Załącznik nr 1

Opis przedmiotu zamówienia

Część 1:

Lp.	Nazwa	Ilość
1.	**Celowym jest zakup macierzy Synology NAS Rack Station RS2418+ (12 Bay) + szyny montażowe do szafy rack 19”** lub produktu równoważnego, spełniającego następujące parametry minimalne: **Kieszenie na dyski** 2,5"/3,5" - 12 szt. **RAID** 0 1 5 6 10 Basic JBOD **Rodzaje wyjść/ wejść** USB 3.0 - 2 szt. RJ-45 10/100/1000 (LAN) - 4 szt. DC-in (wejście zasilania) - 1 szt. **Procesor** Intel Atom C3538 (4 rdzenie, 2.1 GHz) **Pamięć RAM** 4 GB (DDR4) **Protokoły sieciowe** AFP iSCSI Serwer DLNA Serwer FTP Serwer VPN Wake-On-LAN **System plików dla dysków zewnętrznych** FAT NTFS HFS+ EXT3 EXT4 Btrfs **System plików** EXT4 Btrfs **Dodatkowe informacje** Cloud Station Surveillance Station - obsługa kamer IP Szyfrowanie woluminów **Minimalna gwarancja** 36 miesięcy	2 szt.

2.	**Celowym jest zakup dysku WD 10TB 7200 obr. 256MB RED PRO 3,5** lub produktu równoważnego, spełniającego następujące parametry minimalne: **Rodzaj dysku** HDD wewnętrzny **Pojemność** 10000 GB **Format** 3.5" **Interfejs** SATA III (6.0 Gb/s) - 1 szt. **Pamięć podręczna cache** 256 MB **Prędkość obrotowa** 7200 obr./min **Niezawodność MTBF** 1 000 000 godz. **Dodatkowe informacje** Technologia RAID Zwiększona odporność na drgania Zgodność z systemami NAS **Minimalna gwarancja** 60 miesięcy	13 szt.
3.	**Celowym jest zakup dysku Seagate HDD 2.5 SAS 1.2 TB 10K + kieszenie montażowe do serwera Dell PowerEdge R720** lub produktu równoważnego, spełniającego następujące parametry minimalne: **Rodzaj urządzenia** dysk twardy - hot-swap **Pojemność** 1.2 TB **Rodzaj obudowy** 2,5" **Interfejs** SAS 12Gb/s **Szybkość transmisji urządzenia** 1.2 GBps (zewnętrzna) **Prędkość obrotowa** 10000 obr./min **Interfejsy** 1 x SAS 12 Gb/s **Kompatybilna** wnęka do serwera PowerEdge R720 **Minimalna gwarancja** 24 miesięcy	6 szt.
4.	**Celowym jest zakup serwera Dell PowerEdge R240 Xeon E-2176G 3.7GHz, 12M cache, 6C/64GB/4TB 3,5" 7200rpm/ PERC H330 RAID Controller/ NBD 4 lata + szyny montażowe do szafy rack 19"** lub produktu równoważnego, spełniającego następujące parametry minimalne: **Procesor** dedykowany do pracy w serwerach o wydajności pozwalającej na osiągnięcie wartości „Passmark CPU Mark" min. 15594 pkt. w testach CPU opublikowanych przez niezależną firmę PassMark Software na stronie http://www.cpubenchmark.net/cpu_list.php; (dot. tylko wydajności procesora bez względu na testowaną konfiguracje serwera). **Pamięć operacyjna** pojemność 64 GB (2666MT/s UDIMMs) **Pamięć masowa** pojemość 4TB **Rodzaj pamięci:** HDD (4 x 4x3.5" Hot Plug - SATA - 1TB 7.2K RPM SATA 6Gbps 512n 3.5in Hot-plug Hard Drive) **Kontroler** RAID PERC H330 RAID Controller, Adapter, Full Height **Zasilacz** jeden zasilacz - Cabled Power Supply, 250W **Zdalne zarządzanie** IDRAC iDRAC9 Basic **Wyposażenia multimedialne/ dodatkowe** zintegrowana karta sieciowa Broadcom	1 szt.

