**FORMULARZ CENOWO-PRZEDMIOTOWY**

Przedmiotem zamówienia jest system firewall składający się z dwóch urządzeń uruchomionych w wysokiej dostępności jako klaster active-active. System firewall będzie przeznaczony do ochrony zasobów sieci komputerowej Uniwersytetu Gdańskiego.

**TABELA 1.** Opis przedmiotu zamówienia.

|  |  |
| --- | --- |
| **Nazwa elementu** | **Szczegółowy opis oferowanych elementów przez Wykonawcę** |
| 1. **Firewall sprzętowy**
 | Należy podać:**Producent: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****Numery producenta elementów składowych (należy wymienić wszystkie oferowane składowe produktu):****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_sztuk\_\_\_\_\_\_\_\_****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_sztuk\_\_\_\_\_\_\_\_****W tym moduły optyczne:****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_sztuk\_\_\_\_\_\_\_\_****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_sztuk\_\_\_\_\_\_\_\_** |
| 1. **Licencje, subskrypcje**
 | Należy podać:**Producent: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****Numery producenta elementów składowych (należy wymienić wszystkie oferowane składowe produktu):****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_sztuk\_\_\_\_\_\_\_\_****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_sztuk\_\_\_\_\_\_\_\_** |
| 1. **Wsparcie techniczne producenta oferowanego urządzenia**
 | Należy podać:**Producent: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****Numery producenta elementów składowych (należy wymienić wszystkie oferowane składowe produktu):****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_sztuk\_\_\_\_\_\_\_\_****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_sztuk\_\_\_\_\_\_\_\_** |
| Część opisowa:**Własności fizyczne.**1. Urządzenie musi być przystosowane do montażu w szafie rack 19".
2. Wysokość urządzenia nie może przekraczać 3U.
3. Głębokość urządzenia nie może przekraczać 70cm.
4. Jeżeli urządzenie posiada wentylatory, wówczas:
5. urządzenie musi posiadać co najmniej dwa wymienne moduły wentylacji z możliwością wymiany wadliwego modułu podczas pracy urządzenia.
6. przepływ powietrza musi być realizowany z przodu na tył urządzenia.

**II. Środowisko pracy.**1. Urządzenie musi prawidłowo pracować w temperaturze od 5 do 40 stopni Celsjusza.

**III. Interfejsy fizyczne do analizowania i kontroli ruchu.**1. Urządzenie musi posiadać co najmniej 12 interfejsów do analizowania i kontroli ruchu, w tym:
	1. Co najmniej 8 obsługujących standard 10GBase-LR.
	2. Co najmniej 4 interfejsy obsługujące standard 40GBase-LR4.
2. Urządzenie musi być wyposażone w cztery moduły optyczne 10GBase-LR.
3. Wszystkie interfejsy muszą być niezależne od siebie, tzn. wykorzystanie, któregoś interfejsu nie może zmniejszać ilości wymaganych interfejsów.
4. Wszystkie interfejsy muszą znajdować się na przedniej części panelu urządzenia.
5. Zamawiający wymaga oryginalnych modułów optycznych producenta urządzenia.
6. Urządzenie musi obsługiwać agregowanie połączeń fizycznych zgodne z IEEE 802.3ad.
7. Urządzenie musi obsługiwać protokół LACP (ang. Link Aggregation Control Protocol).
8. Interfejs fizyczny musi mieć możliwość umieszczenia na nim wielu interfejsów logicznych.

**IV. Interfejsy fizyczne do zarządzania urządzeniem.**1. Urządzenie musi być wyposażone w port konsoli do zarządzania urządzeniem.
2. Urządzenie musi być wyposażone w dedykowany port Ethernet do zarządzania urządzeniem o przepustowości co najmniej 1Gbps (tzw. Out of Band Ethernet port).

**V. Interfejsy fizyczne dla wysokiej dostępności.**1. Urządzenie musi posiadać dedykowane interfejsy do połączenia w klaster składający się z dwóch urządzeń.
2. Interfejsy muszą umożliwiać wykonanie połączenia po światłowodzie jednomodowym do 10km.
3. Wraz z urządzeniem należy dostarczyć moduły optyczne jeżeli są wymagane do połączenia w klaster.
4. Łącza pomiędzy urządzeniami w klastrze muszą mieć przepustowość co najmniej 10Gbps.
5. Interfejsy dla wysokiej dostępności nie mogą zmniejszać ilości wymaganych interfejsów do zarządzania urządzeniem oraz nie mogą zmniejszać ilości wymaganych interfejsów do analizowania i kontroli ruchu.

