Znak sprawy: I.271.10.2023

*Załącznik Nr 5 do SWZ*

**Szczegółowy opis przedmiotu zamówienia**

**I. Część I**

|  |
| --- |
| Spis przedmiotu zamówienia:   1. Komputery Osobiste (4szt) 2. Komputery stacjonarne (32 szt) 3. Monitor 27” (32 szt) 4. Pakiet Aplikacji Biurowych (5 szt) 5. UTM wraz z licencjami Typ 1 (1 szt) 6. UTM wraz z licencjami Typ 2 (6 szt.) 7. UPS (22 szt.) 8. Oprogramowanie Antywirusowe (80 licencji) 9. Wdrożenie UTM 10. Modernizacja sieci LAN |

1. **Komputery osobiste (4 szt)**

|  |  |  |
| --- | --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne | Wypełnia Wykonawca  (opisać zastosowane rozwiązanie, podać parametry techniczne)\* |
| TYP | * Komputer przenośny z zainstalowanym systemem operacyjnym WIN 11 PRO | *Należy podać producenta, model urządzenia i rok produkcji.*  *………………………….*  spełnia/nie spełnia  …………………………. |
| Gwarancja Producenta | * Min. 36 miesięcy | *spełnia/nie spełnia*  *………………………….* |
| Procesor | * Processor osiągający w testach cpubenchmark passmark minimum 15 125 punktów | *spełnia/nie spełnia*  *………………………….* |
| Pamięć RAM | * Minimum 8 GB DDR4 SDRAM / szybkość min. 3200 MHz   Możliwość rozbudowy do 16 GB RAM | *spełnia/nie spełnia*  *………………………….* |
| Dyski Twarde | * Minimum 512 GB SSD M.2 PCIe - NVM Express | *spełnia/nie spełnia*  *………………………….* |
| Wyświetlacz | * Przeciwoślepieniowy, Szeroki Kąt Patrzenia, kąt patrzenia w poziomie ±80°, kąt patrzenia w pionie ±80°, Wyświetlacz z Wąską Ramką, czas reakcji 35 ms, wielkość piksela 0,17925 mm | *spełnia/nie spełnia*  *………………………….* |
| Jasność Obrazu | 250 cd/m2 | *spełnia/nie spełnia*  *………………………….* |
| Częstotliwość synchr. pionowej przy maks. rozdzielczości: | * 120 Hz | *spełnia/nie spełnia*  *………………………….* |
| Gęstość pikseli (ppi): | * 141 | *spełnia/nie spełnia*  *………………………….* |
| Paleta Kolorów | * 45% NTSC | *spełnia/nie spełnia*  *………………………….* |
| Wielkość przekątnej Ekaranu | * 15,6” - IPS | *spełnia/nie spełnia*  *………………………….* |
| Rozdzielczość Ekranu | * MIN. 1920x1080 (Full HD) | *spełnia/nie spełnia*  *………………………….* |
| Współczynnik kształtu Obrazu | * 16:9 | *spełnia/nie spełnia*  *………………………….* |
| Dźwięk | * Głośniki stereo i mikrofon, dźwięk wysokiej rozdzielczości | *spełnia/nie spełnia*  *………………………….* |
| Aparat fotograficzny | CMOS 30 klatek/sek | *spełnia/nie spełnia*  *………………………….* |
| Czytnik kart pamięci: | Tak (Karta Pamięci SD, karta SDHC, karta SDXC) | *spełnia/nie spełnia*  *………………………….* |
| Bateria | * Min. 3 ogniwa litowo-polimerowe, 41 Wh | *spełnia/nie spełnia*  *………………………….* |
| Interface sieciowy / Bezprzewodowy | * Bluetooth 5.0, WiFI 802.11a/b/g/n/ac + Gigabit Ethernet / | *spełnia/nie spełnia*  *………………………….* |
| Interfacey i rozszerzenia | * HDMI * USB-C 3.2 Gen 1 * USB 3.2 Gen 1 * USB 2.0 * LAN (RJ-45) * Słuchawki/mikrofon combo jack | *spełnia/nie spełnia*  *………………………….* |
| Waga | * Maksymalnie 1,9 kg | *spełnia/nie spełnia*  *………………………….* |
| Ochrona | * Czytnik odcisków Palców, * Trusted Platform Module (TPM 2.0) Security Chip, * Aluminiowa obudowa * Gniazdo bezpieczeństwa Noble Wedge | *spełnia/nie spełnia*  *………………………….* |

