Zał. Nr 2 do umowy …..

# Zestawienie sprzętu w węzłach centralnych sieci „E- Leader” dla potrzeb budowy punktów styku

**Lokalizacja 1**: GOK Moszczenica

Router ASR1002-5G-HA/K9 + 901-3050-XX00
Firewall PaloAlto 3020

**Lokalizacja 2**: Urząd Gminy Ujazd

Router ASR1002-5G-HA/K9 + 901-3050-XX00
Firewall PaloAlto 3020

Firewall-e pracują w trybie klastra Active<->Active

**Lokalizacja 3:** MTI Moszczenica

Stos dwóch przełączników DCN CS6510-48S6Q-HI

Przełącznik 40G Advance Enhanced Datacenter (48 * 10GbE (SFP +) + 6 * 40GbE (QSFP +)), redundantna i modułowa konstrukcja, wysoka wydajność. Pełne funkcje L3, Domyślnie z dwoma zasilaczami AC z możliwością wymiany podczas pracy, Domyślnie z 5 (4 + 1) wentylatorami, chipsetem Broadcom

Firewall PaloAlto PA-820

**Część aktywna sieci:**

W celu zapewnienia bezawaryjnego dostępu do sieci Internet dla potencjalnych inwestorów zgodnie ze sztuką inżynierską zapewnić należy pełną redundancję urządzeń aktywnych.

**Urządzeniem brzegowym będzie klaster routerów z funkcjonalnością firewall (zbudowany z dwóch redundantnych urządzeń ) z wkładkami, dostarczony, zamontowany i wdrożony o** następujących parametrach:

- Urządzenie 1RU o architekturze zabudowanej, wyposażone w 8 portów Gigabit Ethernet przeznaczone dla modułow optycznych typu SFP lub równoważnych, a także w 8 portów 10 Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP+ lub równoważnych. W chwili dostarczenia urządzenia zamawiający wymaga odblokowanych co najmniej 6 portów 1 Gigabit Ethernet oraz 6 portów 10 Gigabit Ethernet.
- Domyślnie urządzenie posiada zasoby sprzętowe pozwalające przełączać minimalnie 30 Mpps oraz 60 Gbps ruchu
- Urządzenie powinno mieć możliwość zrealizowania szyfrowanie IPsec oraz może być wyposażone w dedykowany, sprzętowy akcelerator kryptograficzny osiągający wydajność 8 Gbps dla ruchu IMIX z możliwością licencyjnego podniesienia wydajności do 16Gbps.

- Urządzenie obsługuje szyfrowanie z algorytmem AES-256 zgodnie ze standardem 802.1AE na wszystkich zabudowanych portach 1 Gigabit Ethernet oraz 10 Gigabit Ethernet z prędkością linerate, jeśli odblokowanie funkcjonalności wymaga licencji powinna ona zostać uwzględniona przynajmniej dla 2 portów 10 Gigabit Ethernet.
- Urządzenie posiada 8 GB pamięci RAM z możliwością rozbudowy do 16 GB. W chwili dostarczenia zamawiający wymaga 8 GB RAM.
- Urządzenie obsługuje 1 000 000 prefiksów w tablicach rutingu dla IPv4.
- Urządzenie obsługuje 1 000 000 prefiksów w tablicach rutingu dla IPv6.
- Urządzenie obsługuje 64 000 tras multicast.
- Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv4: OSPF, ISIS, BGP.
- Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv6: OSPFv3, ISIS, BGP.
- Urządzenie obsługuje Policy Based Routing, w tym także routing oparty o pomiar parametrów łącza (opóźnienie, obciążenie, jitter) z możliwością definiowania polityk per aplikacja.
- Urządzenie umożliwia uruchomienie wydzielonych wirtualnych instancji (przestrzeni) routingowych w oparciu o mechanizm VRF (Virtual Routingu Forwarding), umożliwiając m.in. wykreowanie wydzielonej logicznej sieci na potrzebę obsługi ruchu określonej aplikacji lub wydzielonego fragmentu sieci.
- Urządzenie obsługuje co najmniej 7000 instancji wirtualnych tablic routingu.
- Urządzenie obsługuje funkcjonalność Bidirectional Forwarding Detection (BFD), zapewniając przy tym wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego.
- Urządzenie obsługuje funkcjonalność BFD dla interfejsów skonfigurowanych do współpracy z VRF.
- Urządzenie obsługuje multicast, w szczególności: PIM sparse/dense/SSM, IGMP, MLD, Multicast VPN.
- Urządzenie obsługuje protokół NHRP (ang. Next Hop Resolution Protocol).
- Urządzenie obsługuje protokół GDOI (RFC 3547).
- Funkcjonalności związane z niezawodnością pracy:
  - system modularny umożliwiający aktualizację poszczególnych modułów programowych niezależnie od siebie
  - redundancja procesów rutingowych realizowana poprzez uruchomienie dwóch kopii systemu operacyjnego
  - BFD dla OSPF, BGP, ISIS
  - IP FRR
  - BGP Prefix-Independent Convergence (PIC)
  - Graceful Restart dla OSPF, BGP, ISIS, LDP, RSVP
  - funkcjonalność VRRP
  - redundantne zasilacze 230V
  - możliwość wymiany modułów w trakcie pracy (ang. hot swap)
- Urządzenie obsługuje MPLS, w szczególności:
  - TE
  - MPLS LDP
  - EoMPLS, VPLS
  - MPLS L3 VPN