	5720 Dual Port 1Gb LOM **Minimalna gwarancja** 48 miesięcy	

Część 2:

1.	**Celowym jest zakup komputera Dell Vostro 3470 i3-8100/8GB/240SSD/Win 10 Pro + mysz Dell i klawiatura Dell** lub produktu równoważnego, spełniającego następujące parametry minimalne: **Procesor** dedykowany do pracy w komputerach typu desktop o wydajności pozwalającej na osiągnięcie wartości „Passmark CPU Mark" min. 8030 pkt. w testach CPU opublikowanych przez niezależną firmę PassMark Software na stronie http://www.cpubenchmark.net/cpu_list.php; (dot. tylko wydajności procesora bez względu na testowaną konfiguracje komputera). **Pamięć operacyjna** pojemność 8 GB (DIMM DDR4, 2400 MHz) Liczba gniazd pamięci: 2 **Pamięć masowa** pojemość 240GB Rodzaj pamięci: SSD **Wyposażenia multimedialne/ dodatkowe** zintegrowana karta graficzna i dźwiękowa **Rodzaje wejść/ wyjść - panel przedni** USB 3.1 Gen. 1 (USB 3.0) - 2 szt. Wyjście słuchawkowe/głośnikowe - 1 szt. Czytnik kart pamięci - 1 szt. **Rodzaje wejść/ wyjść - panel tylny** USB 2.0 - 4 szt. Wejście/wyjścia audio - 3 szt. RJ-45 (LAN) - 1 szt. VGA (D-sub) - 1 szt. HDMI - 1 szt. AC-in (wejście zasilania) - 1 szt. **Mysz komputerowa:** - typ: optyczna - 3 przyciski - kółko do przewijania - kolor czarny - długość kabla 180 cm (nie dopuszcza się stosowania przedłużaczy) - rozdzielczość czujnika: 1000 dpi - interfejs USB (plug and play) **Klawiatura komputerowa:** - typ klasyczny, niskoprofilowy - interfejs USB (plug and play) - układ standardowy z pełnowymiarowymi klawiszami i klawiaturą numeryczną, przeznaczoną na polski rynek - kolor czarny - długość kabla 180 cm (nie dopuszcza się stosowania przedłużaczy) **Minimalna gwarancja** 36 miesięcy **System operacyjny:** Zainstalowany najnowszy system operacyjny (wraz ze sterownikami) Microsoft **Windows 10 PL 64x w wersji PRO** lub system równoważny pod warunkiem, że funkcjonalność oprogramowania będzie	11 kpl.

	charakteryzowała się co najmniej taką samą jakością oraz kompatybilnością z programami i systemami funkcjonującymi u zamawiającego tj. MS Windows XP. Vista, 7, 8, 10, Podłączenie pulpitu zdalnego do Windows Server 2008 i 2008R2. System operacyjny musi obsługiwać NET Framework 4. System musi w pełni współpracować z pakietem MS Office 2010/2013/2016. Interfejs w języku polskim, licencja bezterminowa/ dożywotnia do użytku komercyjnego.	
2.	**MONITOR – model nr 1** **Celowym jest zakup monitora Philips 243V7QDAB/00** lub produktu równoważnego, spełniającego następujące parametry minimalne: **Przekątna ekranu** 23,8" **Powłoka, rodzaj matrycy** Matowa, LED, IPS **Rozdzielczość ekranu** 1920 x 1080 (FullHD), 16:9 **Jasność** 250 cd/m² **Rodzaje wejść/ wyjść** VGA (D-sub) - 1 szt. HDMI - 1 szt. Wyjście słuchawkowe - 1 szt. Wejście audio - 1 szt. DC-in (wejście zasilania) - 1 szt. **Głośniki** Tak **Minimalna gwarancja** 24 miesiące	5 szt.
3.	**MONITOR – model nr 2** **Celowym jest zakup monitora Philips 223V7QHAB/00** lub produktu równoważnego, spełniającego następujące parametry minimalne: **Przekątna ekranu** 21,5" **Powłoka, rodzaj matrycy** matowa, LED, IPS **Rozdzielczość ekranu** 1920 x 1080 (FullHD), 16:9 **Jasność** 250 cd/m² **Rodzaje wejść/ wyjść** VGA (D-sub) - 1 szt. HDMI - 1 szt. Wyjście słuchawkowe - 1 szt. Wejście audio - 1 szt. DC-in (wejście zasilania) - 1 szt. **Głośniki** Tak, fabrycznie montowane (zintegrowane z obudową) **Minimalna gwarancja** 24 miesiące	10 szt.
4.	**Celowym jest zakup drukarka HP LaserJet Pro M227sdn** lub produktu równoważnego, spełniającego następujące parametry minimalne: **Technologia druku** Laserowa, monochromatyczna **Obsługiwany typ nośnika** Papier zwykły Papier fotograficzny Koperty Etykiety **Obsługiwany format nośnika** A4 A5 A6 B5 **Podajnik papieru** 250 arkuszy **Rodzaje podajników papieru** Kasetowy **Odbiornik papieru** 150 arkuszy **Szybkość druku w mono** 28 str./min **Maksymalna rozdzielczość druku** 1200 x 1200 dpi	3 szt.

