TOM II

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Przedmiotem zamówienia jest dostawa sprzętu komputerowego dla gminy Prabuty w ramach konkursu grantowego „Cyberbezpieczny Samorząd", spełniającego poniższe minimalne parametry techniczne, wymagania i funkcje:

Lp.	Nazwa komponentu/element konfiguracji/cecha/ funkcjonalność	MINIMALNE WYMAGANIA/PARAMETRY/FUNKCJE
I.	**PRZEŁĄCZNIKI SIECIOWE Z OKABLOWANIEM – TYP I – 7 sztuk**	
1.	**Rodzaj urządzenia**	Przełącznik - 52 porty - L2+
2.	**Rodzaje portów**	48 x 10/100/1000 4 x 1/10 Gigabit SFP+
3.	**Przepustowość**	130.95 Mpps
4.	**Zdolność przełączania**	176 Gbps
5.	**Wielkość adresów MAC**	16K wpisów
6.	**Protokół routingu**	IGMPv2, IGMP, routing statyczny IPv4, MSTP, RSTP, STP
7.	**Protokół zdalnego zarządzania**	SNMP, RMON, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SCP, DHCP, IPv4, IPv6
8.	**RAM**	512MB
9.	**Pamięć flash**	256MB
10.	**Rodzaj obudowy**	Montowany w szafie rack 1U
11.	**Okablowanie**	1) 48 szt. - kabel LAN nieekranowany o długości 1m. Patchcord kat. 6 z wtyczką 2x RJ-45 2) 4 szt. - kabel optyczny SFP+ DAC, Prędkość transmisji 10/1 Gb/s. Długość kabla 2m.
12.	**Cechy**	Sterowanie przepływem, obsługa DHCP, obsługa ARP, trunking, obsługa VLAN, auto-uplink (auto MDI/MDI-X), nasłuchiwanie IGMP, dublowanie portów, zarządzalność, obsługa IPv6, tryb półdupleksu, tryb pełnego dupleksu, obsługa protokołu Spanning Tree (STP), obsługa protokołu Rapid Spanning Tree (RSTP), obsługa protokołu Multiple Spanning Tree Protocol (MSTP), obsługa list dostępu (ACL), Quality of Service (QoS), obsługa Jumbo Frames, Trusted Platform Module (TPM), obsługa IPv4, obsługuje LACP, obsługuje LLDP, Link Aggregation Control Protocol (LACP), Class of Service (CoS), obsługuje SNMP, bufor pakietów 1,5MB, Bridge protocol data unit (BPDU), LLDP-MED, Green Ethernet (EEE)
13.	**Gwarancja**	5 lat
II.	**PRZEŁĄCZNIKI SIECIOWE Z OKABLOWANIEM – TYP II – 3 sztuki**	
1.	**Rodzaj urządzenia**	Przełącznik - 52 porty – L2+
2.	**Rodzaje portów**	48 x 10/100/1000 PoE+ (Class 4) 4 x 1/10 Gigabit SFP+
3.	**Przepustowość**	130.95 Mpps
4.	**Zdolność przełączania**	176 Gbps
5.	**Wielkość adresów MAC**	16K wpisów
6.	**Protokół routingu**	IGMPv2, IGMP, routing statyczny IPv4, MSTP, RSTP, STP