1. **Komputery stacjonarne (32 szt)**

|  |  |  |  |
| --- | --- | --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne | | Wypełnia Wykonawca  (opisać zastosowane rozwiązanie, podać parametry techniczne)\* |
| TYP | * Komputer stacjonarny z zainstalowanym systemem operacyjnym WIN 11 PRO | *Należy podać producenta serwera, model urządzenia i rok produkcji.*  *………………………….*  spełnia/nie spełnia  …………………………. | |
| Gwarancja Producenta | * Min. 36 miesięcy | *spełnia/nie spełnia*  *………………………….* | |
| Procesor | * Processor osiągający w testach cpubenchmark passmark minimum 19530 punktów * Minimum 6 core | *spełnia/nie spełnia*  *………………………….* | |
| Pamięć RAM | * Minimum 8 GB DDR4 SDRAM / szybkość min. 3200 MH * Możliwość rozbudowy do 64GB | *spełnia/nie spełnia*  *………………………….* | |
| Dyski Twarde | * Minimum 256 GB SSD M.2 PCIe NVM Express * Minimum 1TB 7200 obr/min Serial ATA | *spełnia/nie spełnia*  *………………………….* | |
| Czytnik kart Pamięci | Karta pamięci SD, karta pamięci SDHC, Karta Pamięci SDXC | *spełnia/nie spełnia*  *………………………….* | |
| Interfejsy wideo: | HDMI, DisplayPort | *spełnia/nie spełnia*  *………………………….* | |
| Wyjście sygnału audio | * Dźwięk Wysokiej Rozdzielczości | *spełnia/nie spełnia*  *………………………….* | |
| Klawiatura | * Klawiatura przewodowa USB | *spełnia/nie spełnia*  *………………………….* | |
| Mysz | * Mysz optyczna USB | *spełnia/nie spełnia*  *………………………….* | |
| Interface sieciowy przewodowy i Bezprzewodowy | * Ethernet, Fast Ethernet, Gigabit Ethernet, IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, Bluetooth 5.0 * Zgodność z normami IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, Bluetooth 5.0 | *spełnia/nie spełnia*  *………………………….* | |
| Rozszerzenie / połączenie: Sloty | * 1 (całkowity) / 0 (wolna) x M.2 Card - 2230/2280 (na SSD) * 1 (całkowity) / 0 (wolna) x M.2 Card - 2230 (zgodność z modułami bezprzewodowymi) * 1 (całkowity) / 1 (wolna) x PCIe x16 - połowa wysokości * 1 (całkowity) / 1 (wolna) x PCIe x1 - połowa wysokości | *spełnia/nie spełnia*  *………………………….* | |
| Interfejsy | * 1 x słuchawki/mikrofon (1 z przodu) * 4 x USB 3.2 Gen 1 (2 z przodu) * 4 x USB 2.0 (2 z przodu) * 1 x LAN (Gigabit Ethernet) - RJ-45 * 1 x DisplayPort 1.4 * 1 x HDMI * 1 x wyjście liniowe audio | *spełnia/nie spełnia*  *………………………….* | |
| Certyfikat ENERGY STAR: | TAK | *spełnia/nie spełnia*  *………………………….* | |
|  |  |  | |