	Szybkość kopiowania 28 str./min **Rozdzielczość skanowania** 1200 x 1200 dpi **Podajnik dokumentów skanera** Tak (ADF) **Maksymalny format skanu** A4 **Miesięczne obciążenie** 30000 str./miesiąc **Maksymalna gramatura papieru** 163 g/m² **Funkcja faksu** Nie **Druk dwustronny (dupleks)** Automatyczny **Interfejsy** USB LAN (Ethernet) AirPrint **Wyświetlacz** Wbudowany **Dołączone akcesoria** Kabel zasilający, toner startowy **Minimalna gwarancja** 12 miesięcy	
5.	**Celowym jest zakup drukarka HP Color LaserJet Pro M281fdn** lub produktu równoważnego, spełniającego następujące parametry minimalne: **Technologia druku** Laserowa, kolorowa **Obsługiwany typ nośnika** Papier zwykły Papier makulaturowy Papier fotograficzny Koperty Etykiety Folia **Obsługiwany format nośnika** A4 A5 A6 B5 **Podajnik papieru** 250 arkuszy **Rodzaje podajników papieru** Kasetowy **Odbiornik papieru** 100 arkuszy **Szybkość druku w mono** 21 str./min **Szybkość druku w kolorze** 21 str./min **Maksymalna rozdzielczość druku** 600x600 dpi **Szybkość kopiowania** 21 str./min **Rozdzielczość skanowania** 1200 x 1200 dpi **Podajnik dokumentów skanera** Tak (ADF) **Maksymalny format skanu** A4 **Miesięczne obciążenie** 40000 str./miesiąc **Maksymalna gramatura papieru** 220g/m² **Funkcja faksu** Tak **Druk dwustronny (dupleks)** Automatyczny **Interfejsy** USB LAN (Ethernet) AirPrint **Wyświetlacz** Wbudowany **Dołączone akcesoria** Kabel zasilający, toner startowy **Minimalna gwarancja** 12 miesięcy	1 szt.
6.	**MYSZ – model nr 1** **Celowym jest zakup myszy Logitech B170 czarnej, bezprzewodowej** lub produktu równoważnego, spełniającego następujące parametry minimalne: - typ myszy: mobilna - łączność: bezprzewodowa - sensor: optyczny - rozdzielczość: 1000 dpi - liczba przycisków: 3	6 szt.