**VI. Funkcje podstawowe.**1. Urządzenie musi umożliwiać synchronizacje czasu z serwerem NTP.
2. Urządzenie musi umożliwiać wysyłanie logów do zewnętrznego serwera zgodnego z protokołem syslog.
3. Urządzenie musi posiadać mechanizm kontroli pasma oraz ruchu (ang. Quality of Service, QoS).
4. Urządzenie musi obsługiwać VLAN zgodne z IEEE 802.1Q.
5. Urządzenie musi obsługiwać protokół SNMP w wersji 2c i 3.
6. Urządzenie musi obsługiwać przekazywanie pakietów DHCP.

**VII. Wydajność.**1. Urządzenie musi obsługiwać co najmniej 150000 (sto pięćdziesiąt tysięcy) nowych połączeń na sekundę.
2. Urządzenie musi obsługiwać co najmniej 4000000 (cztery miliony) jednoczesnych sesji.

**VIII. Pamięć.**1. Urządzenie musi posiadać co najmniej 960GB wymiennej pamięci przeznaczonej na zdarzenia,

uruchomionej w RAID 1 (awaria jednego z dysków nie może powodować utraty danych).**IX. Firewall.**1. Urządzenie musi realizować funkcję firewall na podstawie stref bezpieczeństwa (ang. Security Zones).
2. Strefy bezpieczeństwa.
	1. Urządzenie musi obsługiwać co najmniej 2000 (dwa tysiące) stref.
	2. Strefy muszą obsługiwać interfejsy logiczne należące do różnych sieci VLAN.
3. Polityki bezpieczeństwa (ang. Security Rules).
	1. Urządzenie musi obsługiwać co najmniej 30000 (trzydzieści tysięcy) polityk bezpieczeństwa.
	2. Urządzenie musi pozwalać na używanie poniższych kryteriów do opisania polityki bezpieczeństwa:
		1. Źródłowa lub docelowa strefa bezpieczeństwa.
		2. Źródłowy lub docelowy adres/obiekt IPv4 lub IPv6.
		3. Aplikacja.
4. Urządzenie musi mieć możliwość pracy w trybie transparentnym, w trybie routera oraz w trybie nasłuchu.
5. Urządzenie musi zapewniać filtrowanie ruchu IPv4 i IPv6.

**X. Funkcja VPN.**1. Urządzenie musi obsługiwać sieci VPN IPsec w konfiguracji sieć-sieć (ang. network-to-network).
2. Urządzenie musi obsługiwać algorytmy szyfrowania w ramach IPsec, takie jak:
3. AES o długości klucza: 128, 192, 256 bitów.
4. 3DES
5. Urządzenie musi obsługiwać autentykację w ramach IPsec, takie jak:
	1. MD5, SHA-1, SHA-256.
6. Urządzenie musi obsługiwać co najmniej 5000 (pięć tysięcy) jednoczesnych tuneli IPsec VPN.
7. Wydajność urządzenia dla VPN IPsec nie może być mniejsza niż 8 Gbps.

**XI. Zapobieganie zagrożeniom.**1. Urządzenie musi posiadać mechanizm wykrywania i blokowania ataków sieciowych w czasie rzeczywistym (ang. Intrusion Prevention System, IPS) z wydajnością przetwarzania na poziomie co najmniej 8 Gbps.
2. Wykrywanie ataków musi odbywać się na podstawie sygnatur dostarczonych od producenta.
3. Baza sygnatur musi mieć możliwość automatycznej aktualizacji.
4. Administrator systemu musi mieć możliwość definiowania własnych sygnatur.
5. Urządzenie musi posiadać ochronę antywirusową.