1. **Monitor (32 szt)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nazwa komponentu | | Wymagane minimalne parametry techniczne | Wypełnia Wykonawca  (opisać zastosowane rozwiązanie, podać parametry techniczne)\* | |
| TYP | * Monitor LCD z podświetleniem LED / matryca aktywna TFT | | | *Należy podać producenta serwera, model urządzenia i rok produkcji.*  *………………………….*  spełnia/nie spełnia  …………………………. |
| Gwarancja Producenta | * Min. 36 miesięcy | | | *spełnia/nie spełnia*  *………………………….* |
| Klasa energii: | * D lub wyżej | | | *spełnia/nie spełnia*  *………………………….* |
| Wielkość przekątnej: | * Min 27” | | | *spełnia/nie spełnia*  *………………………….* |
| Technologia Adaptive-Sync: | * AMD FreeSync | | | *spełnia/nie spełnia*  *………………………….* |
| Typ panela: | IPS | | | *spełnia/nie spełnia*  *………………………….* |
| Współczynnik kształtu: | 16:9 | | | *spełnia/nie spełnia*  *………………………….* |
| Rozdzielczość natywna: | * Full HD (1080p) 1920 x 1080 przy 75 Hz | | | *spełnia/nie spełnia*  *………………………….* |
| Rozstaw pikseli: | * 0.3114 mm | | | *spełnia/nie spełnia*  *………………………….* |
| Jasność: | * 300 cd/m² | | | *spełnia/nie spełnia*  *………………………….* |
| Współczynnik kontrastu: | * 1000:1 | | | *spełnia/nie spełnia*  *………………………….* |
| Paleta Kolorów: | * 72% NTSC (CIE 1931) | | | *spełnia/nie spełnia*  *………………………….* |
| Czas reakcji: | * 4 ms (szary-do-szarego, wartość ekstremalna) | | | *spełnia/nie spełnia*  *………………………….* |
| Poziomy i pionowy kąt widzenia: | 178 stopni | | | *spełnia/nie spełnia*  *………………………….* |
| Powłoka ekranu: | Antyrefleksyjna, 3H Hard Coating | | | *spełnia/nie spełnia*  *………………………….* |
| Interfejsy: | 2 x HDMI (HDCP 1.4)  Wyjście audio | | | *spełnia/nie spełnia*  *………………………….* |
| Regulacja pozycji ekranu: | Odchylenie kąt -5/+21 | | | *spełnia/nie spełnia*  *………………………….* |

1. **Pakiet Aplikacji Biurowych (5 szt.)**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Oprogramowane | Pakiet aplikacji biurowych MS Office zawierający moduły: Word, Excel, Powerpoint, Outlook lub pakiet równoważny.  Pakiet musi być dostarczony z licencją bezterminową, w najnowszej dostępnej wersji, do użycia komercyjnego domowego lub biznesowego. | Wymagane jest podanie producenta, pełnej nazwy i wersji oprogramowania.  ………………………..  spełnia/nie spełnia  …………………………. |

1. **UTM wraz z licencjami (1 szt)**

|  |  |  |  |
| --- | --- | --- | --- |
| Nazwa komponentu | Wymagane ogólne parametry techniczne | Wypełnia Wykonawca  (opisać zastosowane rozwiązanie, podać parametry techniczne)\* | |
| TYP | UTM typ I | | *Należy podać producenta serwera, model urządzenia i rok produkcji.*  *………………………….*  spełnia/nie spełnia  …………………………. |

# Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

# Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

# Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

* 10 portami Gigabit Ethernet RJ-45.

1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

# Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

# Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

# Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

* Amazon Web Services (AWS).
* Microsoft Azure.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

# Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

# Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

# Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

# Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

# Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

# Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

# Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

# Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

# Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

# Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

# Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

# Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

# Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

b)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

# Gwarancja oraz wsparcie

1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania w trybie 24x7.
2. **UTM wraz z licencjami (6 szt)**

|  |  |  |  |
| --- | --- | --- | --- |
| Nazwa komponentu | Wymagane ogólne parametry techniczne | Wypełnia Wykonawca  (opisać zastosowane rozwiązanie, podać parametry techniczne)\* | |
| TYP | UTM typ II | | *Należy podać producenta serwera, model urządzenia i rok produkcji.*  *………………………….*  spełnia/nie spełnia  …………………………. |

# Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

# Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

# Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

* 5 portami Gigabit Ethernet RJ-45.

1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

# Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

# Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

# Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

* Amazon Web Services (AWS).
* Microsoft Azure.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

# Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

# Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

# Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

# Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

# Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

# Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

# Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

# Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

# Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

# Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

# Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

# Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

# Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

 Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [12] miesięcy.