	- rolka przewijania: 1 - interfejs USB - kolor: czarny - zasięg: 10 m - minimalna gwarancja: 24 miesiące	
7.	**MYSZ – model nr 2** **Celowym jest zakup myszy Dell MS116 optycznej, czarnej, USB** lub produktu równoważnego, spełniającego następujące parametry minimalne: - typ: optyczna - 3 przyciski - kółko do przewijania - kolor: czarny - długość kabla: 180 cm (nie dopuszcza się stosowania przedłużaczy) - rozdzielczość czujnika: 1000 dpi - interfejs USB (plug and play) - minimalna gwarancja: 24 miesiące	30 szt.
8.	**KLAWIATURA – model nr 1** **Celowym jest zakup klawiatury Logitech K270 Wireless Keyboard** lub produktu równoważnego, spełniającego następujące parametry minimalne: - typ klasyczny, bezprzewodowa, niskoprofilowa, ciche klawisze - interfejs USB (plug and play) 2,4 GHz - układ standardowy z pełnowymiarowymi klawiszami i klawiaturą numeryczną, przeznaczoną na polski rynek - kolor: czarny - czas pracy na baterii do 2 lat - odporna na zachlapanie - minimalna gwarancja: 24 miesiące	3 szt.
9.	**KLAWIATURA – model nr 2** **Celowym jest zakup klawiatury Dell KB216-B QuietKey USB (czarna)** lub produktu równoważnego, spełniającego następujące parametry minimalne: - typ klasyczny, niskoprofilowa, ciche klawisze - interfejs USB (plug and play) - układ standardowy z pełnowymiarowymi klawiszami i klawiaturą numeryczną, przeznaczoną na polski rynek - kolor: czarny - długość kabla: 180 cm (nie dopuszcza się stosowania przedłużaczy) - minimalna gwarancja: 24 miesiące	15 szt.
10.	**Celowym jest zakup urządzenia switch D-Link 1210-48** lub produktu równoważnego, spełniającego następującego następujące parametry minimalne: **Zarządzanie** Zarządzalny L3 **Dostęp** Przeglądarka WWW (GUI) Wiersz poleceń (CLI) SNMP v1/v2c/v3 RMON Telnet **Architektura sieci** Gigabit Ethernet **Całkowita liczba portów** 52 **Rodzaje wejść/ wyjść RJ-45 10/100/1000 Mbps - 48 szt. SFP - 4 szt.** **Power over Ethernet (PoE)** Brak PoE	1 szt.

	Obsługiwane standardy IEEE 802.3 IEEE 802.3 u IEEE 802.3 x IEEE 802.3 ab IEEE 802.3 az IEEE 802.1 p IEEE 802.1 Q **Rozmiar tablicy MAC** 16 k **Liczba grup VLAN** 256 **Algorytm przełączania** Store-and-forward **Przepustowość 104** Gb/s **Bufor pamięci** 3 MB **Minimalna gwarancja** 24 miesiące	

Część 3:

1.	**Celowym jest zakup urządzenia wielofunkcyjnego CANON imagePROGRAF TM-300 L36ei - 914mm** lub produktu równoważnego, spełniającego następujące parametry minimalne: **Parametry podstawowe** - możliwość jednoczesnego drukowania i skanowania - skanowanie do USB - technologia druku: atramentowa, 6 kolorów zintegrowanych (6 kanałów kolorystycznych na głowicy drukującej) **Format** A0 **Ilość wkładów z atramentem** 5 **Ilość głowic** 1 **Ilość dysz głowicy drukującej** 15360 (MBK: 5120 dysz; inne kolory: 2560 dysz) **Precyzja linii** ± 0,1 % **Pamięć** min. 2048 MB **Poziom hałasu** max 44 dB **Parametry druku** typ atramentu: atramenty pigmentowe – czarny, czarny matowy, błękitny, amarantowy, żółty rozdzielczość druku mono: 2400x1200 dpi rozdzielczość druku w kolorze: 2400x1200 dpi szybkość drukowania monochromatycznego: do 0,81 stron/min (format A0, papier zwykły, tryb standardowy) szybkość drukowania w kolorze:	1 szt.