**XII. Identyfikacja aplikacji.**1. Urządzenie musi identyfikować aplikacje niezależnie od wykorzystywanego portu TCP/UDP na podstawie wbudowanej bazy aplikacji.
2. Przy włączonym mechanizmie identyfikowania aplikacji, urządzenie musi mieć przepustowość na poziomie co najmniej 16 Gbps.
3. Baza aplikacji musi mieć możliwość automatycznej aktualizacji.
4. Urządzenie musi rozpoznawać co najmniej 2500 aplikacji.
5. Wraz z urządzeniem należy dostarczyć listę rozpoznawanych przez urządzenie aplikacji w formie drukowanej lub elektronicznej.

**XIII. Routing.**1. Urządzenie musi obsługiwać statyczny routing dla IPv4 i IPv6.
2. Urządzenie musi obsługiwać dynamiczne protokoły routingu takie jak:
	1. OSPFv2.
	2. OSPFv3.
	3. BGP.
3. Urządzenie musi umożliwiać uruchomienie różnych instancji routingu, w ilości nie mniejszej niż 20.
4. Urządzenie musi obsługiwać Policy Based Routing.

**XIV. Funkcja NAT.**1. Urządzenie musi obsługiwać translacje adresów sieciowych (ang. Network Address Translation, NAT) w następujących trybach:
	1. Static NAT.
	2. Destination NAT.
	3. Source NAT.
2. Polityki NAT muszą być definiowane niezależne od polityk bezpieczeństwa.
3. Urządzenie musi obsługiwać co najmniej 5000 polityk NAT.
4. Definiowanie polityki NAT musi być oparte o co najmniej takie kryteria jak:
	1. Źródłowa lub docelowa strefa bezpieczeństwa.
	2. Źródłowy lub docelowy adres IPv4 lub IPv6.
5. Urządzenie musi obsługiwać NAT64.
6. Urządzenie musi obsługiwać NATv6.

**XV. Wirtualne systemy.**1. Urządzenie musi obsługiwać wirtualne systemy.
2. Każdy wirtualny system musi mieć możliwość uruchomienia osobnej tablicy routingu.
3. Każdy wirtualny system musi mieć osobny zestaw polityk bezpieczeństwa.
4. Każdy interfejs fizyczny musi mieć możliwość współdzielenia pomiędzy wirtualnymi systemami.
5. Urządzenie musi obsługiwać co najmniej 20 wirtualnych systemów.

**XVI. Zarządzanie.**1. Praca na urządzeniu musi odbywać się na konfiguracji kandydackiej, a nie aktywnej.
2. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit).
3. Przed zatwierdzaniem zmian na urządzeniu musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej.
4. Zarządzanie urządzeniem musi odbywać się co najmniej za pomocą:
	1. Interfejsu wiersza poleceń (ang. Command Line Interface, CLI) poprzez port konsolowy, Telnet oraz SSH.
	2. Interfejs graficzny poprzez przeglądarkę internetową (ang. web browser).
	3. Interfejs programistyczny (API).
5. Urządzenie musi mieć możliwość przywrócenia konfiguracji z określnego dnia, w którym były dokonywane zmiany, tzn. po każdym zapisie konfiguracji na urządzeniu powinna być automatycznie zapisywana kompletna konfiguracja, liczba przechowywanych w ten sposób konfiguracji nie może być mniejsza niż 50, podczas wyboru konfiguracji musi być widoczna data zapisania konfiguracji.
6. Urządzenie musi umożliwiać uwierzytelnianie użytkowników administracyjnych za pomocą:
	1. Bazy lokalnej.
	2. Serwera RADIUS.
	3. Serwera TACACS+.
7. Urządzenie musi mieć zdefiniowane w systemie co najmniej dwa konta typu:
	1. Administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu
	2. Operator, który ma możliwość tylko odczytu konfiguracji.
8. Urządzenie musi umożliwiać utworzenie nowych typów kont administracyjnych.