# Gwarancja oraz wsparcie

1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania w trybie 24x7.
2. **UPS (22 szt)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nazwa komponentu** | | | **Wymagane minimalne parametry techniczne** | **Wypełnia Wykonawca**  **(opisać zastosowane rozwiązanie, podać parametry techniczne)\*** | |
| TYP | | UPS | *Należy podać producenta serwera, model urządzenia i rok produkcji.*  *………………………….* |
| TYP oraz MOC | * UPS zewnętrzny 1000VA | | *spełnia/nie spełnia*  *………………………….* |
| Zakres Napięcia Wejściowego | * 170 - 280 V | | *spełnia/nie spełnia*  *………………………….* |
| Nominalne Napięcie Wyjściowe | * 230 VAC | | *spełnia/nie spełnia*  *………………………….* |
| Częstotliwość wyjściowa | * 50/60 Hz ± 1% | | *spełnia/nie spełnia*  *………………………….* |
| Wymagana częstotliwość | * 50 - 60 Hz ± 5% | | *spełnia/nie spełnia*  *………………………….* |
| Złącza wejściowe | * 1 | | *spełnia/nie spełnia*  *………………………….* |
| Rodzaje złącz wyjściowych zasilania | * 4 x zasilanie IEC 60320 C13 (UPS i przepięciowe) - 230 V | | *spełnia/nie spełnia*  *………………………….* |
| Napięcie wyjściowe: | * AC 230 V ± 10% - 50/60 Hz | | *spełnia/nie spełnia*  *………………………….* |
| Kształt fali wyjściowej: | * Krokowa aproksymacja sinusoidy | | *spełnia/nie spełnia*  *………………………….* |
| Zabezpieczenie obwodu: | * Odcięcie obwodu | | *spełnia/nie spełnia*  *………………………….* |
| Technologia Baterii: | * Kwasowo-ołowiowy, napięcie wyjściowe 12V, pojemność min 9Ah | | *spełnia/nie spełnia*  *………………………….* |
| Charakterystyka dodatkowa | * Do montowania na ścianie, alarm dźwiękowy, wyświetlacz LED, ochrona przed przegrzaniem, Automatyczna regulacja napięcia (AVR), ochrona nadnapięciowa, ochrona przed przeciążeniem, zabezpieczenie podnapięciowe, automatyczne samotestowanie, Inteligentne Zarządzanie Akumulatorem | | *spełnia/nie spełnia*  *………………………….* |

1. **Oprogramowanie antywirusowe (80 szt.)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nazwa komponentu** | | **Wymagane minimalne parametry techniczne** | **Wypełnia Wykonawca**  **(opisać zastosowane rozwiązanie, podać parametry techniczne)\*** | |
| TYP | Oprogramowanie antywirusowe | *Należy podać producenta oprogramowania, rodzaj.*  *………………………….*  spełnia/nie spełnia  …………………………. |

Rozszerzenie posiadanych licencji do liczby 80 szt na okres 12-u miesięcy

1. **Wdrożenie UTM**

Wymagane jest wdrożenie Urządzeń sieciowych UTM w siedzibie Zamawiającego oraz w **poszczególnych lokalizacjach** wskazanych przez Zamawiającego polegające na wdrożeniu **niezbędnych polityk firewall** na podstawie **wytycznych Zamawiającego** z uwzględnieniem adresacji IP interfejsów LAN/DMZ oraz WAN.

- Uruchomienie usług sieciowych usług aplikacji i zbirów aplikacji.

