Wojewódzki Szpital Specjalistyczny nr 4 w Bytomiu
Aleja Legionów 10, 41-902 Bytom, NIP 626-25-10-567, REGON 000296271
tel. +48 323 964 500, e-mail: szpital@szpital4.bytom.pl, www.wss4.pl

Załącznik Nr 2F do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. DZIAŁANIE

Projekt	382	Fundusz Przeciwdziałania COVID-19 działań w celu do podniesienia poziomu bezpieczeństwa systemów teleinformatycznych WSS4 w Bytomiu
Postępowanie	104	Zakup sprzętu komputerowego: system UTM + IPS + wraz z licencją
Element	101	Opis przedmiotu zamówienia
Wersja	1	2022-10-06

2. OPIS SYTEMU UTM + IPS + WRAZ Z LICENCJĄ

Minimalne wymaganie techniczne dla pojedynczego urządzenia typu firewall.
W ramach postępowania należy dostarczyć 2 zestawy

1. Wydajność firewalla IPv4 dla pakietów o wielkości 1518/512/64B – 12/12/12 Gbps
2. Wydajność modułu IPS – 9Gbps
3. Ilość jednoczesnych połączeń – 6 000 000
4. Ilość nowych połączeń na sekundę – 200 000
5. Wydajność VPN IPSec – 10 Gbps
6. Ilość jednoczesnych tuneli IPsec – 13 000
7. Możliwość utworzenia 40 000 polityk bezpieczeństwa
8. Ilość tuneli SSL VPN – min. 100. Możliwość licencyjnego rozszerzenia do 2000. Jeżeli funkcjonalność SSL VPN wymaga licencji to należy dostarczyć wraz z urządzeniem licencję na obsługę minimum 100 równoległych sesji SSL VPN
9. Urządzenie wyposażone w redundantne zasilacze typy 230V AC z możliwością wymiany w trakcie pracy urządzenia (ang. hot-swap). Nie dopuszcza się rozwiązań z zewnętrznym redundantnym zasilaczem.
10. Urządzenie wyposażone w 3 moduły wentylatora z możliwością wymiany w trakcie pracy urządzenia (ang. hot-swap)
11. Dedykowany system operacyjny firewalla opracowany przez producenta urządzenia.
    Procesor wielordzeniowy.
    Pamięć RAM minimum 8GB.
    MTBF minimum 25 lat.
    Zakres wilgotności pracy co najmniej 5% - 95%.
    Waga urządzenia nie większa niż 9kg.
    Możliwość montażu w stelażu/szafie 19''.
    Wysokość maksymalna 1U.
12. Architektura systemu - dedykowana platforma sprzętowa opracowana przez producenta wykorzystującej wielordzeniową architekturę sprzętową.
13. Urządzenie musi posiadać następującą ilość interfejsów:
    - Minimum 4 porty 10G SFP+. Obsługa modułów optycznych 10G-SR, 10G-LR
    - Minimum 6 portów 1G SFP. Obsługa modułów optycznych 1G-SX, 1G-LX
    - Minimum 12 portów 10/100/1000Base-T
    - dedykowany port konsoli zgodny ze standardem RS-232
    - urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych
    - dedykowany port zarządzający out-of-band Ethernet 10/100/1000Base-T
14. Możliwość uruchomienia firewalla w trybie routingu, transparentnym lub hybrydowym (oba tryby uruchomione jednocześnie).
15. Mechanizmy ochrony sieci IP w wersji IPv6.
16. Obsługa protokołów routingu dla IPv6: BGP4+, IS-ISv6, OSPFv3 oraz RIPng.
17. Obsługa protokołów routingu dla IPv4: RIP, OSPF, BGP, IS-IS, obsługa rutingu multicast'owego (MSDP, PM-DM, PM-SM, IGMP oraz statycznego rutingu multicast'owego)
18. Możliwość uruchomienia funkcjonalności IPS, AV, URL filtering oraz AS. Wraz z urządzeniem ma być dostarczona subskrypcja na aktualizację wszystkich funkcjonalności UTM minimum na 3 lata.
19. Możliwość uruchomienia przynajmniej 200 wirtualnych firewalli. Jeśli jest wymagana licencja urządzenie powinno być dostarczone z licencją na przynajmniej 10 wirtualnych firewalli.
20. Możliwość uruchomienia funkcjonalności NAT w tym translacja adresu IP źródłowego, translacja adresu IP przeznaczenia, PAT, translacja statyczna i translacje puli adresów IP.
21. Wsparcie dla funkcjonalności ASPF. Inspekcja różnych protokołów w celu przepuszczenia odpowiedniego ruchu w tym FTP, H323, SIP, RTSP, NetBios.
22. Możliwość konfiguracji kontroli dostępu na podstawie adresów źródłowych i docelowych, portów, typu protokołu, czasu,

TOS, użytkownika oraz aplikacji rozpoznawalnej przez analizę warstwy siódmej.