**XVII. Zasilanie urządzenia.**1. Urządzenie musi działać przy zasilaniu jednej fazy 230V/50Hz z sieci elektrycznej.
2. Urządzenie musi być wyposażone w wymienne i redundantne zasilacze.
3. Gniazda zasilające muszą się znajdować w tylnej części urządzenia.
4. Awaria połowy zasilaczy nie może wpływać na działanie urządzenia.
5. Urządzenie musi umożliwiać wymianę zasilacza bez wyłączania urządzenia.
6. Wraz z urządzeniem muszą być dostarczone kable zasilające.
7. Połowa kabli zasilających musi mieć możliwość podłączenia do gniazda jednofazowego typu E (standardowe jednofazowe gniazdo elektryczne stosowane w Polsce).
8. Połowa kabli musi mieć możliwość podpięcia do zasilacza awaryjnego, ma to być kabel zakończony wtykiem IEC-320 C14 lub IEC-320 C20.
9. Średnie zużycie energii przez urządzenie nie może przekraczać 700W.

**XVIII. Wysoka dostępność.**1. Urządzenie musi pozwalać na pracę z innym urządzeniem w parze jako klaster.
2. Urządzenie musi mieć możliwość uruchomienia klastra w trybie: active-active (oba urządzenia zajmują się jednocześnie przetwarzaniem ruchu) i active-pasive (pierwsze urządzenie zajmuje się przetwarzaniem ruchu, drugie zaczyna przetwarzanie ruchu w momencie awarii pierwszego urządzenia).
3. Awaria pojedynczego urządzenia w klastrze nie może wpłynąć na prawidłowe działanie sieci komputerowej.
4. Urządzenia uruchomione w klastrze:
	1. Muszą automatycznie między sobą synchronizować konfiguracje.
	2. Muszą obsługiwać synchronizację sesji.

**XIX. Dokumentacja.**1. Na stronie producenta urządzenia muszą być dostępne w języku polskim lub angielskim:
	1. Przewodniki administracji (ang. Administration guide).
	2. Informacje dotyczące wydania aktualizacji oprogramowania (ang. Release notes).

**XX. Licencje, subskrypcje.**1. Wszystkie funkcjonalności wymienione w części opisowej muszą być dostępne, jeżeli wymagają licencji należy dostarczyć je wraz z urządzeniem.
2. Wszystkie licencje muszą być bezterminowe, wyjątkiem mogą być licencje i subskrypcje na aktualizacje:
	1. Bazy aplikacji, która musi być aktywna przez co najmniej okres trwania wsparcia technicznego (wymienionego w pkt XXI tabeli nr 1) urządzenia.
	2. Bazy sygnatur zapobiegania zagrożeniom, która musi być aktywna co najmniej przez okres trwania wsparcia technicznego (wymienionego w pkt XXI tabeli nr 1).
3. Wszystkie interfejsy fizyczne muszą być aktywne, tzn. jeżeli jest wymagana licencja na ich aktywację, należy dostarczyć licencje wraz z urządzeniem.

**XXI. Gwarancja / wsparcie techniczne*** 1. Urządzenie musi być objęte gwarancją przez okres nie krótszy niż 36 miesięcy, z uwzględnieniem zapisów w rozdziale XIV SIWZ - gwarancja stanowi jedno z kryteriów oceny ofert.
1. Gwarancję musi świadczyć producent lub każdy upoważniony przez niego podmiot do świadczenia tych usług (Gwarant).
2. Zgłaszanie wady urządzeń ma odbywać się drogą elektroniczną lub telefonicznie. W przypadku kontaktu telefonicznego ma się to odbyć w krajowej sieci telekomunikacyjnej z wyłączeniem linii o podwyższonej opłacie rozliczeniowej. Sposób komunikacji ma być określony w karcie gwarancyjnej przekazanej w momencie dostawy urządzenia.
3. Komunikacja z Gwarantem ma być dokonywana w języku polskim albo angielskim.
4. Termin usunięcia wady urządzenia nie może przekroczyć 3 dni roboczych od momentu zgłoszenia wady.
5. W ramach gwarancji Wykonawca zapewnia wsparcie techniczne producenta urządzenia – przez cały okres udzielonej gwarancji.
6. W ramach wsparcia technicznego dla oferowanego urządzenia musi:
	1. być możliwość dostępu do systemu obsługi zgłoszeń serwisowych,
	2. być zapewniony dostęp do aktualnej wersji oprogramowania,
	3. istnieć możliwość wymiany urządzenia na wolne od wad w terminie do 3 dni roboczych od momentu zgłoszenia wady (w przypadku braku możliwości jej usunięcia w miejscu instalacji),
	4. istnieć możliwość pozostawienia u Zamawiającego uszkodzonych nośników pamięci wymienionych w pkt VIII.1 (w przypadku ich awarii).

