządzenia oferuje narzędzia diagnostyczne ping, traceroute, nslookup.
7. Wbudowany webowy, graficzny interfejs administracyjny zawiera narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
8. Wbudowany webowy, graficzny interfejs administracyjny zawiera zdefiniowane polityki hasel stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
9. Definiowanie własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
10. Eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
11. Eksportowanie backupu konfiguracji (kopia zapasowa) w zakresie manualnego eksportu do pliku w dowolnym momencie czasu.
12. Anonimizacja logów w zakresie adresu źródłowego oraz nazwy użytkownika.
13. Ręczna aktualizacja baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

Raportowanie

1. Wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. Wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. Predefiniowane raporty dla ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
4. Eksport wyników raportu do formatu CSV.
5. Monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

Usługi i funkcje

1. Wbudowany DHCP z dynamicznym jak i statycznym przypisywaniem adresu IP do adresu MAC karty sieciowej.
2. Przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
3. Tworzenie różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
4. Usługa DNS Proxy.
5. Dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware).

Minimalny zakres wdrożenia urządzeń

1. Wdrożenie prowadzone w języku polskim,
2. Szczegółowe omówienie polityki bezpieczeństwa stosowanej w jednostce oraz topologii sieci w kontekście możliwości urządzenia,
3. Konsultacja z administratorami sieci zakresu wdrożenia, zastosowanych technik i funkcjonalności,
4. Instalacja i konfiguracja oprogramowania zarządzającego/monitorującego,
5. Aktualizacja oprogramowania wewnętrznego (firmware),
6. Konfiguracja ustawień systemowych,
7. Testowanie wdrożonej konfiguracji oraz zabezpieczenie konfiguracji: kopia zapasowa konfiguracji.

2) Dostawa oprogramowania antywirusowego

Przedmiot zamówienia:

Dostawa, instalacja i konfiguracja programu antywirusowego dla 20 jednostek końcowych z zaawansowanymi funkcjami ochrony i wielowarstwowym podejściem.

Wymagania ogólne:

Program antywirusowy powinien charakteryzować się wielowarstwowym podejściem, które polega na jednoczesnym zastosowaniu wielu technologii ochronnych. Taka strategia pozwala na zapewnienie równowagi pomiędzy wydajnością, skutecznością wykrywania zagrożeń oraz minimalizacją liczby fałszywych alarmów.

Funkcjonalności:

1. **Zabezpieczenie przed złośliwym oprogramowaniem:**
Skuteczna ochrona przed wirusami, trojanami, robakami i innymi rodzajami złośliwego oprogramowania.
2. **Blokowanie ukierunkowanych ataków:**
Wykrywanie i zatrzymywanie ataków typu phishing, spear-phishing oraz innych precyzyjnie ukierunkowanych zagrożeń.
3. **Zapobieganie naruszeniom bezpieczeństwa danych:**
Ochrona przed wyciekiem danych poprzez monitorowanie i kontrolowanie ruchu sieciowego oraz dostępu do danych.
4. **Zatrzymywanie ataków bezplikowych:**
Identyfikacja i blokowanie ataków, które nie pozostawiają tradycyjnych plików złośliwego oprogramowania na dysku twardym.
5. **Wykrywanie zaawansowanych stałych zagrożeń (APT):**
Ochrona przed długotrwałymi i skomplikowanymi atakami na infrastrukturę IT.
6. **Ochrona urządzeń mobilnych i MDM:**
Zabezpieczenie urządzeń mobilnych oraz zarządzanie urządzeniami za pomocą Mobile Device Management (MDM).

Server Security:

Program antywirusowy musi zapewniać zaawansowaną ochronę danych jednostki wymienianych między serwerami różnego przeznaczenia, w tym serwerami sieciowymi, plików i baz danych oraz serwerami wielofunkcyjnymi.

1. **Zapobieganie atakom typu ransomware:**
Ochrona przed szyfrowaniem danych przez złośliwe oprogramowanie typu ransomware.
2. **Wykrywanie zagrożeń zero-day:**

Identyfikacja i neutralizacja nowych, nieznanych wcześniej zagrożeń.

3. **Zapobieganie naruszeniom bezpieczeństwa danych:**

Stała ochrona przed próbami nieautoryzowanego dostępu do danych i wyciekiem danych.

4. **Ochrona przed botnetami:**

Wykrywanie i eliminowanie złośliwego oprogramowania, które umożliwia zdalne kontrolowanie zainfekowanych urządzeń.

Warunki techniczne:

1. Program antywirusowy powinien być kompatybilny z systemami operacyjnymi używanymi w jednostkach końcowych i serwerach (Windows, Linux)
2. Wymagana jest możliwość centralnego zarządzania programem antywirusowym z poziomu konsoli administracyjnej.
3. Program powinien oferować regularne aktualizacje baz sygnatur wirusów oraz mechanizmów ochronnych.

Warunki dostawy:

1. Program antywirusowy powinien być dostarczony w wersji elektronicznej, z licencjami na 2 lata.
2. Wymagana jest pełna dokumentacja użytkownika i administratora w języku polskim.
3. Szkolenie dla administratorów w zakresie instalacji, konfiguracji i zarządzania programem antywirusowym.

Warunki gwarancji i wsparcia technicznego:

1. Dostęp do wsparcia technicznego w języku polskim przez okres trwania licencji.
2. Gwarancja na nieprzerwane działanie programu antywirusowego przez cały okres licencji.
3. Wsparcie techniczne dostępne w trybie 24/7.