

CUW doposażenie szafy RACK

1. Przetątnik sieciowy szt.2 o parametrach

1.	Przetątnik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przetątnika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2.	<p>Wymagane parametry fizyczne:</p> <ul style="list-style-type: none">a) możliwość montażu w stelażu/szafie 19”;b) minimum jeden zasilacz 230V AC, moc zasilacza zapewniająca budżet mocy dla portów PoE minimum 380W;c) zakres temperatur pracy ciągłej co najmniej od 0 do +45°C;d) zakres wilgotności pracy co najmniej 5% - 90%;e) port USB umożliwiający podłączenie zewnętrznej pamięci flash.
3.	<p>Przetątnik musi posiadać minimum:</p> <ul style="list-style-type: none">a) 48 portów 10/100/1000BASE-T PoE+ zgodnych z 802.3at oraz 802.3afb) 4 porty 10GE SFP+ <p>Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.</p>
4.	<p>Przetątnik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:</p> <ul style="list-style-type: none">a) zarządzanie stosem poprzez jeden adres IP;b) do min. 8 jednostek w stosie;c) możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation);d) stos przetątników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree;e) jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia. <p>Zamawiający dopuszcza, aby możliwość łączenia w stosy była realizowana za pomocą portów typu uplink.</p>
5.	Układ przetątniający o wydajności min. 176 Gbps, wydajność przetątniania przynajmniej 130 Mpps.
6.	Obsługa min. 32 000 adresów MAC.
7.	<p>Wbudowana pamięć RAM min. 512MB.</p> <p>Procesor wielordzeniowy.</p>
8.	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 500 MB.
9.	Obsługa min. 4000 sieci VLAN jednocześnie.
10.	Możliwość skonfigurowania min. 1000 interfejsów vlan interface SVI działających równocześnie.
11.	Obsługa ramek jumbo o wielkości min. 9000 bajtów.
12.	Obsługa protokołu GVRP lub VTP.
13.	Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP.
14.	Obsługa min. 4 000 tras dla routingu IPv4.

15.	Obsługa min. 1 000 tras dla routingu IPv6.
16.	Obsługa protokołów routingu OSPF, RIP, PIM-SM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania.
17.	Obsługa protokołu LLDP lub CDP.
18.	Obsługa ruchu IGMP v1, v2 i v3.
19.	<p>Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:</p> <ul style="list-style-type: none"> a) min. 2 poziomy dostęp administracyjny poprzez konsolę; b) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydzielenia VLANu oraz dynamicznego przypisania listy ACL; c) możliwość utworzenia minimum 1600 list ACL; d) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www; e) zarządzanie urządzeniem przez HTTPS, SNMPv3 i SSHv2 za pomocą protokołów IPv4 i IPv6; f) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP; g) obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard; h) możliwość synchronizacji czasu zgodnie z NTP.
20.	Obsługa funkcjonalności UDLD lub równoważnej.
21.	<p>Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:</p> <ul style="list-style-type: none"> a) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP; b) wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR.
22.	<p>Wymagane opcje zarządzania:</p> <ul style="list-style-type: none"> a) możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN; b) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC); c) urządzenie musi posiadać wbudowany port USB pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych; d) dedykowany port konsoli musi być zgodny ze standardem RS-232.
23.	<p>Wraz z urządzeniami muszą zostać dostarczone:</p> <ul style="list-style-type: none"> a) pełna dokumentacja w języku polskim lub angielskim; b) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana.
24.	Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
25.	Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.

26.	Zamawiający wymaga, aby przełącznik posiadał minimum 1 roczne wsparcie serwisowe , świadczone przez Wykonawcę na bazie wsparcia serwisowego producenta. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres wsparcia serwisowego liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia.
27.	Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres wsparcia serwisowego dla urządzeń.
28.	Każde urządzenie wyposażone w wkładki SFP+: 1 x 1 Gb/s SM 1 x 10 Gb/s SM 1 x 10 Gb/s RJ 45 1 x STACK CABLE

