*Załącznik nr 6 do SWZ*

Znak sprawy: **PCUW.261.2.26.2025**

|  |
| --- |
| **OPIS PRZEDMIOTU ZAMÓWIENIA** |

|  |
| --- |
| **Urządzenie typ D:**  **Zapora sieciowa UTM w ilości pięciu sztuk:** |
| **Charakterystyka (wymagania minimalne)**   1. Zapora sieciowa typu UTM, 2. Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku. 3. Minimalna ilość interfejsów:    * 1. 8 interfejsów RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa.      2. 2 interfejsy USB 3.0 dla przyszłych potrzeb i do podłączenia modemu Internetu mobilnego      3. 1 interfejs konsoli do zarządzania zaporą, 4. Zapora powinna posiadać możliwość montażu dysku o pojemności przynajmniej 256 GB, 5. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa, 6. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji, 7. Możliwość utworzenia przynajmniej 128 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q, 8. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej, 9. Minimalna ilość jednocześnie obsługiwanych połączeń: 750 000, 10. Możliwość obsłużenia przynajmniej 6 000 nowych połączeń w ciągu 1 sekundy. 11. Przepustowość urządzenia pracującego w trybie stateful firewall: nie niższa niż 2 Gbps – dla ramki 1518B zgodnie z RFC 2544, 12. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: nie niższa niż 1 Gbps, 13. Przepustowość urządzenia pracującego jako koncentrator VPN: nie niższa niż 750 Mbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544, 14. Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – nie niższa niż 750 Mbps, 15. Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 50, 16. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 2 z możliwością rozszerzenia do przynajmniej 50, 17. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 5 z możliwością rozszerzenia do przynajmniej 200, 18. Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne. 19. Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 300 Mbps oraz obsłużyć co najmniej 25 000 połączeń, 20. Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP, 21. Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site), 22. Wsparcie funkcjonalności IP Helper lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa), 23. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP, 24. Wsparcie dla Dynamicznego DNS tzw. DDNS, 25. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne, 26. Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez systemy automatyczne, takie jak np. „Google translate” (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio), 27. Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:     * 1. wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron),       2. wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony,       3. wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki. 28. Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps, 29. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL, 30. Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci, 31. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego, 32. Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN), 33. Kontrola dostępności zestawionych tuneli VPN, 34. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP. 35. Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty, 36. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić), 37. Funkcja NAT oparta o reguły bezpieczeństwa, 38. NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe), 39. Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych, 40. Zintegrowany system skanowania antyspyware, 41. Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www, 42. System IPS musi używać algorytmu szeregowego przetwarzania. 43. Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex), 44. Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji,     * 1. Bazy ww. systemów muszą być aktualizowane co najmniej raz dziennie,       2. Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur,       3. Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur. 45. System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików. 46. Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa, 47. Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi, 48. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p, 49. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń 50. Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Funkcjonalność nie może wymagać zakupu dodatkowych licencji. 51. Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss.   Funkcjonalność nie może wymagać zakupu dodatkowych licencji.   1. Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do minimum 16 takich punktów dostępowych sieci bezprzewodowej. 2. **Gwarancja: Min. 12 mc, wsparcie w trybie 24x7.** 3. **Wymagane licencje dostarczone z urządzeniem:** 4. Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres co najmniej 1 roku. 5. Licencja na oprogramowanie służące do przechowywania logów z systemu firewall i generowania na ich podstawie raportów. Oprogramowanie w formie maszyny wirtualnej powinno działać na oprogramowaniu Hyper-v/VMWare. Licencja powinna umożliwiać przechowywanie logów przez okres co najmniej jednego roku. Eksport danych z zapory sieciowej powinien odbywać się za pomocą protokołu SYSLOG. Licencja na okres co najmniej 1 roku. |
| **Urządzenie typ C:**  **Zapora sieciowa UTM w ilości jednej sztuk:** |
| **Charakterystyka (wymagania minimalne)**   1. Zapora sieciowa typu UTM, 2. Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku, 3. Minimalna ilość interfejsów: 4. 8 interfejsów RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa, 5. 2 interfejsy USB 3.0 dla przyszłych potrzeb i do podłączenia modemu Internetu mobilnego, 6. 1 interfejs konsoli do zarządzania zaporą, 7. Zapora powinna posiadać możliwość montażu dysku o pojemności przynajmniej 256 GB, 8. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa, 9. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji, 10. Możliwość utworzenia przynajmniej 128 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q, 11. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej, 12. Minimalna ilość jednocześnie obsługiwanych połączeń: 900 000, 13. Możliwość obsłużenia przynajmniej 9 000 nowych połączeń w ciągu 1 sekundy, 14. Przepustowość urządzenia pracującego w trybie stateful firewall: nie mniejsza niż 3 Gbps – dla ramki 1518B zgodnie z RFC 2544, 15. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: nie mniejsza niż 1,5 Gbps, 16. Przepustowość urządzenia pracującego jako koncentrator VPN: nie mniejsza niż 1,38 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544, 17. Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – nie niższa niż 1 Gbps, 18. Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 100, 19. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 2 z możliwością rozszerzenia do przynajmniej 100, 20. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 5 z możliwością rozszerzenia do przynajmniej 200, 21. Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne, 22. Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 500 Mbps oraz obsłużyć co najmniej 30 000 połączeń, 23. Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP, 24. Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site), 25. Wsparcie funkcjonalności IP Helper lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa), 26. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP, 27. Wsparcie dla Dynamicznego DNS tzw. DDNS, 28. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne. 29. Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez systemy automatyczne, takie jak np. „Google translate” (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio) , 30. Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak: 31. wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron), 32. wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony, 33. wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki. 34. Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps, 35. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL. 36. Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci. 37. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego, 38. Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN), 39. Kontrola dostępności zestawionych tuneli VPN, 40. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP, 41. Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty, 42. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić), 43. Funkcja NAT oparta o reguły bezpieczeństwa, 44. NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe), 45. Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych, 46. Zintegrowany system skanowania antyspyware, 47. Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www, 48. System IPS musi używać algorytmu szeregowego przetwarzania, 49. Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex). 50. Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji, 51. Bazy ww. systemów muszą być aktualizowane co najmniej raz dziennie. 52. Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur, 53. Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur, 54. System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików, 55. Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa, 56. Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi, 57. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p, 58. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń 59. Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Funkcjonalność nie może wymagać zakupu dodatkowych licencji, 60. Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss.   Funkcjonalność nie może wymagać zakupu dodatkowych licencji,   1. Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do minimum 16 takich punktów dostępowych sieci bezprzewodowej.   **Gwarancja: Min. 12 mc, wsparcie w trybie 24x7.**  **Wymagane licencje dostarczone z urządzeniem:**   1. Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres co najmniej 1 roku, 2. Licencja na oprogramowanie służące do przechowywania logów z systemu firewall i generowania na ich podstawie raportów. Oprogramowanie w formie maszyny wirtualnej powinno działać na oprogramowaniu Hyper-v/VMWare. Licencja powinna umożliwiać przechowywanie logów przez okres co najmniej jednego roku. Eksport danych z zapory sieciowej powinien odbywać się za pomocą protokołu SYSLOG. Licencja na okres co najmniej 1 roku. |
| **Urządzenie typ B:**  **Zapora sieciowa UTM w ilości trzech sztuk** |
| **Charakterystyka (wymagania minimalne)**   1. Zapora sieciowa typu UTM 2. Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku. 3. Minimalna ilość interfejsów: 4. 2 interfejsy 2,5G SFP+, 5. 8 interfejsów RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa. 6. 2 interfejsy USB 3.0 dla przyszłych potrzeb i do podłączenia modemu Internetu mobilnego, 7. 1 interfejs konsoli do zarządzania zaporą, 8. Zapora powinna posiadać możliwość montażu dysku o pojemności przynajmniej 256 GB, 9. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa, 10. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji, 11. Możliwość utworzenia przynajmniej 128 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q, 12. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej, 13. Minimalna ilość jednocześnie obsługiwanych połączeń: 1 000 000, 14. Możliwość obsłużenia przynajmniej 12 000 nowych połączeń w ciągu 1 sekundy, 15. Przepustowość urządzenia pracującego w trybie stateful firewall: nie niższa niż 3,5 Gbps – dla ramki 1518B zgodnie z RFC 2544, 16. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: nie niższa niż 2 Gbps, 17. Przepustowość urządzenia pracującego jako koncentrator VPN: nie niższa niż 1,5 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544, 18. Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – nie niższa niż 1,5 Gbps, 19. Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 150, 20. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 2 z możliwością rozszerzenia do przynajmniej 150, 21. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 5 z możliwością rozszerzenia do przynajmniej 200, 22. Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne, 23. Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 600 Mbps oraz obsłużyć co najmniej 35 000 połączeń, 24. Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP, 25. Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site), 26. Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa), 27. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP, 28. Wsparcie dla Dynamicznego DNS tzw. DDNS, 29. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne, 30. Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez systemy automatyczne, takie jak np. „Google translate” (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio), 31. Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak: 32. wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron), 33. wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony, 34. wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki, 35. Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps, 36. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL, 37. Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci, 38. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego, 39. Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN), 40. Kontrola dostępności zestawionych tuneli VPN, 41. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP, 42. Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty, 43. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić), 44. Funkcja NAT oparta o reguły bezpieczeństwa, 45. NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe), 46. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p, 47. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń, 48. Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss.   Funkcjonalność nie może wymagać zakupu dodatkowych licencji,   1. Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 32 takich punktów dostępowych sieci bezprzewodowej,   **Gwarancja: Min. 12 mc, wsparcie w trybie 24x7.**  **Wymagane licencje dostarczone z urządzeniem:**   1. Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres co najmniej 1 roku, 2. Licencja na oprogramowanie służące do przechowywania logów z systemu firewall i generowania na ich podstawie raportów. Oprogramowanie w formie maszyny wirtualnej powinno działać na oprogramowaniu Hyper-v/VMWare. Licencja powinna umożliwiać przechowywanie logów przez okres jednego roku. Eksport danych z zapory sieciowej powinien odbywać się za pomocą protokołu SYSLOG. Licencja na okres co najmniej 1 roku. |
| **Urządzenie typ A:**  **Zapora sieciowa UTM w ilości jednej sztuki** |
| 1. **Charakterystyka (wymagania minimalne)** 2. Zapora sieciowa typu UTM, 3. Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku, 4. Minimalna ilość interfejsów: 5. 2 interfejsów 10 GbE SFP+, 6. 8 interfejsów RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa, 7. 2 interfejsy USB 3.0 dla przyszłych potrzeb i do podłączenia modemu Internetu mobilnego, 8. 1 interfejs konsoli do zarządzania zaporą, 9. Zapora powinna posiadać wbudowany dysk o wielkości minimum 32 GB oraz możliwość montażu dysku o pojemności przynajmniej 256 GB, 10. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa, 11. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji, 12. Możliwość utworzenia przynajmniej 256 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q, 13. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej, 14. Minimalna ilość jednocześnie obsługiwanych połączeń: 1 500 000, 15. Możliwość obsłużenia przynajmniej 25 000 nowych połączeń w ciągu 1 sekundy, 16. Przepustowość urządzenia pracującego w trybie stateful firewall: nie mniejsza niż 5 Gbps – dla ramki 1518B zgodnie z RFC 2544, 17. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: nie mniejsza niż 3 Gbps, 18. Przepustowość urządzenia pracującego jako koncentrator VPN: nie mniejsza niż 2,1 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544, 19. Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – nie mniejsza niż 2,5 Gbps, 20. Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 250, 21. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 2 z możliwością rozszerzenia do przynajmniej 250 22. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 10 z możliwością rozszerzenia do przynajmniej 500. 23. Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne, 24. Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 800 Mbps oraz obsłużyć co najmniej 75 000 połączeń, 25. Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP, 26. Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site), 27. Wsparcie funkcjonalności IP Helper lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa), 28. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP, 29. Wsparcie dla Dynamicznego DNS tzw. DDNS, 30. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne, 31. Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez systemy automatyczne, takie jak np. „Google translate” (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio), 32. Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak: 33. wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron), 34. wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony, 35. wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki, 36. Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps, 37. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL, 38. Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci, 39. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego. 40. Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN), 41. Kontrola dostępności zestawionych tuneli VPN, 42. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP. 43. Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty, 44. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić), 45. Funkcja NAT oparta o reguły bezpieczeństwa, 46. NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe), 47. Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych, 48. Zintegrowany system skanowania antyspyware, 49. Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www, 50. System IPS musi używać algorytmu szeregowego przetwarzania, 51. Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex), 52. Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji, 53. Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie. 54. Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur, 55. Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur, 56. System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików, 57. Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa, 58. Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi, 59. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p, 60. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń, 61. Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Funkcjonalność nie może wymagać zakupu dodatkowych licencji, 62. Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss.   Funkcjonalność nie może wymagać zakupu dodatkowych licencji,   1. Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 32 takich punktów dostępowych sieci bezprzewodowej. 2. **Gwarancja: Min. 12 mc, wsparcie w trybie 24x7.** 3. **Wymagane licencje dostarczone z urządzeniem:** 4. Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres co najmniej 1 roku, 5. Licencja na oprogramowanie służące do przechowywania logów z systemu firewall i generowania na ich podstawie raportów. Oprogramowanie w formie maszyny wirtualnej powinno działać na oprogramowaniu Hyper-v/VMWare. Licencja powinna umożliwiać przechowywanie logów przez okres co najmniej jednego roku. Eksport danych z zapory sieciowej powinien odbywać się za pomocą protokołu SYSLOG. Licencja na okres co najmniej 1 roku. |

Wszystkie oferowane urządzenia muszą posiadać jednolity, graficzny interfejs zarządzania oraz jednolity interfejs CLI, zapewniający identyczną składnię komend oraz sposób konfiguracji na wszystkich urządzeniach objętych zamówieniem.