**Załącznik do umowy nr ……………………**

**Szczegółowy opis przedmiotu zamówienia**

1. Serwery.

|  |  |
| --- | --- |
| **Nazwa elementu, parametru lub cechy** | **Opis wymagań Serwerów** |
| **Ilość sztuk** | 2 sztuki |
| **Obudowa** | Do instalacji w szafie Rack 19", wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych, |
| **Procesor** | Architektura x86, maksymalny TDP dla procesora – 100W.  Minimalna ilość rdzeni dla procesora – 16. |
| **Liczba procesorów** | Min. 2 |
| **Płyta główna** | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon). |
| **Pamięć operacyjna** | Zainstalowane 512GB pamięci RAM w kościach min. 32GB.  Minimum 24 sloty na pamięć, wsparcie pamięci typu RDIMM lub LRDIMM.  Pamięć o częstotliwości min. 2933MHz.  Wsparcie dla pamięci DCPMM. |
| **Zabezpieczenie pamięci** | ECC, Memory Rank Sparing, Memory Mirror |
| **Procesor Graficzny** | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.  Port VGA. |
| **Dyski** | Zainstalowane dyski:  SSD: 2 szt. 480GB RI SATA SSD  HDD: 6 szt. 12TB SATA HDD |
| **Rozbudowa dysków** | Serwer musi posiadać 8 zatok na dyski Hot-Swap, umożliwiających instalację dysków SATA/SAS – bez wymiany/dokładania jakichkolwiek elementów serwera.  Możliwość instalacji dysków SED.  Możliwość zastosowania w serwerze backplane’u umożliwiającego instalację zarówno dysków SATA/SAS jak i w tych samych zatokach z tym samym backplane zamiennie. |
| **Kontroler dyskowy** | Zainstalowany kontroler 12 Gb SAS/SATA z obsługą RAID 0, 1, 10, 5, 50, 6, 60  Minimum 2 GB flash-backed cache. |
| **Zasilacz** | Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Platinum. |
| **Interfejsy sieciowe** | Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. |
| **Karty sieciowe** | 4 x 1G RJ45 (dopuszcza się 1 kartę 4x1G lub 2 karty po 2x1G)  4 x 10G SFP+ (dopuszcza się 1 kartę 4x10G lub 2 karty po 2x10G) |
| **Dodatkowe sloty I/O** | Dostępne, niezajęte i gotowe do użytku 2 sloty PCIe.  Możliwość rozbudowy do minimum 7 slotów PCIe, w tym min. jednego x16 |
| **Dodatkowe porty** | * z przodu obudowy: 1x USB 3.0, 1x USB 2.0, opcjonalnie VGA. * z tyłu obudowy: 2x USB 3.0, VGA. |
| **Chłodzenie** | Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 |
| **Zarządzanie** | * Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania * Monitoring statusu i zdrowia systemu * Logowanie zdarzeń * Umożliwiający Update systemowego firmware * Umożliwiający zdalną konfigurację serwera * Monitoring i możliwość ograniczenia poboru prądu * Zdalne włączanie/wyłączanie/restart * Przekierowanie konsoli szeregowej przez IPMI * Zrzut ekranu w momencie zawieszenia system * Możliwość przejęcia zdalnego ekranu 1920x1200, 60 Hz,16 bpp * Zdalny dostęp do serwera * Możliwość zdalnej instalacji systemu operacyjnego * Alerty Syslog * Przekierowanie konsoli szeregowej przez SSH * Wyświetlanie danych aktualnych I historycznych dla użycia energii I temperatury serwera * Możliwość mapowania obrazów ISO z lokalnego dysku operatora * Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS * Możliwość jednoczesnej pracy do 4 użytkowników przez wirtualną konsolę   Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, REST API |
| **Funkcje zabezpieczeń** | Hasło włączania, hasło administratora, moduł TPM. |
| **Urządzenia hot swap** | Dyski twarde, zasilacze oraz wentylatory |
| **Obsługa** | Możliwość instalacji serwera, dysków twardych, pamięci i wentylatorów do celów serwisowych bez użycia dodatkowych narzędzi mechanicznych. |
| **Systemy operacyjne** | Microsoft Windows Server 2016 i 2019, Red Hat Enterprise Linux 7 oraz 8, SUSE Linux Enterprise Server 12 oraz 15, VMware vSphere (ESXi) 6.5 oraz 6.7. |
| **Gwarancja** | Minimum 36 miesięcy gwarancji producenta z gwarantowanym czasem naprawy 24h i zachowaniem dysków. |

