**Załącznik nr 5**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

***Zadanie nr 1***

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa** | **Opis** | **ilość** |
| **1.** | **Monitor Biurowy** | |  |  | | --- | --- | | Model | **Monitor Biurowy** | | Przekątna ekranu | **27"** | | Proporcje obrazu | **16:9** | | Rozdzielczość | **1920 x 1080 (FHD 1080)** | | Technologia podświetlania | **Diody LED** | | Typ matrycy | **TFT IPS** | | Częstotliwość odświeżania | **100Hz** | | Powierzchnia matrycy | **Matowa** | | Ilość kolorów | **16,7 mln** | | Ekran dotykowy | **Nie** | | Czas reakcji | **0.4ms** | | Jasność | **250cd/m²** | | Plamka matrycy | **0.311mm** | | Kontrast dynamiczny | **80 000 000:1** | | Kontrast statyczny | **1 300:1** | | Kąt widzenia poziomy | **178°** | | Kąt widzenia pionowy | **178°** | | Częstotliwość pozioma min. | **31kHz** | | Częstotliwość pozioma max. | **115kHz** | | Obszar widzialny w pionie | **336.3mm** | | Obszar widzialny w poziomie | **597.9mm** | | Standard VESA | **100 x 100** | | Pobór mocy | **17W** | | Klasa energetyczna | **E** | | Etykieta energetyczna |  | | Regulacja wysokości | **Tak** | | Wbudowane głośniki | **Tak** | | Kamera internetowa | **Brak** | | Wbudowany tuner TV | **Nie** | | Pivot | **Tak** | | Bluetooth | **Nie** | | WiFi | **Nie** | | Gniazda we/wy | **1 x DisplayPort**  **1 x HDMI**  **1 x Audio out**  **4 x USB 3.2 Type-A Gen 1** | | Certyfikaty | **CE**  **RoHS**  **TCO**  **TUV**  **VCCI**  **EAC**  **PSE**  **ErP**  **WEEE**  **REACH**  **UKCA** | | Akcesoria w zestawie | * **Kable: zasilający, USB, HDMI, DP** * **Pozostałe: skrócona instrukcja obsługi, instrukcja bezpieczeństwa** | | Kolor | **Czarny** | | Szerokość | **612.5mm** | | Głębokość z podstawą | **209.5mm** | | Wysokość z podstawą | **394mm** | | Waga z podstawą | **5.7kg** | | Okres gwarancji | **36 miesięcy** | | **2 szt.** |
| **2.** | **Projektor Laserowy** | |  |  | | --- | --- | | Typ projektora | Bezlampowy - Laserowy, Biznes i edukacja, Instalacyjny | | Jasność | 5000 ANSI lumenów | | Kontrast | 3000000:1 | | Rozdzielczość | 1920 x 1080 (Full HD) | | Żywotność źródła światła | 20000 h (pełna jasność) / 30000 h (Eco) | | Poziom hałasu | 32 dB (normalny) / 26 dB (tryb Eco) | | Zoom optyczny / cyfrowy | 1.3x / 0.8x–2.0x | | Keystone | ±30° (pionowo) | | Współczynnik odległości | 1.13–1.47 | | Obiektyw | F=2.43–2.78, f=16.90–21.61mm | | Wielkość obrazu | 30″ – 300″ | | Zużycie energii | 210W (tryb normalny) | | Porty | HDMI x2, RS232, USB-A (5V/1.5A), Audio Out | | Funkcje | Projekcja 360°, Tryb portretowy, Zoom cyfrowy |   W zestawie: Baterie do pilota, Pilot sterowania, Przewód zasilający  Gwarancja na źródło światła: 3 lata lub 20 000h w zależności, które minie pierwsze  Kalkulator projekcji:  Projektor ma dawać obraz o wymiarach: Szerokość 221 cm, Wysokość 124 cm, Przekątna 253 cm z odległości od **250** do **325** cm od powierzchni projekcyjnej. Liczone do obiektywu. | **1 szt.** |
| **3.** | **Urządzenie Wielofunkcyjne mono, laser wraz z dodatkowym tonerem.** | |  |  | | --- | --- | | **Prędkość druku w czerni (ISO, A4)** | Do 40 str./min | | Wydruk pierwszej strony w czerni (A4, po wyjściu ze stanu gotowości) | W ciągu zaledwie 6,3 s | | Normatywny cykl pracy (miesięcznie, format A4) | Do 80 000 stron | | Zalecana ilość stron drukowanych miesięcznie | 750 do 4000 | | Technologia druku | Urządzenia laserowe | | Jakość druku w czerni (tryb best) | Precyzyjne linie (1200 × 1200 dpi) | | Wyświetlacz | 2.7" (6.86 cm) intuitive color touchscreen (CGD) | | Możliwość druku mobilnego | Apple AirPrint™ Certyfikat Mopria™ Funkcja drukowania Wi-Fi® Direct | | Łączność, tryb standardowy | 1 port USB z przodu 1 port sieciowy Gigabit Ethernet 10/100/1000 Base-T 1 port Hi-Speed USB 2.0 (host) 