Wymagania ogólne dotyczące przedmiotu zamówienia.

1. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów.
2. Zamawiający dopuszcza realizację poszczególnych grup funkcjonalnych urządzeń przez zespoły urządzeń pod następującymi warunkami:

- połączenie urządzeń będzie zrealizowane w sposób nie ograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),
- zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,
- wszystkie elementy kompletu będą spełniały wymagania związane z zarządzaniem,

3. Dostarczone urządzenia muszą współpracować z posiadanym przez Zamawiającego systemem zarządzania Cisco Works LMS.

Wymagania szczegółowe dotyczące dostarczanego sprzętu

Przedmiotem zamówienia jest dostawa urządzeń oraz usługa:
1. Urządzenie zabezpieczające Typ A – sztuk 1.
2. Urządzenie zabezpieczające Typ B – sztuk 1.
3. Przełącznik dostępowy – sztuk 11.
4. Moduł rozbudowy przełącznika sieciowego Cisco WS-C6509-E 24-port typ A – sztuk 3.
5. Moduł rozbudowy przełącznika sieciowego Cisco WS-C6509-E 48-port typ B – sztuk 2.
6. Moduł światłowodowy – sztuk 17.
7. Kable optyczne – sztuk 50.
8. Licencja użytkowników VPN dla urządzenia zabezpieczającego Typ A – sztuk 1.
9. Zasilacz redundantny dla urządzenia zabezpieczającego Typ A- sztuk 1.
10. Instruktaż uruchomieniowy i użytkowy dostarczonych urządzeń sieciowych.

Wszystkie urządzenia muszą być zgodne z wymaganiami minimalnymi zamieszczonymi poniżej.

Specyfikacja techniczna przedmiotu zamówienia – minimalne wymagania techniczne i funkcjonalne:

<u>Urządzenie zabezpieczające Typ A</u>

- Urządzenie modularne pozwalające na uzyskanie funkcji firewall, VPN (sprzętowe wsparcie szyfrowania), IPS
- Typ i liczba portów – co najmniej 16 interfejsów GE 10/100/1000 i co najmniej dwa interfejsy 10/100/1000 dla zarządzania poza pasmowego (OOB)
- Wydajność:
  - co najmniej 4 Gbps ruchu poddawanego inspekcji przez mechanizmy ściany ogniowej
  - co najmniej 1 Gbps ruchu szyfrowanego
  - Obsługa min. 5.000 tuneli IPSec VPN
  - Obsługa min. 5.000 tuneli SSL VPN (w trybie client lub clientless) - Zamawiający wymaga w momencie dostawy dostarczenia licencji na minimum 2 tunele SSL VPN i wymaga, aby urządzenie miało możliwość uruchomienia funkcji z docelową liczbą tuneli w przyszłości bez konieczności jego modernizacji/rozbudowy sprzętowej
  - obsługa co najmniej 1.000.000 jednoczesnych sesji/połączeń z prędkością 50.000 nowych połączeń na sekundę
  - obsługa min. 2 wirtualnych instancji firewall z możliwością rozbudowy do stu instancji
  - obsługa min. 1000 sieci logicznych VLAN
- Co najmniej 2 porty USB (tokeny, certyfikaty etc.)
- Ściana ogniowa śledząca stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji bez ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
- Dostarczone wraz z dedykowanym oprogramowaniem klienta VPN (IPSec i SSL). Oprogramowanie musi mieć możliwość instalacji na stacjach roboczych PC pracujących pod kontrolą systemów operacyjnych Windows, Linux, a także komputerach Mac. Oprogramowanie musi umożliwiać zestawienie do urządzenia

stanowiącego przedmiot postępowania połączeń VPN z osobistych stacji roboczych PC. Oprogramowanie musi być zgodne z oferowanym urządzeniem zabezpieczającym.