23. Integracja z wewnętrzną i zewnętrzna bazą użytkowników (local, RADIUS, TACACS, AD, LDAP)
24. Ochrona przed atakami typu SYN flood, ICMP Flood, IP spoofing, UDP Flood, Land, Fraggle, Smurf, Winnuke, Ping of Death, Tear Drop, skanowanie adresów oraz portów, IP Option control, IP fragment, large ICMP packet, ICMP redirect packet, ICMP unreachable.
25. Ograniczanie pasma dla ruchu P2P poprzez tworzenie odpowiednich polityk. Możliwość tworzenia różnych polityk ograniczania pasma dla ruchu przychodzącego i ruchu wychodzącego
26. Wykrywanie i kontrolowanie ruch P2P poprzez identyfikację aplikacji typu P2P
27. Możliwość statycznej konfiguracji tzw. blacklisty jak i mechanizm dynamicznego wpisu adresów do blacklisty na podstawie wykrytych źródeł ataku oraz połączenie ACL z blacklistą.
28. Możliwość uruchomienia firewalla w trybie redundantnej pracy dla zwiększenie niezawodności. Możliwość pracy w trybie active/active oraz active/standby
29. Wsparcie dla mechanizm redundancji systemu (klaster urządzeń) w trybie routingu jak i transparentnym.
30. Wsparcie dla funkcjonalności Policy Based Routing (PBR).
31. Wsparcie dla protokołów tunelowania: SSL VPN, IPSec VPN, L2TP VPN, GRE VPN, L2TP over IPSec oraz GRE over IPSec.
32. Wsparcie dla mechanizmu redundancji dla połączeń IPSec VPN.
33. Wsparcie dla funkcjonalności IPS. Wykrywanie anomalii w różnych protokołach, w tym w: HTTP, SMTP, FTP, POP3, IMAP4, NETBIOS, SMB, MS_SQL, Telnet, IRC oraz DNS.
34. Wykrywanie rodzaju protokołu poprzez zawartość danych: HTTP, SMTP, FTP, POP3, IMAP4, MSRPC, NETBIOS, SMB, MSSQL, Telnet, IRC, TFTP, eMule oraz eDonkey.
35. Grupowanie sygnatur IPS na kategorie.
36. Możliwość definiowania sygnatur IPS przez użytkownika.
37. Automatyczna aktualizacja bazy sygnatur IPS poprzez sieć, definiowanie czasu aktualizacji, ręczna aktualizacja offline, przywracanie poprzedniej wersji.
38. Możliwość powiązania polityk IPS z regułami ACL i przypisania polityk IPS do strefy.
39. Możliwość włączania i wyłączania jednej lub wszystkich reguł IPS w polityce oraz konfiguracji rodzaju reakcji na zdarzenie.
40. Możliwość włączenia i wyłączenia funkcji IPS globalnie dla całego urządzenia.
41. Możliwe rodzaje reakcji na zdarzenie IPS: logowanie i blokowanie pakietów.
42. Wysyłanie logów z modułu IPS do zewnętrznego serwera oraz generowanie różnych rodzajów raportów umożliwiających sprawdzenie najczęściej występujących ataków, ich źródeł i przeznaczenia.
43. W zależności od ustawień przesłanie danych dalej lub blokada w przypadku przeciążenia modułu IPS.
44. Wsparcie dla funkcjonalności antywirus (AV).
    Skanowaniu różnych protokołów w celu wykrycia wirusów.
    Wsparcie dla wykrywania wirusów w plikach przesyłanych przez HTTP, SMTP, POP3, IMAP, NFS, SMB oraz FTP.
45. Dekompresja wielokrotnie skompresowanych plików od 2 do 8 poziomów w celu skanowania AV
46. Możliwość automatycznej aktualizacji bazy wirusów poprzez sieć, definiowanie czasu aktualizacji, ręczna aktualizacja offline, przywracanie poprzedniej wersji.
47. Możliwość wylistowania wirusów zawartych w bazie AV.
48. Możliwość usunięcia wirusa, wyświetlenie strony alarmującej, oznaczanie wiadomości mailowej oraz logowanie.
49. Możliwość powiązania polityk AC z regułami ACL i przypisania polityk AV do strefy.
50. Możliwość włączenia i wyłączenia funkcji AV globalnie dla całego urządzenia.
51. Możliwość wysyłania logów z modułu AV do serwera syslog. Możliwość wygenerowania raportów z modułu AV.
52. Możliwość przesłania ruchu danych dalej lub ich blokada w przypadku przeciążenia modułu AV.
53. Wsparcie dla funkcjonalności URL filtering.
    Obsługa dopasowywania wpisów w whitelist oraz blacklist w oparciu o prefiks, sufiks słowa kluczowego. Blacklist i whitelist mają wyższy priorytet niż kategoria URL. Whitelist ma wyższy priorytet niż blacklist.
54. Obsługa kategorii URL tworzonych przez użytkownika. Kategorie stworzone przez użytkownika mają wyższy priorytet od predefiniowanych kategorii.
55. Możliwość otrzymania kategorii URL z serwera kategorii dostępnego w sieci Internet. Reakcja podejmowana jest na podstawie skonfigurowanej polityki i przypisanej akcji do konkretnej grupy URL.
56. Możliwe reakcje modułu URL filtering - "zablokuj" lub "zezwól".
    Możliwość wyświetlenia częściowo spersonalizowanej strony informującej o zablokowaniu dostępu.
57. Polityka filtrowania URL może być oparta o grupę adresów i określony czas.
58. Możliwość filtrowania stron typu https w oparciu o kategorię bez konieczności deszyfrowania całej komunikacji
59. Funkcja logowania dostępu do adresów URL. Możliwość określenia osiągniętych zasobów.
60. Automatyczne generowanie polityk na podstawie analizy ruchu przechodzącego przez firewall.
61. Funkcjonalność wykrywaniu zdublowanych i nieużywanych polityk
62. Możliwość zarządzania urządzeniem przy wykorzystaniu protokołów HTTP i HTTPS, SSH, Telnet oraz z poziomu linii komend.
63. Możliwość tworzenia kopii zapasowych, eksportowania i przywracania konfiguracji.
64. Urządzenie musi posiadać wewnętrzny dysk twardy o pojemności minimum 240GB w celu logowania i tworzenia raportów dotyczących np.:
    - Analizy ruchu z uwzględnieniem nazwy użytkownika, adresu IP, rodzaju aplikacji, ilości transmitowanych danych
    - Statystyki dostępu do stron www z uwzględnieniem kategorii stron www oraz witryn www
    - Możliwość tworzenia cyklicznych raportów i wysyłania ich na wskazany adres e-mail