	do 0,81 stron/min (format A0, papier zwykły, tryb standardowy) **Marginesy** Górny: 20 mm Dolny: 3 mm (papier w rolce, 20 mm - arkusz) Lewy: 3 mm Prawy: 3 mm **Parametry skanera** technologia skanowania: LED (SingleSensor) rozdzielczość skanowania: do 1200 dpi maks. format skanowania: 914.4 mm **Obsługa nośników** grubość nośnika: min. 0,07 mm max 0,8 mm odbiornik papieru: niestandardowe wymiary nośników (szerokość) min. 203,2 mm max 917 mm niestandardowe wymiary nośników (długość) min. 203,2 mm szerokość rolki do: 36 cali długość rolki do 18 m średnica rolki do 150 mm obsługiwane rodzaje nośników: papier zwykły papier powlekany papier w rolce obsługiwane formaty nośników: B2 (JIS), B1 (BIS), A1 (ISO), A0 (ISO), 10 cali, 14 cali, 17 cali, 24 cale, 36 cali, B4 (JIS), A3 (ISO), A3+ (ISO), A2 (ISO), 8 cali, 12 cali, 16 cali, 20 cali, 30 cali automatyczne odcinanie nośnika **Języki i emulacje** standardowe języki drukarki SG Raster (Swift Graphic Raster) HP-GL/2 HP RTL JPEG (w wersji JFIF 1.02) **Komunikacja** ethernet - druk w sieci LAN standardowe rozwiązania komunikacyjne USB (Hi-Speed, typ: B) Ethernet (IEEE 802.3 1-base-T/IEEE 802.3u 100base-TX/IEEE 802.3ab 1000base-T/IEEE 802.3x Full Duplex) Wireless (IEEE802.11n/IEEE802.11g/IEEE802.11b - sposób włączania/ wyłączania	

	bezprzewodowej sieci LAN **Zasilanie** rodzaj zasilania: sieciowe AC (100-240V) **Wymagania systemowe** Windows Microsoft Windows 32-bitowy: Windows 7, 8.1, 10, Wersja 64-bitowa: Windows 7, 8,1, 10, Server 2008R2, Server 2012/2012R2, Server 2016 **Minimalna gwarancja** 24 miesiące	

Część 4:

1.	**Celowym jest zakup rutera klasy UTM FortiGate-60E plus 24x7 FortiCare and FortiGuard Unified (UTM) Protection na 3 lata + wdrożenie i wsparcie (tefoniczne oraz e-mail) w języku polskim na 1 rok** lub produktu równoważnego, spełniającego następujące parametry minimalne: **Wymagania Ogólne** Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania administratorów do poszczególnych instancji systemu. System musi wspierać 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 – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. **Interfejsy, dyski:** 1. System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz	2 szt.

	gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. **Parametry wydajnościowe:** 1. W zakresie Firewall'a obsługa nie mniej niż 1,2 mln jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 3 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 500 Mbps. 4. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA1: nie mniej niż 2 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 1400 Mbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 180 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem AES256-SHA1) dla ruchu http – minimum 300 Mbps. **Funkcje systemu bezpieczeństwa:** W ramach dostarczonego systemu ochrony muszą być 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 – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Analiza ruchu szyfrowanego protokołem SSL. 10. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 11. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach	

połączeń VPN typu client-to-site.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać 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.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM)
   - Obsługa protokołu Diffiego-Hellman grup 19 i 20
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - 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.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
3. Dla modułów: IPSec VPN oraz SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. Klient VPN musi umożliwiać weryfikację stanu bezpieczeństwa stacji zdalnej.
4. Rozwiązanie powinno zapewniać funkcjonalność VTEP (VXLAN Tunnel End

	Point) **Routing i obsługa łączy WAN** 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego • Policy Based Routingu • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. **Zarządzanie pasmem** 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. **Kontrola antywirusowa** 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. **Ochrona przed atakami** 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.	

	Kontrola aplikacji 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2800 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P, Botnet. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. **Kontrola WWW** 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware, phishing, spam, Dynamic DNS, proxy avoidance. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. **Uwierzytelnianie użytkowników w ramach sesji** 1. System Firewall musi umożliwiać 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. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu	

	Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. **Zarządzanie** 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. **Logowanie** 1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG. **Certyfikaty** Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: • ICSA lub EAL4 dla funkcji Firewall • ICSA lub NSS Labs dla funkcji IPS • ICSA dla funkcji: SSL VPN, IPSec VPN **Serwisy i licencje** Zaoferowany produkt musi posiadać licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one	

	obejmować: • Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 36 miesięcy. **Gwarancja oraz wsparcie** Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. **Opisy do wymagań ogólnych** Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.	

Ponadto powyższy sprzęt powinien:
1. posiadać deklarację zgodności dla towarów sprzedawanych w UE;
2. być fabrycznie nowy i wolny od obciążeń prawami osób trzecich;
3. posiadać dołączone niezbędne instrukcje i materiały dotyczące użytkowania.