1 karta Wi-Fi 802.3az Łączność radiowa 802.11b/g/n (2,4 GHz) Wi-Fi | | Zgodne systemy operacyjne | Windows 11 Windows 10 Klient systemu Windows Android Ios Mobilny system operacyjny macOS 10.15 Catalina macOS 11 Big Sur macOS 12 Monterey macOS 13 Ventura macOS 15 Sekwoja Chrome OS | | Pamięć | 512 MB | | Maksymalna wielkość pamięci | 512 MB | | **Wewnętrzna pamięć masowa** | Nie | | **Standardowa pojemność podajnika papieru** | Podajnik 1 na 100 arkuszy, podajnik 2 na 250 arkuszy, automatyczny podajnik dokumentów (ADF) na 50 arkuszy | | Podajnik papieru, opcj. | Opcjonalny trzeci podajnik na 550 arkuszy | | Standardowa pojemność odbiornika papieru | Odbiornik papieru na 150 arkuszy | | Drukowanie dwustronne | Automatycznie (wartość domyślna) | | Podawanie nośników, wykańczanie dokumentów | Skaner szczelinowy | | Obsługiwane formaty nośników | Podajnik 1: A4 A5 A6 B5 (JIS) Oficio (216 × 340 mm) 16K (195 × 270 mm) 16K (184 × 260 mm) 16K (197 × 273 mm) Pocztówka japońska Podwójna obrócona pocztówka japońska Koperta nr 10 Koperta Monarch Koperta B5 Koperta C5 Koperta DL Formaty niestandardowe 4 × 6 cali 5 × 8 cali Statement Podajniki 2 i 3: A4 A5-R B6 (JIS) | | Nośniki | Papier (zwykły, EcoEFFICIENT, cienki, gruby, typu bond, kolorowy, firmowy, z nadrukiem, dziurkowany, makulaturowy, szorstki) koperty etykiety | | **Typ skanera** | Skaner płaski, automatyczny podajnik dokumentów | | **Rozdzielczość skanowania, optyczna** | Maks. 1200 × 1200 dpi | | Format skanowania, maksymalny | 216 x 297 mm | | Maks. format skanowania (automatyczny podajnik dokumentów) | 216 x 356 mm | | Dwustronne skanowanie z automatycznego podajnika dokumentów | Tak | | Pojemność automatycznego podajnika dokumentów | Standardowo, 50 arkuszy | | Prędkość kopiowania (w czerni, tryb normal, format A4) | Maks. 38 kopii/min | | Rozdzielczość kopii (tekst w czerni) | Do 600 × 600 dpi | | Rozdzielczość kopiowania (tekst i grafika w kolorze) | Do 600 × 600 dpi | | Ograniczenie liczby kopii/poszerzenie ustawień | 25 do 400% | | Etykiety ekologiczne | Deklaracja IT ECO Blue Angel | | Certyfikat Blue Angel | Tak, Blue Angel DE-UZ 219 – gwarancja tylko przy korzystaniu z oryginalnych materiałów eksploatacyjnych | | Specyfikacje dotyczące zrównoważonego wpływu | Możliwość recyklingu w ramach programu producenta Zgodność z akcesoriami ułatwiającymi dostęp Zawiera pokonsumenckie tworzywa sztuczne pochodzące z recyklingu | | **Zakres temperatur podczas eksploatacji** | Od 10 do 32,5°C | | **Dopuszczalna wilgotność względna podczas eksploatacji** | Wilgotność względna od 30 do 70% | | **Certyfikat Energy Star** | Nie | | Certyfikaty i normy | RCM (Australia), TUV i znak GS (Niemcy), BSMI (Tajwan), CCC (Chiny), BIS (Indie), KC (Korea Południowa), DIMIM (Malezja), Kambodża, Ukraina, EAC, certyfikaty EAC, znak CE, FCC, Energy Star, UL, Paragwaj, Chile, Argentyna, Singapur, Filipiny itd. | | Minimalne wymiary (szer. x głęb. x wys.) | 420 x 390 x 323 mm | | Wymiary maksymalne (szer. x głęb. x wys.) | 430 x 634 x 325 mm | | Waga | 12,6 kg | | Gwarancja | Roczna gwarancja, naprawa na miejscu. |   Dodatkowy Toner - 1 sztuka do drukarki. Dopuszczamy zastosowanie zamiennika z chipem w wersji XXL z wydajnością: Wydajność (5% pokrycia) - 9500 str. . Toner musi posiadać certyfikaty TUV oraz ISO 9001 i 14001. |  |