Zamawiający dopuszcza możliwość zaoferowania rozwiązania które funkcje logowania i raportowania wymagane powyżej będzie realizowało za pomocą zewnętrznego systemu. W takim przypadku należy zaoferować rozwiązanie z dedykowanym serwerem sprzętowym wyposażonym w dysk twardy z przestrzenią na logi o powierzchni minimum 240GB oraz wszystkimi niezbędnymi licencjami do prawidłowego działania. W przypadku zaoferowania zewnętrznego systemu raportującego wraz z serwerem Zamawiający wymaga, aby wszystkie element (typu sprzęt i oprogramowanie) objęte były identycznym wsparciem serwisowym jak oferowane firewalle

65. Firewalle muszą zostać dostarczone z 3 letnią licencją na funkcjonalności IPS/AV/URL Filtering
66. Zamawiający wymaga, aby firewalle posiadały 3 letni serwis gwarancyjny. Wymiana uszkodzonego elementu w trybie 8x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia
67. Dostarczone rozwiązanie musi być nowe, nie używane w żadnych innych projektach, zakupione w oficjalnym kanale sprzedaży. Zamawiający może podczas etapu dostawy żądać oświadczenia producenta bądź oficjalnego przedstawiciela na rynku Polskim o spełnieniu powyższego punktu.