Opis Przedmiotu Zamówienia
na dostawę routerów

I. Wymagania ogólne

1. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na rynek europejski.
2. Całość dostarczanego sprzętu musi być fabrycznie nowa (nie używana w innych środowiskach).
3. Urządzenia nie mogą być używane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
4. Całość dostarczanego sprzętu musi być dostępna w obecnej ofercie produktowej producenta oraz nie może być przeznaczona do wycofania z produkcji, sprzedaży bądź wsparcia (end-of-life, end-of-sale, end-of-support).
5. Wszystkie dostarczane urządzenia i pakiety oprogramowania były sprawdzone w praktyce rynkowej. Oznacza to, iż oprogramowanie systemowe (firmware urządzeń) realizujące wszystkie wymagane funkcje, jak też samo urządzenie musi być objęte pełnym serwisem producenta (niedopuszczalne jest proponowanie oprogramowanie np. w wersji Beta)
6. Sprzęt musi zostać dostarczony z najnowszą wersją oprogramowania systemowego (firmware) lub z wersją oprogramowania rekomendowaną przez producenta oferowanego rozwiązania. Jeżeli urządzenia są fabrycznie wysyłane z inną wersją oprogramowania to Wykonawca zobowiązany jest do dostarczenia wersji najnowszej lub wersji rekomendowanej przez producenta (na nośniku, poprzez wskazanie jej lokalizacji w portalu producenta z możliwością jej pobrania, lub też poprzez pobranie jej bezpośrednio na urządzenie itp.)
7. Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, żeby była możliwa identyfikacja zarówno produktu jak i producenta.
8. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych producenta.
9. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej (dopuszczalne jest dostarczenie dokumentacji w języku angielskim).
10. Wszystkie urządzenia muszą posiadać Certyfikat CE produktu.
11. System musi być objęty minimum 36 miesięczną gwarancją przez centrum serwisowe W ramach gwarancji, muszą być serwisowane wszystkie elementy sprzętu, zapewniony dostęp do baz wiedzy producenta, aktualizacji oprogramowania oraz nieograniczony dostęp do TAC (Technical Assistance Center). W ramach gwarancji muszą być również dostępne wszystkie licencje/subskrypcje na okres minimum 36 miesięcy zapewniające opisane wyżej funkcjonalności.

II. Wdrożenie

1. Zamawiający wymaga zapewnienia certyfikowanych inżynierów [1] na czas wdrożenia. W ramach wdrożenia całość zostanie zintegrowana z siecią Zamawiającego.
2. W ramach wdrożenia, inżynierowie zainstalują zaoferowane urządzenia w wyznaczonym przez Zamawiającego miejscu, podłączą do sieci zamawiającego oraz dostosują i przeniosą konfigurację z posiadanych przez Zamawiającego routerów Cisco ISR4331.
3. Inżynierowie muszą posiadać odpowiednią wiedzę i doświadczenie – minimum dwóch inżynierów z certyfikatami producenta dostarczanego rozwiązania.
4. Wszyscy inżynierowie muszą się biegle porozumiewać w języku polskim w mowie i piśmie.
5. Wykonawca w ramach wdrożenia przeszkoli trzech pracowników Zamawiającego z zaoferowanego rozwiązania