| **4.** | **Urządzenie wielofunkcyjne Atramentowe, kolorowe na tusze dolewane z dodatkowymi tuszami** | Technologia druku Atramentowa, kolorowa  Funkcje urządzenia Wielofunkcyjne - drukowanie, skanowanie, kopiowanie  Skanowanie Tak, automatyczne jednostronne (Podajnik ADF)  Dostępne tanie zamienniki Tak  Stałe zasilanie tuszem Tak, tusz dolewany z butelki  Druk dwustronny (Duplex) Automatyczny  Wireless - druk przez WiFi Tak  Ethernet - druk w sieci LAN Tak  Drukowanie ze smartfona Tak, Android i iOS  Apple AirPrint Tak  Wyświetlacz Wbudowany  Maksymalny format papieru A4  Maksymalna rozdzielczość druku 6000 x 1200 dpi  Maksymalna rozdzielczość skanowania 2400 x 1200 dpi  Kolor urządzenia Czarny  Gwarancja producenta 36 miesięcy (po bezpłatnej rejestracji na stronie producenta)  Szybkość druku: 17 stron na minutę (mono) 16,5 strony (Kolor)  Podajnik papieru Główny: 150 arkuszy | Wielofunkcyjny: 80 arkuszy | ADF: 20 arkuszy  Maksymalna gramatura papieru 220 g/m²  Liczba wkładów drukujących 4 o wydajności: Czarny - do 7500 stron Cyan / magenta / żółty - C/M/Y do 5000 stron  Język menu Polski, angielski i inne  Obsługiwane systemy operacyjne Windows 11, 10, 8, 7, Server, macOS, Linux, Android, iOS  Szerokość 435 mm  Głębokość 418 mm  Wysokość 180 mm  Waga 10 kg  Dołączone akcesoria Kabel zasilający, Zestaw tuszów startowych .  **Dodatkowe Tusze w zestawie:** oryginalne tusze producenta – zestaw (2 x czarny i komplet kolorów) w wersji XXL dołączone przez dostawcę do urządzenia. | **1 szt.** |
| **5.** | **Aparat telefoniczny analogowy bezprzewodowy DECT – sztuk 2** | **Specyfikacja techniczna** **Dźwięk** **Jakość dźwięku** • Doskonała jakość dźwięku i wysoka głośność, również w trybie głośnomówiącym Tryb głośnomówiący w słuchawce Profile dźwiękowe  Dwa profile dźwiękowe (wysokie / niskie tony) Sygnał dzwonka • Odtwarzany w słuchawce i stacji bazowej • Głośność regulowana w 5 stopniach Współpraca z aparatami słuchowymi Tak  **Klawiatura** **Typ klawiatury** Ergonomiczna klawiatura wysokiej jakości z wyczuwalnym punktem zadziałania przycisków **Podświetlenie klawiatury** • Podświetlana klawiatura i przycisk nawigacyjny: kolor pomarańczowy • Podświetlane przyciski odbioru / zakończenia połączenia • 5-kierunkowy przycisk nawigacyjny **Działanie** • Bezpośrednie wybieranie z listy połączeń • Precyzyjna obsługa dzięki powiększonym przyciskom **Funkcje** • Dwa przyciski wyświetlacza z możliwością przypisania najczęściej używanych funkcji • Przypisywanie funkcji: długie naciśnięcie przycisku • Programowane przyciski skróconego wybierania (2 - 9) • Funkcja Flash (przycisk "0") • Regulowany czas Flash • Blokada klawiatury (przycisk #) • Wyłączanie dzwonka (przycisk \*) **Wyświetlacz** **Typ** Kolorowy wyświetlacz TFT Przekątna (cali) 2.2" Rozmiar (W x S) 44 x 35 mm Rozdzielczość 220 x 176 pikseli Kolory 64 tys. Schematy kolorów Podświetlany wyświetlacz z dwoma schematami kolorów (czarny / biały) **Właściwości** • Najlepsza czytelność • Wysoki kontrast **Funkcje** **SMS** • Obsługa wiadomości SMS do 612 znaków • Przechowywanie do 50 SMS  **Budzik** Budzik z melodią do wyboru i funkcją drzemki **Baby phone** • Monitoring pomieszczenia (baby monitor) z możliwością interkomu  • Połączenie na zewnętrzny numer (np. telefonu komórkowego) • Połączenie na wewnętrzny numer (inna słuchawka) **Wybieranie bezpośrednie** Funkcja połączenia bezpośredniego pozwala na połączenie z zaprogramowanym numerem po naciśnięciu dowolnego przycisku. **Kalendarz** • Kalendarz z podglądem miesiąca i funkcją terminarza: • 30 wydarzeń z opisem i oddzielnym sygnałem dzwonka • Przypomnienie o urodzinach dla każdego wpisu w książce   **Sygnalizacja i informacje na wyświetlaczu** **Tryb powiększonej czcionki** Powiększona czcionka przy wybieraniu numeru **Wygaszacz ekranu** • Zegar analogowy lub cyfrowy • CLIP Identyfikacja numeru / nazwy dzwoniącego (CLIP/CNIP) **Połączenia przychodzące** • Animacja połączenia na wyświetlaczu • Migające podświetlenie przycisku „zielonej słuchawki” • Prezentacja opisu numeru z książki telefonicznej **Połączenia nieodebrane**  Informacja na wyświetlaczu oraz migające podświetlenie przycisku wiadomości (z możliwością wyłączenia) **Tryb oczekiwania** • Data i godzina • Siła sygnału i stan naładowania