**XXII. Szkolenie.**1. W ramach dostawy urządzeń należy zrobić 3 dniowe szkolenie dla 25 pracowników z możliwością podzielenia na mniejsze grupy. Czas szkolenia ma wynosić 8 godzin każdego dnia.
2. Szkolenie ma zostać przeprowadzone nie później niż w ciągu 7 dni roboczych od momentu podpisania protokołu odbioru sprzętu. Dokładny termin szkolenia należy ustalić z Centrum Informatycznym UG.
3. Szkolenie musi być przeprowadzone w siedzibie Zamawiającego.
4. Szkolenie musi być przeprowadzone w języku polskim.
5. Szkolenie musi być przeprowadzone przez Instruktora posiadającego stosowne uprawnienia wydane przez producenta urządzenia do prowadzenia odpowiednich szkoleń.
6. Szkolenie musi składać się z części teoretycznej i praktycznej.
7. Szkolenie musi być przeprowadzone z wykorzystaniem sprzętu fizycznego zgodnego z dostarczanym urządzeniem, z tym, że nie mogą to być urządzenia, które dostarcza Wykonawca dla Zamawiającego.
8. Na szkoleniu muszą być omówione co najmniej zagadnienia:
	1. Wstępna konfiguracja urządzenia.
	2. Konfiguracja dostępu dla użytkowników administracyjnych.
	3. Konfiguracja polityk bezpieczeństwa.
	4. Konfiguracja VPN IPsec.
	5. Konfiguracja protokołów routingu.
	6. Konfiguracja NAT.
	7. Konfiguracja wirtualnych systemów.
	8. Monitorowanie zdarzeń.
	9. Logowanie wybranych zdarzeń.
	10. Analiza zdarzeń.
	11. Konfiguracja wysokiej dostępności, tryb active-active i active-pasive.
	12. Aktualizacja oprogramowania.
	13. Zaawansowane rozwiązywanie problemów.
	14. Zgłoszenie problemów związanych z urządzeniem w ramach wsparcia technicznego.
9. Zagadnienia wymienione w pkt XXII.8 należy omówić z poziomu interfejsu graficznego i wiersza poleceń (CLI).
10. Dla każdego uczestnika szkolenia należy dostarczyć materiały szkoleniowe obejmujące zagadnienia wymienione w pkt XXII.8 w postaci elektronicznej lub drukowanej.
 |

**Tabela nr 2.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Lp.** | **Przedmiot zamówienia** | **Ilość** | **Cena jednostkowa netto****PLN** | **Wartość netto****PLN** | **Kwota****podatku VAT****PLN** | **Wartość brutto/bez VAT\*****PLN** |
| 1 | Firewall sprzętowy | 2 |  |  |  |  |
| 2\*\*\* | Licencje, subskrypcje, oprogramowanie w celu realizacji wymaganych funkcjonalności – pkt XX w tabeli 1 | 2  |  |  |  |  |
| 3 | Wsparcie techniczne - pkt XXItabeli 1 | 2  |  |  |  |  |
| 4 | Usługa szkoleniowa - pkt XXII w tabeli 1 | 1 |  |  |  |  |
| **Razem\*\***  |  |  |  |

***\* niepotrzebne skreślić***

***\*\* zsumowane wartości netto, VAT, brutto/bez VAT\* należy wpisać do formularza ofertowego - załącznika nr 1 do SIWZ.***

***\*\*\* w sytuacji gdy Lp. 2 tabeli 2 załącznika nr 1a do SIWZ zawarta jest w cenie urządzenia z Lp. 1 tabeli 2, Zamawiający wymaga wpisania wartości 0,00 PLN.***

*Oferta ma być podpisana kwalifikowanym podpisem elektronicznym, przez osobę(y) uprawnioną(e) do składania oświadczeń woli w imieniu Wykonawcy, zgodnie z formą reprezentacji Wykonawcy określoną w dokumencie rejestracyjnym (ewidencyjnym), właściwym dla formy organizacyjnej Wykonawcy lub pełnomocnika.*