III. Specyfikacja routera – Dwa urządzenia

1. Urządzenie musi być dostarczone jako dedykowane urządzenie typu appliance. Musi być przystosowane do montażu w szafie 19”, obudowa wykonana z metalu. Wraz z urządzeniem musi być dostarczy zestaw montażowy rack tj. wszystkie niezbędne elementy konieczne do ich montażu w Lokalizacjach Zamawiającego, w szczególności: śrubki, nakrętki koszykowe, szyny montażowe, itp.
2. Musi być wyposażone w dwa zasilacze typu AC, przystosowany do zasilania prądem naprzemiennym 230V, pracujące redundantnie. Wykonawca musi dostarczyć kable zasilające zakończone wtykiem IEC C14.
3. Musi posiadać co najmniej 4 interfejsów 1GE RJ45 oraz co najmniej 2 interfejsy 1GE / 10GE SFP+. Należy dostarczyć minimum 2 wkładek 10GE SR wraz z urządzeniem.
4. Musi pozwalać na rozszerzenie o co najmniej 2 moduły z dodatkowymi portami 10GE, wspierającymi standard szyfrowania MACSec. W przypadku braku możliwości rozszerzenia o takie moduły, urządzenie musi mieć wbudowane 4 interfejsy 1GE RJ-45 i 4 interfejsy 10GE SFP+.
5. Urządzenie musi umożliwiać rozszerzenie o moduł łączności poprzez sieć komórkową przynajmniej w standardzie LTE kategorii 6.
6. Musi być wyposażone w co najmniej 8 GB pamięci RAM.
7. Musi umożliwiać na rozbudowę pamięci RAM do co najmniej 32GB RAM.
8. Musi być wyposażone w pamięć o pojemności co najmniej 16 GB do przechowywania obrazów systemu operacyjnego, konfiguracji oraz logów systemowych.
9. Musi obsługiwać co najmniej 1 500 000 prefiksów w tablicach routingu IPv4/IPv6 i umożliwiać na rozbudowę przez odpowiednie moduły – do co najmniej 2 500 000 prefiksów IPv4/IPv6.
10. Musi oferować sumaryczną wydajność dla pakietów 1400B na poziomie przynajmniej 18Gbps dla ruchu IPv4;
11. Musi oferować sumaryczną wydajność dla pakietów szyfrowanych 1400B na poziomie przynajmniej 8Gbps dla ruchu IPv4;

[1] Opis warunków które musi spełnić certyfikat producenta zaoferowanego rozwiązania znajduje się w pkt IV „Warunki równoważności”

12. Musi obsługiwać routing dynamiczny co najmniej: RIP, OSPF, ISIS, EIGRP, BGP dla IPv4 i IPv6;
13. Musi obsługiwać protokoły i funkcjonalności sieciowe co najmniej: 802.1q, VRRP, Serwer DHCP, SSHv2, SNMP v2c i v3, NTP z uwierzytelnieniem, Syslog.
14. Musi być w stanie obsłużyć co najmniej 4000 instancji VRF (Virtual Route Forwarding);
15. Musi posiadać ochronę warstwy zarządzającej (Control Plane Policing);
16. Music obsługiwać co najmniej 4000 ACL (Access Control Lists) z 40 000 wpisów ACE (Access Control Entries);
17. Musi wspierać multicast w szczególności: PIM sparse/SSM/Bi-directional, IGMP, MLDv2;
18. Musi obsługiwać RPF (Reverse Path Forwarding);
19. Musi obsługiwać zarzadzanie ruchem (QoS):
    a. minimum 16000 kolejek per system;
    b. hierarchiczne polityki QoS;
    c. minimum 3 poziomy hierarchii;
    d. minimum dwie kolejki priorytetowe LLQ per polityka.
    e. obsługa kształtowania (shaping), ograniczania (policing) ruchu, gwarancje pasma
    f. kolejkowanie z kolejką priorytetową i model WFQ (Weighted Fair Queuing) dla pozostałych klas ruchu
    g. mechanizm tail-drop i RED (Random Early Detect);
    h. oznaczanie i zmiana oznaczeń DSCP na bazie przekroczeń ograniczeń ruchu
    i. mechanizm odzyskiwania utraconych pakietów przez dodanie dodatkowych nadmiarowych danych do transmisji. Mechanizm powinien mieć możliwość skonfigurowania aplikacji, dla których jest aplikowany oraz możliwość załączenia się (wysyłania nadmiarowych danych) tylko, gdy warunki sieciowe ulegną degradacji
20. Musi obsługiwać funkcjonalność Sflow lub odpowiednik (J-Flow, NetFlow);
21. Musi posiadać funkcjonalność VRRP lub odpowiednika;
22. Musi umożliwiać zarzadzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3;
23. Musi posiadać wsparcie dla systemów AAA (RADIUS, TACACS);
24. Musi posiadać 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;
25. Musi posiadać możliwość wyszukiwania fragmentów konfiguracji z linii poleceń Urządzenia, dzięki stosowaniu wyrażeń-filtrów;
26. Musi wspierać standardy szyfrowania ruchu – IPSec z wykorzystaniem co najmniej AES-256 w trybie CBC lub GCM, HMAC-SHA1, ECDSA (256/384 bit), SHA-1 i SHA-2.
27. Musi posiadać funkcjonalność uwierzytelnienia urządzeń na bazie certyfikatów X.509 podpisanych zaufanymi kluczami prywatnymi – zintegrowane w systemie CA z mechanizmem automatycznej dystrybucji kluczy (bez wykorzystania kluczy typu pre-shared)
28. Musi mieć możliwość segmentacji sieci, np. w oparciu o osobne tablice routingu (obsługa nakładających się przestrzeni adresowych); możliwość definicji topologii sieciowej per segment; obsługa co najmniej 4-ech segmentów