akumulatora • Opis funkcji przycisków wyświetlacza • Powiadomienia o nowych wiadomościach **Połączenie telefoniczne** Wyświetlanie czasu trwania bieżącego połączenia **Nazwa urządzenia** • Edycja nazwy wewnętrznej słuchawki • Edycja nazwy stacji bazowej **Dzwonki**  • 5 poziomów głośności + wył. + narastający • 18 melodii w słuchawce • Indywidualnie przypisywane dzwonki dla połączeń zewnętrznych, wewnętrznych i VIP **Tony serwisowe** • Ton ostrzegawczy przy utracie zasięgu oraz rozładowaniu akumulatora • Potwierdzenie naciśnięcia przycisku **Melodia w trybie oczekiwania** Melodia podczas zawieszenia połączenia przy konsultacji  **Ochrona przed niechcianymi połączeniami** **Lista blokowanych numerów** Lista 150 numerów Wyciszanie połączeń anonimowych Połączenia bez identyfikacji numeru sygnalizowane są jedynie wizualnie **Tylko kontakty** Sygnalizowane są tylko połączenia z numerów zapisanych w książce telefonicznej **Kontrola czasowa** Tryb dzienny/nocny: wyciszanie sygnału dzwonka w określonych godzinach, za wyjątkiem połączeń zapisanych jako VIP   **Książka telefoniczna** • Książka telefoniczna na 200 wpisów • Imię • Nazwisko • Numer telefonu (prywatny) • Numer telefonu (komórkowy) • Numer telefonu (biurowy) • Melodia VIP • Urodziny / rocznica  **Funkcje dzwonienia Powtarzanie wybierania** • Wybieranie bezpośrednio z listy • Lista 20 ostatnio wybieranych numerów **Funkcje** • Wybieranie numeru z możliwością korekty przed zestawieniem połączenia • Obsługa prefiksów **Tryb wybierania** • Wybieranie DTMF • Wybieranie impulsowe (IWV) **Menu** **Obsługa** • Łatwa instalacja: odpakuj, podłącz, rozmawiaj (słuchawka zarejestrowana fabrycznie w stacji bazowej) • Intuicyjne menu dla łatwej obsługi • Wygodne menu w wielu językach • Łatwa obsługa dzięki kolorowym symbolom, menu tekstowemu i przyciskom kontekstowym wyświetlacza **Prezentacja** Czytelne menu główne z 6 ikonami na ekranie   **Zasięg** Na zewnątrz Do 300 m W pomieszczeniach Do 50 m **Zwiększenie zasięgu** Za pomocą Repeater / Repeater HX **Listy połączeń** Lista połączeń z numerami (CLIP/CNIP) z datą i godziną dla wszystkich połączeń (60 wpisów) lub listy połączeń wychodzących,  odebranych i nieodebranych. **Wybieranie** Bezpośrednie oddzwonienie na numery zapisane na liście  **Obsługa systemu z więcej niż 1 słuchawką** **Jednoczesne połączenia** 2 jednoczesne rozmowy (1 zewnętrzna oraz 1 wewnętrzna pomiędzy 2 słuchawkami) **Liczba słuchawek** Rejestracja do 6 słuchawek **Połączenia wewnętrzne** • Bezpłatne połączenia wewnętrzne • Wywołanie wybranej lub wszystkich słuchawek **Transfer książki telefonicznej** Kopiowanie książki telefonicznej pomiędzy słuchawkami Przekazywanie połączenia Przekazywanie połączenia do innej słuchawki, z możliwością zapowiedzi / powrotem do połączenia w przypadku niepowodzenia.   **Zasilanie** Czas rozmów Do 17 h Czas czuwania Do 320 h **Akumulatory** 2 x AAA (NiMH) Ochrona przed utratą zasilania Data i godzina chroniona w przypadku utraty zasilania **Zasilacz** • Zasilacz wtyczkowy 230V do stacji bazowej • Zasilacz wtyczkowy 230V do ładowarki   **ECO-DECT** Redukcja mocy nadawczej Automatyczna redukcja mocy nadawczej w zależności od odległości słuchawki i stacji bazowej Redukcja zużycia energii Do 60% niższe zużycie energii dzięki energooszczędnemu zasilaczowi Brak promieniowania Brak promieniowania radiowego w trybie oczekiwania, również przy kilku słuchawkach, jeśli stacja bazowa i współpracujące słuchawki  obsługują tryb ECO- DECT    **Kompatybilność** **Standardy** • DECT • GAP • DECT-CAT-iq 2.0 (słuchawka) • DECT-CAT-iq 2.1 (słuchawka) **Łączność Zestaw słuchawkowy** Złącze Jack (3.5 mm) **Analogowa linia telefoniczna** Podłączenie 1 analogowej linii telefonicznej (a/b)    **Specyfikacje** Stopień ochrony: IP20 (słuchawka) | **2 szt.** |