- Możliwość pracy jako transparentna ściana ogniowa warstwy drugiej ISO OSI (dla IPv4 i IPv6)

- Możliwość routingu pakietów zgodnie z protokołami RIP, OSPF

- Urządzenie musi zapewniać obsługę ruchu multicast, w tym wsparcie dla protokołów PIM i IGMP oraz definiowanie list kontroli dostępu dla ruchu multicast

- Urządzenie musi posiadać możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się z usługą katalogową Microsoft Active Directory

- Urządzenie musi zapewniać współpracę z serwerami certyfikatów (CA)

- Urządzenie musi zapewniać obsługę protokołów IKE i IKEv2

- Urządzenie musi zapewniać mechanizmy inspekcji aplikacyjnej i kontroli następujących usług: http, FTP, SMTP, DNS, SIP, H.323, LDAP, ICMP, NFS

- Urządzenie musi zapewniać poprawną pracę w sieci z adresacją IPv6 oraz umożliwiać obsługę list ACL dla IPv6

- Inspekcja ruchu IPv6 z wykorzystaniem nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload

- Mechanizmy redundancji, w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w modelu active/standby oraz active/active

- Mechanizmy kolejkowania ruchu z obsługą kolejki absolutnego priorytetu i możliwością kształtowania (shaping) ruchu

- Współpraca z serwerami autoryzacji (RADIUS, TACACS+ lub równoważny) w zakresie przesyłania list kontroli dostępu z serwera do urządzenia z granulacją per użytkownik, o wielkości przekraczającej 4KB

- Zarządzanie i konfiguracja:

    - możliwość eksportu informacji przez syslog

    - możliwość eksportu informacji o przekazywanym ruchu w oparciu o NetFlow

lub równoważny protokół (sFlow, JFlow itp.)

- możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołu RADIUS, TACACS+ lub równoważnego, LDAP

- konfigurowalne przez CLI oraz interfejs graficzny (oczekiwane są narzędzia dodatkowe
w postaci kreatorów połączeń, etc.)

- dostęp do urządzenia przez SSHv2, HTTPS (w tym również w sieci IPv6)

- obsługa SNMPv3

- obsługa funkcji SCP

- możliwość eksportu konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline

- Funkcjonalność IPS:

  - praca w trybach in-line oraz promiscous

  - identyfikacja, klasyfikacja i powstrzymywanie ruchu zagrażającego bezpieczeństwu organizacji w tym: robaki sieciowe, adware, wirusy sieciowe, nadużycia aplikacyjne

  - wykrywanie i powstrzymywanie działań wskazujących na przekroczenie polityk bezpieczeństwa w tym: działania z wykorzystaniem komunikatorów internetowych, działania z wykorzystaniem aplikacji peer-to-peer, filtracja w oparciu o typy MIME

  - wykrywanie robaków sieciowych oraz wirusów sieciowych w szczególności z wykorzystaniem analizy anomalii ruchu w monitorowanych segmentach sieci

  - monitoring ruchu IPv6

  - analiza kontekstowa – wykrywanie ataków ukryte w wielu następujących po sobie pakietach

  - wykrywanie anomalii związanych z ruchem w monitorowanym segmencie sieci

  - wykrywanie anomalii związanych z protokołami (w szczególności odstępstw

od normalnych zachowań zdefiniowanych przez odpowiednie dokumenty RFC)

- wykrywanie ataków związanych z działaniami w warstwie 2. modelu OSI w szczególności ataków na ARP oraz ataków Man-in-the-middle w środowisku przełączanym
- mechanizmy zapobiegające „omijaniu" systemów IPS w szczególności:
    - normalizacji ruchu
    - scalania strumieni TCP
    - deobfuscation
    - scalające (defragmentujące) dla pakietów IP
- mechanizmy dla OS Fingerprinting – identyfikacji systemu operacyjnego hosta dla celów przyszłej oceny znaczenia ataku
- definiowanie kryteriów oceny znaczenia ataku w oparciu o co najmniej następujące parametry:
    - ważność zdarzenia (potencjalne zagrożenie jeżeli ruch zostanie dopuszczony – nie będzie filtrowany)
    - wartość zasobu (określenie krytyczności atakowanego urządzenia dla organizacji)
    - potencjalna skuteczność ataku (wstępne określenie czy atak mógł być skuteczny)
- wskazanie limitów na pasmo dla określonych aplikacji celem zapobiegania wykorzystaniu całego pasma przez atakującego
- wydajność na poziomie 2 Gbps dla ruchu poddawanego inspecji IPS