7.	**Protokół zdalnego zarządzania**	SNMP 1, RMON, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, RADIUS
8.	**RAM**	512MB
9.	**Pamięć flash**	256MB
10.	**Rodzaj obudowy**	Montowany w szafie rack 1U
11.	**Okablowanie**	1) 48 szt. - kabel LAN nieekranowany o długości 1m. Patchcord kat. 6 z wtyczką 2x RJ-45 2) 4 szt. - kabel optyczny SFP+ DAC, Prędkość transmisji 10/1 Gb/s. Długość kabla 2m.
12.	**Cechy**	Sterowanie przepływem, obsługa DHCP, obsługa ARP, obsługa VLAN, automatyczna funkcja uplink (auto MDI/MDI-X), nasłuchiwanie IGMP, obsługa IPv6, tryb półdupleksu, tryb pełnego dupleksu, obsługa protokołu Spanning Tree (STP), obsługa protokołu Multiple Spanning Tree Protocol (MSTP), obsługa list dostępu (ACL), Quality of Service (QoS), Trusted Platform Module (TPM), obsługuje LLDP, Link Aggregation Control Protocol (LACP), Energy Efficient Ethernet, Class of Service (CoS), BPDU Filter, PoE Class 4
13.	**Gwarancja**	5 lat
III.	**MACIERZ DYSKOWA Z OSPRZĘTEM – 1 sztuka**	
1.	**Wymagania ogólne**	1) Urządzenia muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych. 2) Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta. 3) Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta. 4) Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta. 5) Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej. 6) Urządzenia na etapie dostawy pomiędzy producentem, a zamawiającym nie mogą podlegać modyfikacjom.
2.	**Typ obudowy**	Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U z możliwością instalacji min. 24 dysków 2.5”
3.	**Przestrzeń dyskowa**	Zainstalowane: 1) 7 x dysk SSD SAS o pojemności min. 1.92TB, Hot-Plug 2) 7 x dysk HDD SAS 12Gbps o pojemności min. 2,4 TB, 10 tys. obr./min., 2,5”, Hot-Plug
4.	**Możliwość rozbudowy**	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.
5.	**Obsługa dysków**	Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej.
6.	**Sposób zabezpieczenia danych**	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
7.	**Tryb pracy kontrolerów macierzowych**	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.

8.	**Pamięć cache**	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
9.	**Rozbudowa pamięci cache**	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
10.	**Interfejsy**	Macierz musi posiadać co najmniej 8 portów 25Gb iSCSI w standardzie SFP28 (4 porty na kontroler). W zestawie musi znajdować się 6 kabli DAC 25GbE SFP28/SFP28 min. 3m, dostarczone przez producenta macierzy.
11.	**Zarządzanie**	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
12.	**Zarządzanie grupami dyskowymi oraz dyskami logicznymi**	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
13.	**Thin Provisioning**	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
14.	**Tiering**	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
15.	**Wewnętrzne kopie migawkowe**	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
16.	**Wewnętrzne kopie pełne**	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
17.	**Migracja danych w obrębie macierzy**	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do

		danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
18.	**Zdalna replikacja danych**	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
19.	**Podłączanie zewnętrznych systemów operacyjnych**	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwiema ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
20.	**Redundancja**	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.
21.	**Dodatkowe wymagania**	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
22.	**Standardy bezpieczeństwa**	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International)
23.	**Inne**	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
24.	**Warunki gwarancji**	1) Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat lub 7 lat (w zależności od okresu podanego w ofercie). 2) Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet lub z wykorzystaniem aplikacji. 3) Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. 4) Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 5) Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających wykrywanie usterek sprzętowych z predykcją awarii,

		automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. 6) Zamawiający będzie wymagał od podmiotu realizującego serwis lub producenta sprzętu dołączenia do umowy oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. 7) Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. Zamawiający będzie wymagał załączenia ww. dokumentów do umowy. 8) Zamawiający będzie wymagał dołączenia do umowy oświadczenia Producenta potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
25.	**Karty sieciowe dla posiadanych serwerów**	1) 1 szt. karta sieciowa dwuportowa 25Gb SFP28 OCP NIC 3.0, zatwierdzona do pracy w posiadanym przez zamawiającego serwerze DELL R450. Karta musi pochodzić z autoryzowanej dystrybucji producenta posiadanego serwera. 2) 1 szt. karta sieciowa dwuportowa 25Gb SFP28 PCIe, zatwierdzona do pracy w posiadanym przez zamawiającego serwerze DELL R440. Karta musi pochodzić z autoryzowanej dystrybucji producenta posiadanego serwera.
IV.	**ZAPORA SIECIOWA KLASY UTM – 1 sztuka**	
1.	**Obsługa sieci**	Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
2.	**Zapora korporacyjna (firewall)**	1) Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2) Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3) Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4) Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5) Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 6) Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7) Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8) Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 9) Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 10) Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). 11) System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
3.	**Intrusion prevention system (ips)**	1) System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2) Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3) Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.