1. Urządzenia sieciowe.

Wymagania wykonawcy

Wykonawca musi być autoryzowanym/certyfikowanym partnerem producenta.

Żadne oprogramowanie dostarczone (również oprogramowanie zainstalowane na dostarczonym sprzęcie) nie będzie wytworzoną wersją jedynie na potrzeby niniejszego postępowania. Musi być dostępne dla wszystkich klientów. Wersje tego oprogramowania muszą posiadać wsparcie techniczne ich producenta albo producenta dostarczanego sprzętu.

Oferowane urządzenia muszą być nowe oraz pochodzić z autoryzowanej sieci sprzedaży na teren Unii Europejskiej.

Żadne oferowane urządzenie i oprogramowanie nie może mieć ogłoszonego statusu EoL (End of Life) / EoS (End of Support).

Jeśli urządzenia posiadają licencje do portów 10G lub Stack lub protokołów routingu ospf/rip itp należy je wgrać.

Wszystkie urządzenia należy dostarczyć z kompletem okablowania do STACK i kabli zasilających.

Wszystkie przełączniki muszą pochodzić od tego samego producenta.

1. Przełącznik A - jedna sztuka

Typ i liczba portów liniowych w ramach urządzenia:

Minimum 26 portów RJ45 - 10/100/1000 Ethernet.

Minimum 4 porty pracujące z prędkością 1/10 Gbps na wkładki SFP/SFP+. Jeśli wymagana jest licencja lub moduł SFP/SFP+ jest wymagane na tym etapie postępowania.

Wszystkie porty liniowe muszą być z przodu obudowy.

Porty 1GE (SFP) muszą umożliwiać ich obsadzanie wkładkami – minimum 1000Base-SX, 1000BaseLX/LH, 1000Base-BX-D/U, 10GBaseSR, 10GBaseLR, 10G-Twinax-DAC zależnie od potrzeb Zamawiającego.

Wymagane jest, aby minimum 24 portów dostępowych 10/100/1000 obsługiwały standard zasilania poprzez sieć LAN (Power over Ethernet) zgodnie ze standardami IEEE 802.3af oraz IEEE 802.3at.  Budżet mocy PoE/PoE+ dla wszystkich portów nie może być mniejszy niż 370W.

Urządzenie musi obsługiwać minimum 4000 VLAN 802.1q.

Urządzenie musi obsługiwać minimum 16200 adresów MAC.

Urządzenie musi obsługiwać minimum 250 instancji STP (spanning trees).

Urządzenie musi posiadać min. 1GB pamięci DRAM i 1GB pamięci flash.

Parametry fizyczne – możliwość montażu w szafie 19”, wielkość urządzenia nie może przekroczyć 1U, ewentualne zestawy montażowe powinny być w komplecie razem ze switchem.

Urządzenie musi być pozbawione wentylatorów - chłodzone pasywnie.

Minimalna wydajność przełączania ruchu 98 Mpps oraz wymagana minimalna przepustowość matrycy 132 Gb/s.

Urządzenie musi posiadać funkcjonalność łączenia w stosy z zachowaniem następującej parametrów:

Do min. 12 jednostek w stosie.

Magistrala stackująca o przepustowości co najmniej 40Gbps.

Możliwość tworzenia połączeń EtherChannel LACP zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (Cross-stack EtherChannel) – minimum z 6 różnych przełączników w stosie jednocześnie.

