Zp 2130-193/18

Załącznik Nr 1 do SIWZ
Załącznik Nr 1 do Umowy

S Z C Z E G Ó Ł O W Y O P I S P R Z E D M I O T U Z A M Ó W I E N I A

Przedmiotem zamówienia jest dostawa nowych, nieużywanych i nieobciążonych prawami osób trzecich urządzeń do sieci rozległej sterowanej programowo, spełniających poniżej opisane wymagania:

Wymagania ogólne dla urządzeń aktywnych

- Dostarczane urządzenia muszą być nowe (tzn. wyprodukowane nie dawniej niż na 6 miesięcy przed ich dostarczeniem, nierefabrykowane) oraz nieużywane.
- Dostarczane rozwiązania muszą odpowiadać wymaganiom polskich norm przenoszących normy europejskie lub norm innych państw członkowskich europejskiego obszaru gospodarczego przenoszących te normy.
- Urządzenia wraz z zainstalowanym na nich oprogramowaniem muszą pochodzić z legalnego źródła i być przeznaczone do użytkowania na terenie unii europejskiej.
- Całość dostarczonego rozwiązania musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w wymaganym okresie.
- Dostarczane licencje i subskrypcje na oprogramowanie muszą zapewniać pracę rozwiązania przez cały okres gwarancji.
- Korzystanie przez użytkownika z dostarczonych produktów nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
- Każdego dostarczanego urządzenia/materiału należy dostarczyć certyfikat pochodzenia lub inny dokument wystawiony przez producenta lub jego lokalnego przedstawiciela (zawierającego m.in. Dane identyfikacyjne produktu pozwalające na jego identyfikację np. Kod produktu, nr seryjny itp.) Potwierdzający, że dany dostarczony produkt jest fabrycznie nowy, jest oznakowany symbolem ce, pochodzi z autoryzowanej sieci sprzedaży – oficjalnego kanału sprzedaży na rynek europejski.
- Dostarczone oprogramowanie musi być oprogramowaniem w wersji aktualnej (tzn. Opublikowanej przez producenta nie wcześniej niż 6 miesięcy albo ostatniej opublikowanej)
- Jeżeli wymagania szczegółowe nie stanowią inaczej, wszystkie wymagane funkcjonalności muszą być dostępne w oferowanych rozwiązaniach w dniu dostawy.
- Zamawiający zastrzega sobie prawo do zwrócenia się do oferenta lub producentów oferowanych rozwiązań o potwierdzenie spełniania wybranych wymagań i wskazanie potwierdzenia ich spełnienia w publicznie dostępnej dokumentacji produktów (dopuszczalny język polski lub angielski).