		4) Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5) Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 6) Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 7) Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 8) Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 9) Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). 10) Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
4.	**Kształtowanie pasma (traffic shapping)**	1) Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2) Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 3) Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4) Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
5	**Ochrona antywirusowa**	1) Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 2) Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 3) Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 4) Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
6.	**Ochrona antyspam**	1) Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2) Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. Skaner heurystyczny. 3) W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 4) Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
7.	**Wirtualne sieci prywatne (vpn)**	1) Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2) Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a) PPTP VPN, b) IPSec VPN, c) SSL VPN. 3) SSL VPN ma działać co najmniej w trybach tunelu i portalu. 4) Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 5) Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) 6) Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 7) Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 8) Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

8.	**Filtr dostępu do stron www**	1) Urządzenie ma posiadać wbudowany filtr URL. 2) Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 3) Administrator ma mieć możliwość dodawania własnych kategorii URL. 4) Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: 5) blokowanie dostępu do adresu URL, 6) zezwolenie na dostęp do adresu URL, 7) blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 8) Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 9) Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 10) Filtr URL musi uwzględniać komunikację po protokole HTTPS. 11) Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 12) Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. 13) Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
9.	**Uwierzytelnianie**	1) Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a) lokalną bazę użytkowników (wewnętrzny LDAP), b) zewnętrzną bazę użytkowników (zewnętrzny LDAP), c) usługę katalogową Microsoft Active Directory. 2) Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 3) Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: a) SSL, b) Radius, c) Kerberos. 4) Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 5) Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 6) Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. 7) Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). 8) Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 9) Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
10.	**Administracja łączami do internetu (isp)**	1) Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2) Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a) równoważenie względem adresu źródłowego, b) równoważenie względem połączenia. 3) Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4) Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). 5) Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 6) W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).

		7) Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
11.	**Routing (trasowanie)**	1) Urządzenie ma umożliwiać statyczne trasowanie pakietów. 2) Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 3) Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 4) Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
12.	**Administracja urządzeniem**	1) Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2) Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 3) Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 4) Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5) Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 6) Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) 7) Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 8) Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 9) Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 10) Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 11) Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. 12) Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). 13) System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). 14) Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. 15) Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku. 16) Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 17) Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 18) Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a) manualnego eksportu do pliku w dowolnym momencie czasu, b) automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu 19) Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. 20) Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. 21) Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
13.	**Raportowanie**	1) Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2) System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3) System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 4) System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.

		5) System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 6) System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 7) Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 8) Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 9) Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
14.	**Pozostałe usługi i funkcje**	1) Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. 2) Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 3) Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 4) Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 5) Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). 6) Urządzenie ma posiadać usługę DNS Proxy. 7) Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). 8) Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 9) Urządzenie musi mieć zaimplementowane Open API 10) Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
15.	**Gwarancja i serwis**	1) Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. 2) W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
16.	**Parametry sprzętowe**	1) Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB. 2) Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy. 3) Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16. 4) Liczba portów światłowodowych 1Gbps – min. 2 z możliwością rozszerzenia do 10. 5) Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy: a) Moduł z 8 interfejsami miedzianymi 2,5Gbps b) Moduł z 4 interfejsami miedzianymi 10Gbps. c) Moduł z 4 interfejsami światłowodowymi 1Gbps. d) Moduł z 8 interfejsami światłowodowymi 1Gbps. e) Moduł z 4 interfejsami światłowodowymi 10Gbps. 6) Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 7) Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45. 8) Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps. 9) Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 5Gbps. 10) Przepustowość filtrowania Antywirusowego – minimum 1.3 Gbps. 11) Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2.5Gbps. 12) Maksymalna liczba tuneli VPN IPSec – minimum 1000. 13) Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 150. 14) Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 150. 15) Obsługa interfejsów 802.11q (VLAN) – minimum 256. 16) Liczba równoczesnych sesji – minimum 600 000 i nie mniej niż 30 000 nowych sesji/sekundę. 17) Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 18) Urządzenie nie ma limitu na liczbę użytkowników. 19) Liczba reguł filtrowania – minimum 16 384.

		20) Liczba tras statycznego routingu – minimum 5 120. 21) Liczba tras dynamicznego routingu – minimum 10 000. 22) Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U. 23) Urządzenie musi być wyposażone w moduł TPM.
17.	**Szkolenie z obsługi**	Szkolenie dla jednej osoby autoryzowane przez producenta odbywające się w autoryzowanym ośrodku producenta na terenie kraju w formie warsztatów online zakończone egzaminem producenta i zaświadczeniem ukończenia szkolenia.