***Zadanie nr 2***

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa** | **Opis** | **Ilość** |
|  | **Ekspres do kawy** | Typ ekspresu: Automatyczny  Ciśnienie [bar]: 19 barów  Preferowany typ młynka: Stalowy  Rodzaj kawy: Mielona, Ziarnista  Moc [W]: min. 1450  Preferowane funkcje: Dotykowy ekran, Pojemnik na mleko, Regulacja ilości zaparzanej kawy, Regulacja mocy kawy, Parzenie 2 kaw jednocześnie, Regulacja stopnia zmielenia kawy, Regulacja temperatury kawy, Wbudowany młynek, Spienianie mleka, Wskaźnik poziomu wody, Filtr, Spienianie mleka na zimno, | **1 szt.** |

***Zadanie nr 3***

**Router UTM wraz z wdrożeniem i szkoleniem**

# 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 5 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 instalację 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 50 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 2 Gbps.
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 o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 2 Gbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

# 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.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. 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.
10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
12. 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: adresy 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. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec 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).
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. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
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 usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
9. 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. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. 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 wieloskładnikowego.
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 wieloskładnikowego 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 lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.

# 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 60 miesięcy.

# Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

# Opisy do wymagań ogólnych

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

***Informacje dotyczące szkolenia dla Administratora***:

Szkolenie w trybie online dla minimum dwóch administratorów jednostki

Realizowane przez certyfikowanego inżyniera producenta sprzętu

Zakres Szkolenia:  
Architektura urządzeń   
Wstępna konfiguracja urządzenia   
Tryby pracy NAT/Transparent  
Konfiguracja sieci i routingu  
System Dashboard i moduły systemu  
Konfiguracja routingu  
Polityki zapory sieciowej  
Koncepcja firewall w urządzeniach   
Tworzenie obiektów dla reguł firewall  
Translacja adresów NAT i Virtual IP  
Konfiguracja funkcji ochronnych (profile bezpieczeństwa)  
Ochrona antywirusowa  
Filtrowanie antyspamowe  
System IPS  
Kontrola ruchu WWW / blokowanie URL  
Kontrola aplikacji  
Data Leak Prevention (DLP)  
Wirtualne sieci prywatne – VPN IPSec  
Bieżąca obsługa systemu  
Tworzenie kopii zapasowej konfiguracji i jej odtwarzanie  
Aktualizacja firmware  
Logowanie i alerty  
Filtry logów  
Zewnętrzne mechanizmy logowania  
Dobre praktyki w zarządzaniu urządzeniem