Wymagania funkcjonalne rozwiązania WAN

- Rozwiązanie ma należeć do klasy rozwiązań sieci rozległych sterowanych programowo - przez co rozumie się rozwiązania szyfrujące wszystkie łącza WAN, z centralnym, redundantnym kontrolerem zarządzającym i monitorującym całą sieć, z możliwością ustalania polityk związanych z jakością obsługi aplikacji i ew. przełączeniem ruchu aplikacji na łącza spełniające wymagania aplikacji zdefiniowane w polityce.
- Rozwiązanie ma umożliwiać bezpieczne połączenie WAN oddziałów, wykorzystując w tym celu dowolną kombinację połączeń przez sieci prywatne (np. IP VPN) i publiczne (Internet).
- Rozwiązanie ma umożliwiać aktywne wykorzystanie wszystkich dostępnych połączeń pomiędzy oddziałami, odpowiednio sterując ruchem zależnie od aktualnych warunków:
    - elastyczne tworzenie topologii (gwiazda, możliwość rozbudowy funkcjonalności o częściową lub pełną kratę, punkt-punkt),
    - monitorowanie wydajności wszystkich łączy systemu,
    - równoważenie obciążenia poszczególnych łącz (per sesja):
        - statyczne (active/standby i active/active równoważne i ważone),
        - dynamiczne oparte o monitorowanie jakości w danym czasie,
    - możliwość redundancji active-active urządzeń na poziomie każdego oddziału z możliwością obsługi poszczególnych łączy przez dedykowane urządzenia.
- Obsługa funkcjonalności z zakresu bezpieczeństwa:
    - szyfrowanie co najmniej AES256,
    - funkcja skrótu co najmniej SHA-2 512bitów,
    - uwierzytelnienie urządzeń na bazie certyfikatów X.509 podpisanych zaufanymi kluczami prywatnymi,
    - zabezpieczenia warstwy kontroli urządzeń przed atakami DDoS w postaci list kontroli dostępu (ACL) i ograniczników ruchu do urządzeń - wymaga się możliwości stworzenia polityki ograniczającej przepływność zdefniowanego ruchu, rozpoznanego jako np. część ataku DDoS) przez mechanizm kształtowania (shaping) do niskiej wartości (bezpiecznej dla urządzenia),
    - możliwość rozbudowy funkcjonalności o:
        - stanowy firewall z możliwością obsługi podinterfejsów z VLANami,
        - segmentację sieci w oparciu o osobne tablice routingu - w szczególności osobna tablica routingu na komunikację związaną z zarządzaniem; możliwość definicji topologii sieciowej per segment,
        - przesyłanie wybranego ruchu do urządzeń zewnętrznych:
            - możliwość określenia ruchu - np. z danej aplikacji, czy poprzez ACL - w celu przekierowania go do zewnętrznego urządzenia lub usługi z możliwością budowy łańcucha usług (service chaining) - np. w celu inspekcji IPS, Firewalla, Proxy, itp.,
            - przekierowany może być tylko ruch określony przez administratora, pozostały ruch ma być routowany wg polityki sieci.
- Polityki jakości obsługi aplikacji:
    - wykrywanie aplikacji na bazie głębokiej inspekcji ruchu (DPI),
    - możliwość rozbudowy funkcjonalności o:
        - definicję polityki systemu określającej maksymalne tolerowane przez określoną aplikację parametry sieci: opóźnienie, zmienność opóźnień, straty w pakietach - w przypadku przekroczenia zdefiniowanych progów ruch

aplikacyjny powinien zostać przekierowany na inne łącze WAN, jeśli spełnia ono wymogi aplikacji wg polityki,
        - monitorowanie jakości dostępu do usług chmurowych typu SaaS (co najmniej Amazon, Azure, Google, Office365, Dropbox) z możliwością optymalizacji dostępu do nich - system musi umożliwiać przekierowanie ruchu do usług przez każdy węzeł dysponujący lokalnym wyjściem do Internetu, zapewniający w danym czasie najlepszą jakość dostępu do usługi,
- Mechanizmy zapewnienia jakości ruchu (QoS):
    - obsługa kształtowania (shaping), ograniczania (policing) ruchu, gwarancje pasma,
    - kolejkowanie z kolejką priorytetową i model WFQ (Weighted Fair Queuing) dla pozostałych klas ruchu,
    - mechnizm tail-drop i RED (Random Early Detect),
    - oznaczanie i zmiana oznaczeń DSCP na bazie przekroczeń ograniczeń ruchu.
- Obsługa translacji adresów NAT i NAT Traversal:
    - wsparcie dla NAT i PAT,
    - wsparcia dla komunikacji oddziałów, jeśli są one za poszczególnymi rodzajami NATowania:
        - NAT, PAT,
        - Full Cone NAT,
        - Port Restricted Full Cone NAT,
        - Symmetric NAT,
          dopuszczalna jest możliwość braku komunikacji w przypadku dwóch oddziałów podłączonych Symmetric NAT - Port/Address Restricted lub Symmetric NAT - Symmetric NAT
    - 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.
- Obsługa API umożliwiającego konfigurację wszystkich możliwości oferowanych przez kontroler centralny za pomocą wywołań API:
    - dopuszczalne standardy API to: Python, Ansible, REST, RESTConf, NETConf/Yang, XML,
    - API nie może opierać się o SNMP lub dostęp po SSH:
- Wymaga się wsparcia dla protokołów routingu dynamicznego:
    - OSPFv2,
    - BGP,
    - BFD ,
    - Multicast (IGMP, PIM, SSM).
- Obsługa protokołów i funkcjonalności sieciowych:
    - VRRP,
    - IPSec/IKEv1/IKEv2 dla połączeń na zewnątrz sieci;,
    - 802.1q,
    - Serwer DHCP,
    - SSHv2 ,
    - SNMP v2c, v3,
    - obsługa RBAC,
    - uwierzytelnienie Radius,
    - NTP z uwierzytelnieniem,