- Pamięć DRAM oraz flash wystarczająca do zapewnienia powyższej funkcjonalności i przechowywania obrazów systemu operacyjnego (nie jest dopuszczalna konieczność rozbudowy pamięci przy zwiększaniu funkcjonalności urządzenia)
- Możliwość montażu w szafie rack 19". Wysokość nie większa niż 2RU
- Redundantne zasilacze 230V AC

Urządzenie zabezpieczające Typ B

- Firewall statefull inspection zapewniający wydajność min. 2Gb/s dla ruchu IPv4 i IPv6
- Możliwość rozbudowy urządzenia o funkcjonalność systemu IPS. W przypadku jednocześnie uruchomionych usług firewall'a i systemu IPS urządzenie musi zapewniać wydajność nie mniejszą niż 600Mb/s
- Funkcjonalność bramy dla połączeń VPN:
  - Wydajność szyfrowania min. 300Mbps dla algorytmów 3DES/AES
  - Obsługa min. 750 tuneli IPSec VPN
  - Obsługa min. 750 tuneli SSL VPN (w trybie client lub clientless) - Zamawiający wymaga w momencie dostawy dostarczenia licencji na minimum 2 tunele SSL VPN i wymaga, aby urządzenie miało możliwość uruchomienia funkcji z docelową liczbą tuneli w przyszłości bez konieczności jego modernizacji/rozbudowy sprzętowej
- Typ i liczba portów - co najmniej 8 portów Gigabit Ethernet 10/100/1000 Base-T z możliwością rozbudowy o kolejne 6 portów Gigabit Ethernet (SFP lub 10/100/1000 Base-T)
- Urządzenie musi zapewniać obsługę co najmniej 500.000 połączeń oraz umożliwiać zestawianie co najmniej 20.000 nowych połączeń na sekundę
- Obsługa ramek jumbo o wielkości minimum 9216 bajtów
- Obsługa minimum 200 sieci VLAN
- Urządzenie musi umożliwiać grupowanie VLANów w trybie pracy jako transparent firewall
- Rozwiązanie musi być oparte o dedykowany system operacyjny. Nie dopuszcza się rozwiązań, gdzie platformą systemową jest system operacyjny ogólnego zastosowania, a na nim instalowane oprogramowanie firewall jako aplikacja
- Urządzenie musi mieć możliwość pracy w trybie L3 (routed mode) i L2 (transparent mode)
- Urządzenie nie może posiadać licencyjnych ograniczeń w zakresie liczby pracujących użytkowników w sieci chronionej

• Urządzenie musi posiadać możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się z usługą katalogową Microsoft Active Directory

• Urządzenie musi zapewniać mechanizmy inspekcji aplikacyjnej i kontroli następujących usług: http, FTP, SMTP, DNS, SIP, H.323, LDAP, ICMP, NFS

• Urządzenie musi zapewniać obsługę routingu dynamicznego – co najmniej RIPv2 i OSPF

• Urządzenie musi zapewniać obsługę ruchu multicast w tym wsparcie dla protokołów PIM i IGMP oraz definiowanie list kontroli dostępu dla ruchu multicast

• Urządzenie musi zapewniać współpracę z serwerami certyfikatów (CA)

• Urządzenie musi zapewniać obsługę protokołów IKE i IKEv2

• Wymagane jest wsparcie dla funkcji Secure Hash Algorithm SHA-2 o długości 256, 384 i 512 bitów dla połączeń IPSec z IKEv2 - dla dostępu zdalnego w oparciu o klienta VPN

• Urządzenie musi zapewniać poprawną pracę w sieci z adresacją IPv6 oraz umożliwiać obsługę list ACL dla IPv6

• Inspekcja ruchu IPv6 z wykorzystaniem nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload

• Urządzenie musi pozwalać na wirtualizację konfiguracji poprzez wirtualne firewalle/konteksty. Wymagana jest obsługa co najmniej 2 wirtualnych kontekstów z możliwością rozszerzenia ilości obsługiwanych wirtualnych kontekstów do co najmniej 20

• Urządzenie musi pozwalać na realizację modelu wdrożenia w wysokiej dostępności dla IPv4 i Ipv6 w trybach active-standby i active-active (z możliwością obsługi ruchu asymetrycznego w modelu active-active)