- MPLS FRR w trybach protekcji łącza oraz węzła

– Urządzenie obsługuje następujące mechanizmy jakości usług (QoS):
  - klasyfikacja, kolejkowanie, oznaczanie, policing, shaping per port/VLAN zarówno dla IPv4 jak i IPv6
  - hierarchiczny QoS (H-QoS) - 3 poziomy
  - klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: adres MAC, adres IP, port TCP, VLAN ID, MPLS EXP, 802.1p (CoS), IP ToS/DSCP.
  - dynamiczna alokacja kolejek sprzętowych, dostępne min. 100 000 kolejek
  - algorytm Round Robin (Shaped Round Robin) dla obsługi kolejek
  - możliwość obsługi jednej kolejki z priorytetem w stosunku do innych
  - mechanizm ograniczania ilości ruchu w kolejce priorytetowej
  - możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
  - możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi (ingress policing, rate limiting)
  - mechanizm WRED
  - możliwość wykorzystania rodzajów aplikacji/ruchu aplikacyjnego w tworzeniu polityk QoS

– Urządzenie obsługuje następujące funkcje i elementy bezpieczeństwa:
  - sprzętowa ochrona warstwy zarządzającej (Control Plane Policing), ze wsparciem dla list kontroli dostępu
  - Unicast RPF (Reverse Path Forwarding)
  - listy kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL
  - musi istnieć możliwość wprowadzenia 60 000 wpisów IPv4 na wszystkich listach kontroli dostępu (ACL), a także 4 000 list kontroli dostępu (ACL)
  - dostęp administracyjny oparty o role z przypisanymi uprawnieniami
  - urządzenie ma realizować funkcjonalności zapory ogniowej typu statefull (ang. statefull firewall) z wydajnością nie mniejszą niż 50Gbps, przy czym zapora ogniowa:
  - umożliwia definicję stref bezpieczeństwa (zone-based firewall) z elastyczną definicją scenariuszy przesyłu ruchu pomiędzy różnymi strefami (inspekcja ruchu, odrzucanie ruchu, brak inspekcji)
  - obsługuje ruch IPv4 oraz IPv6
  - umożliwia konfigurację polityk per wirtualna tablica routingu (VRF)
  - umożliwia obsługę 2 000 000 równoczesnych sesji
  - umożliwia zestawianie 200 000 nowych połączeń HTTP na sekundę
  - zasoby sprzętowe realizujące funkcjonalności szyfrowania VPN z wydajnością 19 Gbps (AES256) z obsługą 8 000 tuneli IPSec
  - sieci VPN typu site-2-site oparte o IPSec
  - dynamiczne zestawianie VPN z wykorzystaniem protokołu NHRP w relacji spoke to spoke w celu optymalizacji transmsji danych pomiędzy lokalizacjami
  - bez-tunelowe sieci VPN w relacji każdy z każdym w celu zapewnienia optymalnej transmisji pomiędzy dowolnymi węzłami oraz optymalnej realizacji polityk jakości usług (QoS) i transmisji multicast