    - określanie IP MTU, TCP MSS,
    - Syslog .
- Rozwiązanie ma opierać się o centralny kontroler, routery agregacyjne i oddziałowe uwierzytelniające się z innymi komponentami rozwiązania poprzez certyfikaty X.509 podpisane kluczami prywatnymi związanymi ze sprzętowymi modułami TPM (Trusted Platform Module) routerów.
- Routery mają mieć możliwość automatycznego nawiązania połączenia przez sieć Internet z kontrolerami centralnymi bez jakiejkolwiek konfiguracji urządzenia:
    - w celu pełnej konfiguracji routera wystarczy podłączyć go do prądu i łącza internetowego (przewodowego lub sieci komórkowej),
    - wyklucza się możliwość konfiguracji wstępnej przez CLI lub interfejs HTTP(s) - urządzenie powinno się zarejestrować do sieci bez żadnej konfiguracji wstępnej,
    - proces plug'n'play (inaczej nazywany np. Zero Touch Provisioning) powinien uwierzytelnić router z kontrolerami w sposób zapewniający kryptograficzną weryfikację tożsamości oraz ustanowić bezpieczne tunele szyfrowane, przez które router jest automatycznie konfigurowany do pracy w sieci.
- Zarządzanie routerami ma odbywać się całkowicie z poziomu kontrolerów centralnych:
    - wymaga się zarządzania aktualizacją oprogramowania z centralnego systemu,
    - w przypadku niepowodzenia aktualizacji oprogramowania system przywraca urządzenia do poprzedniej działającej wersji oprogramowania w sposób automatyczny,
    - w przypadku utraty łączności po skonfigurowaniu urządzeń system przywróci konfigurację urządzeń do ostatniej działającej wersji.
- Konfiguracja urządzeń ma opierać się o tzw. wzorce konfiguracyjne:
    - jeden wzorzec może obsłużyć wiele routerów,
    - wzorce muszą mieć możliwość definicji zmiennych uzupełnianych dla poszczególnych routerów,
    - wzorce konfiguracyjne po ich zmianie przekładają zmianę konfiguracji na powiązane ze wzorcem urządzenia. Ew powinna istnieć możliwość skopiowania wzorca do nowego, który nie ma powiązanych ze sobą urządzeń.
- Wymagana jest dostawa wszystkich niezbędnych elementów rozwiązania, w tym redundantnych kontrolerów z niezbędnymi platformami sprzętowymi, platform dla poszczególnych lokalizacji oraz licencji i subskrypcji na oprogramowanie.

Warunki gwarancji i serwisu

- Gwarancja producenta min. do **31-12-2021**; Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta, gwarancja musi być przypisana na klienta końcowego którym jest Zamawiający.
- Serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego (poniedziałek – piątek 7:00 - 15:00); usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) ma zostać wykonana w przeciągu dwóch dni roboczych od momentu zdiagnozowania usterki; Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań.