• Urządzenie musi zapewniać dostęp administracyjny do interfejsu zarządzania w oparciu o role (RBAC)

• Dedykowany port konsoli oraz dedykowany interfejs zarządzający GigabitEthernet dla zarządzania Out-of-band

• Minimum 2 porty USB

- Urządzenie musi posiadać możliwość eksportu konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline

- Wraz z urządzeniem należy dostarczyć graficzną aplikację zapewniającą przyjazną konfigurację z wykorzystaniem w tym kreatorów konfiguracji dla najważniejszych funkcji
- Rozwiązanie musi posiadać możliwość współpracy z zewnętrznymi serwerami uwierzytelnienia i autoryzacji co najmniej z wykorzystaniem protokołu RADIUS
- Zarządzanie urządzeniem poprzez SSHv2, HTTPS (w tym również w sieci IPv6)
- Możliwość montażu w szafie rack 19". Wysokość nie większa niż 2RU

Urządzenia zabezpieczające Typ A i B muszą być zgodne pod względem połączeń VPN.

Przełącznik dostępowy

- Min. 24 porty Gigabit Ethernet 10/100/1000 Base-T (Auto-MDIX)
- Min. 4 dodatkowe porty GE ze stykiem definiowanym przez SFP
- Pamięć DRAM oraz flash wystarczająca do poprawnego działania urządzenia i przechowywania obrazów systemu operacyjnego (nie jest dopuszczalna konieczność rozbudowy pamięci przy zwiększaniu funkcjonalności urządzenia)
- Szybkość przełączania minimum 41,7 Mpps dla pakietów 64-bajtowych (wire-speed)
- Możliwość stackowania – nie jest wymagane w momencie dostawy, niemniej przełącznik musi umożliwiać rozbudowę (np. dodatkowy moduł itp.) o taką funkcjonalność przy zachowaniu następujących funkcjonalności:
    - Zarządzanie poprzez jeden adres IP
    - Przepustowość w ramach stosu min. 20Gb/s
    - Możliwość połączenia min. 4 przełączników w ramach stosu
    - Możliwość tworzenia połączeń cross-stack link aggregation w oparciu

o 802.3ad

- Przełącznik musi posiadać możliwości łączenia wg standardu 802.3at.

- Wbudowane reflektometry (TDR) na wszystkich portach 10/100/1000
- Obsługa 8.000 adresów MAC i 250 sieci VLAN 802.1q
- Możliwość uruchomienia centralnej definicji sieci VLAN i propagacji bazy na inne przełączniki w domenie administracyjnej (kompatybilny z pozostałymi przełącznikami)
- Obsługa protokołów:
    - IEEE 802.1w Rapid Spanning Tree
    - IEEE 802.1s Multi-Instance Spanning Tree
    - min. 128 instancji protokołu STP
- Obsługa ramek jumbo (9000B) na wszystkich portach
- Obsługa IGMPv3 i MLDv1/2 Snooping
- Routing statyczny IPv4 – min. 16 tras
- Parametry QoS:
    - Możliwość automatycznego wykrycia terminala głosowego IP dołączonego do portu przełącznika
    - Implementacja co najmniej czterech kolejek sprzętowych dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
    - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (StrictPriority)
    - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
    - Obsługa policing-u (rate limiting)
    - Możliwość definicji makr konfiguracyjnych dla portów (określenie listy poleceń konfiguracyjnych aplikowanych za pomocą pojedynczej komendy)
- Funkcje bezpieczeństwa:

- Co najmniej dwa poziomy dostępu administracyjnego poprzez konsolę
- Autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL
- Obsługa funkcji Guest VLAN
- Voice VLAN
- Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
- Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X (bez konieczności stosowania zewnętrznego serwera www)
- Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie
- Obsługa funkcji bezpieczeństwa sieci LAN: Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
- Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+
- Obsługa list kontroli dostępu (ACL)

- Możliwość synchronizacji czasu ze źródłem zewnętrznym zgodnie z NTP
- Obsługa protokołu LLDP i LLDP-MED
- Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
- Wbudowany serwer DHCP
- Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN)
- Dedykowany port Ethernet do zarządzania out-of-band
- Minimum 1 port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia nośnika danych umieszczonego w porcie USB