- algorytmy IPSec następnej generacji oparte o krzywe eliptyczne (RFC 4869), w szczególności:
- Elliptic Curve Diffie-Hellman (ECDH)
- Galois Counter Mode Advanced Encryption Standard (GCM-AES) - 128/256 bitów
- Galois Message Authentication Code (GMAC-AES) - 128/256 bitów
- Elliptic Curve Digital Signature Algorithm (ECDSA) dla IKEv2
- konfiguracja tuneli IPSec VPN w oparciu o protokół IKEv2
- IKEv2 zarówno dla VPN typu site-2-site jak i dynamicznych
- IKEv2 zarówno dla ruchu IPv4 jak i IPv6
- funkcjonalność VPN per VRF
- ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU
- logowanie pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU
- możliwość uruchomienia funkcjonalności analizy i klasyfikacji pakietów w warstwie 2-7 polegającej na przeszukiwaniu pakietów pod kątem zawierania specyficznych ciągów znaków i wykrywania na tej podstawie ataków

- Urządzenie w chwili dostarczenia ma wspierać usługi klasyfikacji ruchu w oparciu o głęboką analizę pakietów, przy czym klasyfikacja ta:
  - opiera się na kilku mechanizmach gwarantujących poprawne rozpoznawanie wielu aplikacji / protokołów. Wykonawca wraz z urządzeniem dostarczy ich listę.
  - udostępnia 3 atrybuty opisujące daną aplikację / protokół (atrybuty ułatwiają konfigurowanie QoS na urządzeniu poprzez grupowanie podobnych aplikacji / protokołów - na przykład wszystkie aplikacje typu p2p mają taką samą wartość atrybutu określającego typ aplikacji).
  - nie wymaga rozbudowy sprzętowej urządzenia, jedynie zakup licencji
- Urządzenie obsługuje 4000 tuneli GRE.
- Urządzenie posiada możliwość tunelowania przesyłanych danych w postaci tuneli GRE typu punkt-punkt oraz punkt-wielopunkt z możliwością uruchomienia protokołów routingu dynamicznego pomiędzy urządzeniami połączonymi za pomocą tuneli GRE.
- Urządzenie umożliwia ochronę kryptograficzną tuneli GRE.
- W ramach funkcjonalności zarządzania, urządzenie:
  - umożliwia zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3
  - obsługuje Ethernet OAM (IEEE 802.3ah, IEEE 802.1ag, ITU-T Y.1731)
  - obsługuje MPLS OAM
  - umożliwia pisanie skryptów konfiguracyjnych
  - obsługuje protokół Netflow ze wsparciem dla multicast oraz IPv4/IPv6
  - posiada narzędzia IP SLA umożliwiające pomiar parametrów jakościowych łącza (np. czas odpowiedzi aplikacji/serwera, opóźnienie, jitter, straty pakietów) i dostęp do tych informacji za pomocą SNMP
  - posiada obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+
  - posiada dedykowane porty do zarządzania urządzeniem: port konsoli (RJ45), port Ethernet 10/100/1000 oraz port AUX
  - posiada dwa porty USB

- posiada możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej
- konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona
- urządzenie posiada możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów

- Urządzenie posiada redundante zasilacze AC 230V zintegrowane w obudowie urządzenia.
- Urządzenie umożliwia montaż w szafie 19”.
- Licencje dostarczone wraz z urządzeniem nie mogą być przypisanego do niego na stałe.
- Zamawiający wymaga dostarczenia wraz z urządzeniem licencji do systemu zarządzania będącego w posiadaniu Zamawiającego – System Center Configuration Manager.