- Uruchomienie translacji adresów NAT/PAT

- Wydzielenie stref bezpieczeństwa DMZ

- Uruchomienie Rejestrowania Zdarzeń

- Uruchomienie tuneli IPSEC-VPN ze wszystkimi urządzeniami (7 szt)

- Wykreowanie połączeń SSL-VPN do istniejących użytkowników systemu zdalnych połączeń

- Połączenie do domeny i umożliwienie logowania SSO na podstawie grupy

1. **Modernizacja sieci LAN**

Rozbudowa i modernizacja sieci LAN w budynku Urzędu Miasta i Gminy w Białobrzegach - Plac Zygmunta Starego 9

Zakres prac:

* Wykonanie nowej sieci LAN na terenie budynku Urzędy Gminy – w szczególności:
  + konstrukcję tras kablowych
  + instalację gniazd
  + układanie kabli miedzianych oraz światłowodowych
  + terminowanie kabli w modułach
  + terminowanie kabli światłowodowych w modułach
  + montaż punktów dystrybucyjnych wraz z panelami, organizerami
  + uruchomienie sieci
* Wykonanie sieć musi być poprzedzone wizją lokalną oraz projektem (koncepcją) budowanej sieci będące następnie częścią dokumentacji powykonawczej sieci.
* Pomoc przy przełączeniu urządzeń gminy na nową sieć – przełączenia musi się odbywać tak, żeby nie zakłócić pracy Urzędu.

Założenia:

* Sieć będzie obejmować piwnicę (3 podwójne gniazda RJ), parter (14 podwójnych gniazd RJ), piętro 1 (13 podwójnych gniazd RJ) , piętro 2 (12 podwójnych gniazd RJ), piętro 3 (12 podwójnych gniazd RJ). Łączna ilość gniazd: 108 (54 podwójnych).
* Całe okablowanie miedziane oraz pasywne elementy sieci będą kat.6
* Sieć będzie podzielona na 2 fizyczne segmenty w ramach których będzie zastosowane „poziome” okablowanie miedziane.
* Każdy segment będzie posiadał dedykowaną szafę telekomunikacyjnej w standardzie 19’’. Każda z tych szaf będzie zbierała okablowanie dla danego piętra/pięter: szafa na 2 piętrze – okablowanie dla pietra 3 i 2, szafa na 1 piętrze – okablowanie dla pietra 1, parteru i piwnicy.
* Obie szafy będą miały połączenie światłowodowe z piwnicą gdzie jest istniejąca szafa serwerowa.
* Szafa na 1p Urzędu będzie wysokości 42U i będzie zamieniała istniejącą szafę Urzędu.
* Szafy dla każdego z segmentów sieci będą wyposażone w panele krosownicze RJ45, panele krosownicze światłowodowe, organizery kabli.
* Każda z szaf (segmenty sieci) będzie posiadała dedykowane zasilanie poprowadzone z piwnicy i zakończone listwą zasilającą
* Okablowanie światłowodowe będzie zapewniało nadmiarowość połączeń dla realizacji różnych połączeń fizycznych w ramach sieci LAN.
* Gmina posiada 3 urządzenia aktywne sieci wyposażone w gniazda SFP+ dla których należy dostarczyć moduły SFP+ dla realizacji połączeń światłowodowych.
* Nowa sieć będzie maksymalnie wykorzystywała istniejące listwy i trasy kablowe.
* Należy zapewnić możliwość wydzielenia fizycznego fragmentu sieci dla systemu obsługującego dowody osobiste
* Wykonawca wykona wszelkie konieczne prace oraz zapewni wszelkie konieczne materiały i narzędzia do kompletnego wykonania sieci LAN.
* Każdorazowo prace należy uzgadniać z Zamawiającym, ponieważ mogą być wykonywane po godzinach pracy lub w weekendy

\* Prawą stronę tabeli, należy wypełnić stosując słowa „spełnia” lub „nie spełnia”, zaś w przypadku wyższych wartości niż minimalne-wykazane w tabeli należy wpisać oferowane wartości techniczno-użytkowe. W przypadku, gdy Wykonawca w którejkolwiek z pozycji wpisze słowa „nie spełnia” lub zaoferuje niższe wartości oferta zostanie odrzucona, gdyż jej treść jest niezgodna z warunkami zamówienia (art. 226 ust. 1 pkt 5 ustawy PZP ).

……..…………………...

(miejscowość, data)

**/podpisano elektronicznie/\***

**\* UWAGA: oświadczenie należy podpisać kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym osoby uprawnionej do zaciągania zobowiązań w imieniu Wykonawcy.**