- Parametry fizyczne:
    - Obudowa rack-mount 19”
    - Wysokość 1RU
    - Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego lub dołączenia zewnętrznego systemu RPS
- Możliwość kopiowania konfiguracji do pliku tekstowego (przez FTP, SCP lub równoważny)
- Zarządzanie przez konsolę szeregową, SSHv2, SNMPv3, RMON, HTTPS, SCP (przez Ipv i IPv6)

Moduł rozbudowy przełącznika sieciowego będącego na wyposażeniu Zamawiającego Cisco WS-C6509-E TYP A

- Minimum 24-porty Gigabit Ethernet SFP
    - Podłączenie do matrycy przełączającej o szybkości minimum 20Gb/s
- Możliwość rozbudowy modułu o kartę przetwarzania rozproszonego
- QoS - obsługa minimum 4 kolejek sprzętowych per port (w tym 1 kolejka z bezwzględnym priorytetem)

Moduł rozbudowy przełącznika sieciowego będącego na wyposażeniu Zamawiającego Cisco WS-C6509-E TYP B

- 48 portów 10Base-T/100Base-TX/1000Base-T – RJ-45 (Auto-MDIX)
    - Podłączenie do matrycy przełączającej o szybkości minimum 40Gb/s
- Możliwość rozbudowy modułu o kartę przetwarzania rozproszonego
- QoS - obsługa minimum 4 kolejek sprzętowych per port (w tym 1 kolejka z bezwzględnym priorytetem)

Moduł światłowodowy

- standard złącza SFP (mini-GBIC)
- wydajność 1Gbps full duplex.
- praca full duplex na jednym włóknie jednomodowym do 20 km
- zapewniona współpraca ze wszystkimi dostarczonymi w tym zadaniu urządzeniami posiadającymi porty SFP

Kable optyczne

- 50 szt. patchcordów optycznych LC-SC

Instruktaż uruchomieniowy i użytkowy dostarczonych urządzeń sieciowych

Autoryzowany (przez producenta oferowanego rozwiązania) instruktaż dla **dwóch osób** przygotowujący do administracji i obsługi dostarczonymi rozwiązaniami firewall przeprowadzony i zakończony stosownym certyfikatem z zakresem obejmującym:

- Omówienie cech funkcjonalnych i zasad licencjonowania
- Wdrożenie podstawowej konfiguracji i zarządzania firewall'ami; diagnozowanie problemów
- Konfigurowanie funkcjonalności typu NAT
- Konfigurowanie list ACL
- Konfigurowanie routingu statycznego, dynamicznego i wsparcia dla multicastów
- Konfigurowanie firewall'a do pracy w trybie transparentnym
- Wdrożenie funkcjonalności kontroli dostępu za pomocą oferowanego firewall'a (inspekcja stanu połączeń, wdrożenie polityki inspekcji na poziomie aplikacji)
- Wdrożenie funkcjonalności wirtualizacji i wysokiej dostępności (wirtualne firewalle, redundantne interfejsy, rozwiązanie typy ether-channel, redundancja typu active/standy i typu active/active)
- Omówienie różnych typów połączeń VPN dostępnych na urządzeniu
- Konfigurowanie połączeń typu Clientless VPN
- Konfigurowanie pełnego dostępu do sieci z wykorzystaniem klienta SSL VPN
- Konfigurowanie połączeń IPSec VPN site-to-site i remote-access
- Wykorzystanie cech wysokiej dostępności w ramach połączeń VPN

Wymagany czas trwania instruktażu co najmniej 5 dni (5 x 8 godzin)

W czasie przeprowadzonego instruktażu Wykonawca powinien zapewnić dostęp do laboratorium ze sprzętem, na którym będą testowane konfiguracje i mechanizmy sieciowe.

W przypadku prowadzenia instruktażu w miejscowości innej niż Lublin, Wykonawca musi pokryć koszty związane z dojazdem, zakwaterowaniem i wyżywieniem osób w nich uczestniczących.

Instruktaż musi być prowadzony w języku polskim – dopuszcza się wykorzystanie instrukcji obsługi opracowanych w języku angielskim.