- W przypadku Sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający dopuszcza podstawienie na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 14 dni od momentu zgłoszenia usterki.
- Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego.
- Zamawiający uzyska dostęp do części chronionych stron internetowych producentów rozwiązań, umożliwiający:
    - pobieranie nowych wersji oprogramowania,
    - dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
    - dostęp do pomocy technicznej producentów,
    - bezpośrednie zgłaszanie awarii i problemów.
- Zamawiający będzie miał możliwość aktualizacji oprogramowania wszystkich komponentów do najnowszej wersji oferowanej przez producenta, jeżeli w tym celu wymagane jest zaoferowanie dodatkowych aktualizacji tzw. Upgrade, do aktualnie obowiązującej wersji wspieranej przez producenta to takie aktualizacje muszą zostać uwzględnione w ofercie, wraz z wykonaniem aktualizacji do najnowszej obowiązującej wersji przez Oferenta w czasie dogodnym dla Zamawiającego.

Wymagania dla platform sprzętowych dla poszczególnych lokalizacji

Wymagania ogólne

- urządzenia dedykowane dla rozwiązania sieci rozległych sterowanych programowo lub znajdujące się na oficjalnej liście kompatybilności producenta oprogramowania
- możliwość instalacji w szafie rack 19” (dostarczone niezbędne akcesoria, szyny, adaptery itp.), wysokość nieprzekraczająca 2U
- zasilanie 230V AC
- możliwość pracy w zakresie temperaturowym 0 – 40 ^{o}C i wilgotności powietrza 10 – 80 % (bez kondensacji)

TYP 1: Wymagania dla platformy agregacyjnej

Liczba kompletów: 2 szt.

- co najmniej 8 portów 1 Gbps ze stykiem definiowanym przez moduły SFP lub równoważne (obsadzone min. 4 modułami 1000Base-SX)
- co najmniej 4 porty 10 Gbps ze stykiem definiowanym przez moduły SFP+ lub równoważne
- możliwość rozbudowy o co najmniej:
    - 16 portów 1 Gbps

      lub

    - 8 portów 10Gbps
- zasoby przetwarzania wystarczające do obsługi ruchu szyfrowanego na poziomie 20Gbps (AES-256)
- dostarczone wraz z urządzeniami licencje umożliwiające obsługę zdublowanego łącza 1Gbps

TYP 2: Wymagania dla platformy dostępowej dla dużych oddziałów

Liczba kompletów: 8 szt

- co najmniej 4 porty 1 Gbps ze stykiem definiowanym przez moduły SFP lub równoważne (obsadzone modułami 1000Base-SX) z możliwością rozbudowy o co najmniej:
    - 16 portów 1 Gbps

    lub

    - 4 portów 10 Gbps
- zasoby przetwarzania wystarczające do obsługi ruchu szyfrowanego na poziomie 10Gbps (AES-256)

- dostarczone wraz z urządzeniami licencje umożliwiające obsługę łączy 100Mbps (podstawowe) i 100 Mbps (zapasowe)

TYP 3: Wymagania dla platformy dostępowej dla średnich oddziałów

Liczba kompletów: 68 szt

- co najmniej 8 portów 1 Gbps ze stykiem definiowanym przez moduły SFP lub równoważne (min. 4 obsadzone modułami 1000Base-T)
- zasoby przetwarzania wystarczające do obsługi ruchu szyfrowanego na poziomie 1Gbps (AES-256)
- dostarczone wraz z urządzeniami licencje umożliwiające obsługę łączy 100Mbps (podstawowe) i 100 Mbps (zapasowe)

Dostawa, projekt wdrożenia, szkolenia:

Zamawiający wymaga dostawy sprzętu we wskazanych przez siebie lokalizacjach.
Wykonawca musi przygotować szczegółowy projekt wdrożenia i migracji z obecnie używanej topologii do nowo projektowanego rozwiązania.
Wykonawca musi dostarczyć vouchery dla trzech osób do autoryzowanego przez producenta centrum szkoleniowego na:

- min. 3 dniowe szkolenie z dostarczonej technologii
- min. 5 dniowe szkolenie z projektowania w dostarczonej technologii

do wykorzystania w terminie nie krótszym niż 6 miesięcy od dnia zawarcia umowy.