29. Musi obsługiwać translację adresów NAT/PAT i NAT Traversal - wsparcie dla lokalnego wyjścia do Internetu z pominięciem komunikacji przez sieć WAN dla zdefiniowanych aplikacji - ruch taki powinien być translowany i lokalnie wychodzić do Internetu
30. Musi mieć możliwość segmentacji routera na co najmniej 4 odseparowane na warstwie IP podsieci – poprzez funkcjonalność VPN
31. Musi mieć funkcjonalność zapory sieciowej dla protokołu IPv4 i IPv6 opartej o definicję stref bezpieczeństwa (zone-based firewall)
32. Musi mieć funkcjonalność IPS
33. Musi mieć funkcjonalność filtracji URL
34. Musi mieć funkcjonalność analizy ruchu pod kątem występowania w nim malware'u
35. Musi mieć funkcjonalność TLS Proxy – umożliwiająca rozszyfrowanie ruchu płynącego od użytkownika i poddania go inspekcji np. przez mechanizm wykrywania malware'u
36. Musi mieć możliwość rozszerzenia o funkcjonalność umożliwiającą agregację tuneli VPN z komputerów użytkowników
37. Musi posiadać funkcjonalności dla trybu pracy SD-WAN
38. Musi posiadać graficzny interfejs konfiguracyjny
39. Musi posiadać obsługę RBAC - możliwość zróżnicowania ról administratorów w zakresie brak dostępu, tylko odczyt, pełen dostęp dla poszczególnych funkcjonalności systemu zarządzania – co najmniej alarmów, logów, monitorowania urządzeń, aktualizacji oprogramowania, interfejsów, polityk, routingu, bezpieczeństwa)
40. Urządzenie musi być objęte wsparciem producenta (sprzęt oraz oprogramowanie):
    a. minimum 36 miesięcy
    b. wymiana uszkodzonego sprzętu w terminie maksymalnie 3 dni roboczych [zgonie ze złożoną oferta Wykonawcy]
    c. nielimitowana ilość zgłoszeń u wsparcia technicznego (TAC)
    d. dostęp do baz wiedzy
    e. możliwość ściągania nowego oprogramowania
41. Wszystkie opisane w niniejszym dokumencie funkcje muszą być wspierane przez urządzenie na poziomie licencyjnym. Zamawiający dopuszcza licencje w formie subskrypcji – subskrypcje nie mogą być dostarczone na okres krótszy niż 36 miesięcy.

IV. Warunki równoważności

1. Certyfikat producenta – certyfikat wydany przez akredytowane centrum szkoleniowe producenta oferowanego rozwiązania, potwierdzający poniższe umiejętności:
   a. - wdrażanie i konfiguracja
   b. - zarządzanie regułami routera
   c. - monitorowanie i raportowanie
   d. - najlepsze praktyki w zakresie bezpieczeństwa