2. Pamięć masowa NAS szt.1 o parametrach

1.	Urządzenie musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające jego instalację w szafie rack.
2.	CPU Dwurdzeniowy procesor AMD Ryzen™ R1600 (4-wątkowy) z taktowaniem 2,6 GHz (maksymalnie 3,1 GHz)
3.	Sprzętowy mechanizm szyfrowania AES-NI
4.	Pamięć Pamięć ECC DDR4 2 GB
5.	4 dyski SATA HDD 3,5 cala lub dyski SATA SSD 2,5 cala. Urządzenie wyposażone w 4 dyski SATA HDD 3.5 cala o pojemności 6 TB dedykowane do tego typu urządzenia
6.	Wymiana dysków podczas pracy: Tak
7.	Porty zewnętrzne 1 porty USB 3.2 1. generacji
8.	Sieć: Porty LAN 2 porty 1GbE RJ-45 oraz dodatkowo karta rozszerzeń 10Gb/s RJ 45
9.	Funkcja Wake on LAN/WAN Tak
10.	Zaplanowane włączanie /wyłączanie: Tak
11.	Protokoły sieciowe SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP i VPN (PPTP, OpenVPN™, L2TP)
12.	Obsługiwane typy macierzy RAID: RAID 0, RAID 1, RAID 5, RAID 6 i RAID 10
13.	Dodatkowo urządzenie doposażone w zewnętrzny dysk twardy USB o pojemności 20 TB

3. Serwer szt. 1 o parametrach

1.	Urządzenie musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające jego instalację w szafie rack.
----	---

2.	CPU Szesnastordzeniowy procesor Intel® Xeon® Gold z taktowaniem min. 2.5 GHz i 37,5 MB pamięci cache L3
3.	RAM pamięć: 32 GB (1 x 32 GB) ECC DDR5 RDIMM z możliwością rozbudowy do 4TB
4.	Wbudowane zatoki na dyski: 8 x SFF (2.5") możliwość instalacji dysków zgodnych z U.3 NVMe/SAS/SATA.
5.	Zainstalowane dyski: min 2x 500GB SSD zgodne z zaproponowanym serwerem
6.	Kontroler RAID: HPE MR408i-o Gen11, 8 linii, 4 GB pamięci cache OCP SPDM z obsługą poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
7.	Kontroler sieciowy: Broadcom BCM57416 Ethernet 10Gb 2-port BASE-T Adapter
8.	Obsługa 8 slotów PCIe Gen5 oraz 2 slotów OCP 3.0
+	
9.	Moduł TPM: TPM 2.0 w standardzie, wbudowany na płycie głównej.
10.	Typ zasilacza: 1000W Flex Slot Titanium Hot Plug Power Supply z certyfikatem 80 PLUS Titanium
11.	Typ napędu: Opcjonalny napęd DVD-ROM dostępny przez Universal Media Bay lub zewnętrzne rozwiązania.

4. UTM szt. 1 o parametrach

1.	Urządzenie musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające jego instalację w szafie rack.
2.	System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania oraz musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. 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, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: 5 • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
	<p>Redundancja, monitoring i wykrywanie awarii</p> <p>1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive, Clustering. W trybach tych powinna istnieć funkcja synchronizacji sesji firewall.</p> <p>W ramach postępowania musi zostać dostarczone pojedyncze urządzenie, które utworzy klaster HA z posiadanym i używanym przez Zamawiającego urządzeniem Fortinet FortiGate 61F.</p> <p>2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</p> <p>3. Monitoring stanu realizowanych połączeń VPN</p>

	<p>Interfejsy, Dysk, Zasilanie:</p> <p>1. System realizujący funkcję Firewall musi dysponować minimum:</p> <ul style="list-style-type: none"> • 5 portami LAN Gigabit Ethernet RJ-45 • 2 portami WAN Gigabit Ethernet RJ-45 • 1 port konsolowy RJ-45 • 1 port USB
	System Firewall musi posiadać wbudowany dysk SSD min. 128 GB
	W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q
	System musi być wyposażony w zasilanie AC.
	<p>Parametry wydajnościowe:</p> <ol style="list-style-type: none"> 1. Przepustowość firewalla dla pakietów UDP rozmiar 512 B nie mniej niż 10 Gbps 2. Obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę 3. Przepustowość ochrony przed zagrożeniami mierzona przy włączonej zaporze, systemie IPS, kontroli aplikacji i ochronie przed złośliwym oprogramowaniem mniej niż 700 Mb/s 4. Przepustowość (NGFW) Stateful Firewall nie mniej niż 1 Gbps 5. Przepustowość IPS nie mniej niż 1,4 Gbps 6. Przepustowość kontroli aplikacji nie mniej niż 1,8 Gbps 7. Przepustowość SSL VPN nie mniej niż 900 Mb/s 8. Ilość równoczesnych połączeń użytkowników SSL-VPN (tryb tunelowy) nie mniej niż 200 9. Gateway-to-Gateway IPsec VPN Tunnels nie mniej niż 200 10. Client-to-Gateway IPsec VPN Tunnels nie mniej niż 500 11. Przepustowość IPsec VPN nie mniej niż 6,5 Gbps 12. Przepustowość systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 630 Mbps 13. Równoczesne sesje inspekcji SSL nie mniej niż 55 tys.
	<p>Funkcje Systemu Bezpieczeństwa:</p> <p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje:</p> <ol style="list-style-type: none"> 1. Kontrola dostępu - zaporę ogniową 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.

	<p>7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.</p> <p>8. Zarządzanie pasmem (QoS, Traffic shaping).</p> <p>9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).</p> <p>10. 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.</p> <p>11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.</p> <p>12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.</p>
	<p>Polityki, Firewall</p> <p>1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</p> <p>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.</p> <p>3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.</p> <p>5. Element systemu realizujący funkcję Firewall musi integrować 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 - Google Cloud Platform (GCP). - OpenStack. - VMware NSX</p>
	<p>Połączenia VPN</p> <p>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 Diffie-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.</p> <p>2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: 7 • 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.</p>
	<p>Routing i obsługa łącz WAN</p> <p>1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routing. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.</p>

	<p>Zarządzanie pasmem</p> <ol style="list-style-type: none"> 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.
	<p>Ochrona przed malware</p> <ol style="list-style-type: none"> 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. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
	<p>Ochrona przed atakami</p> <ol style="list-style-type: none"> 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać 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) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
	<p>Kontrola aplikacji</p> <ol style="list-style-type: none"> 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 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

	<p>3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> <p>4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.</p>
	<p>Kontrola WWW</p> <p>1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p> <p>2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</p> <p>3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.</p> <p>4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.</p> <p>6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.</p> <p>7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.</p>
	<p>Uwierzytelnianie użytkowników w ramach sesji</p> <p>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.</p> <p>2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</p> <p>3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.</p> <p>4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p>
	<p>Zarządzanie</p> <p>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.</p> <p>2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.</p> <p>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. 9</p>

	<p>5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>6. Element systemu pełniący funkcję firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p>
	<p>Logowanie</p> <p>1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze producenta, z funkcją rocznej retencji logów.</p> <p>2. W ramach logowania system pełniący funkcję Firewall 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.</p> <p>3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.</p> <p>4. Musi istnieć możliwość logowania do serwera SYSLOG</p>
	<p>Serwisy i licencje</p> <p>W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen oraz chmurowy system logowania na okres 12 miesięcy.</p>
	<p>Dostarczone urządzenia i rozwiązania powinny zostać objęte serwisem gwarancyjnym producenta przez okres 12 miesięcy, realizowanym na terenie Rzeczypospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości lub uszkodzenia. Dostarczone urządzenia i rozwiązania muszą być objęte rozszerzonym serwisem gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym (8x5), realizowanym przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta, w zakresie serwisu gwarancyjnego (dołączyć na wezwanie Zamawiającego).</p>

5. UPS szt. 1 o parametrach

1.	Urządzenie musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające jego instalację w szafie rack.
2.	Topologia UPS: Podwójnej konwersji (online),
3.	Maksymalna możliwa do konfiguracji moc: 2 kVA, Moc rzeczywista: 1600 W.
4.	Certyfikaty zgodności: RoHS, Certyfikaty: CE, IEC 62040-1-1, IEC 62040-1-2 REACH.
5.	Interfejs RS-232.

6.	Typ wyświetlacza: LCD.
----	------------------------