Jeżeli realizacja funkcji stackowania wymaga dodatkowych modułów/kabli itp. ich dostarczenie w ramach tego postępowania jest wymagane. Dopuszczalne jest stackowanie po portach liniowych opisanych w punkcie 1b (SFP/SFP+) lub portach dedykowanych.

Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9216 bajtów (Jumbo Frames)

Urządzenie musi wspierać mechanizm QinQ.

Obsługa protokołu NTP lub SNTP.

Musi zapewniać obsługę min. 1000 tras w bazie Forwarding Information Base (FIB) IPv4 lub IPv6.

Musi zapewniać routing statyczny, dynamiczny i wsparcie dla protokołów multicast: OSPFv2, OSPFv3, RIP, RIP-NG, PIM-SM, PIM-DM, PIM-SSM, PIM-Passive. Jeśli funkcjonalność wymaga dodatkowej licencji – nie jest ona wymagana na tym etapie postępowania.

Musi zapewniać obsługę protokołów First-Hop Redundancy – np. VRRP zarówno dla IPv4 jaki i IPv6. Jeśli funkcjonalność wymaga dodatkowej licencji – nie jest ona wymagana na tym etapie postępowania.

Obsługa ruchu multicast – IGMPv2, IGMPv3, MLDv1/2 Snooping.

Wsparcie dla protokołów Per-VLAN Spanning-Tree, IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 252 instancji protokołu STP.

Wsparcie dla funkcji BPDU Guard oraz funkcji wykrywania i zabezpieczenia przed pętlami Layer 2.

Wsparcie dla funkcji Auto-MDI/MDI-X na portach 10/100/1000.

Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP Server oraz wspierać funkcję DHCP Helper.

Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad.

Przełącznik musi obsługiwać wkładki SFP/SFP+ wszystkich producentów bez wydawania specjalnych dodatkowych komend.

Przełącznik musi obsługiwać następujące mechanizmy bezpieczeństwa:

Minimum 3 poziomów dostępu administracyjnego.

Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL. Wsparcie dla Critical-VLAN, Restricted-VLAN oraz Guest-VLAN.

Obsługa Private VLAN.

Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,

Możliwość uwierzytelniania użytkowników w oparciu o portal www (WebAuth).

Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC.

Wymagana jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie.

Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176.

Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6

Obsługa list kontroli dostępu (ACL).

Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection.

Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne).

Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:

Klasyfikacja ruchu do klas różnej jakości obsługi (QoS).

Implementacja co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu WRR lub SRR lub innego podobnego dla obsługi tych kolejek.

Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).

Możliwość mapowania ruchu do określonych kolejek QoS z wykorzystaniem ACL

Możliwość ograniczania pasma dostępnego na każdym porcie jednocześnie dla ruchu wychodzącego oraz przychodzącego za pomocą Shapingu lub Policingu.

Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP).

Obsługa protokołu UDLD.

Obsługa protokołu wspierającego topologię pierścienia zbudowaną z przełączników (tzw. Ethernet Ring) – Np. G.8032 lub REP lub inny równoważny.

Obsługa protokołu GVRP lub MVRP lub innego równoważnego (np. VTP).

Obsługa protokołu OpenFlow 1.3 lub nowszego dla współpracy z kontrolerem OpenFlow.

Wsparcie dla AAA z wykorzystaniem serwerów TACACS oraz Radius.

Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli

Urządzenie musi posiadać port konsoli szeregowej (RJ45 lub DB9), port konsoli USB (dla laptopów bez portu szeregowego) oraz port Ethernet typu out-of-band (niezależny od portów liniowych opisanych w pkt.1) – do zarządzania.

Urządzenie musi być wyposażone w port USB umożliwiający podłączenie pamięci flash.

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). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją.

MTBF (Mean Time Between Failure) nie może być mniejszy niż 500000 godzin.

Urządzenie powinno być bez wentylatorowe (fan less) lub posiadać tryb cichy pracy czyli możliwość wyłączenia wentylatorów zapewniając jednocześnie budżet POE o wielkości 150 wat.

Wymagane jest, aby przełącznik posiadał gwarancję producenta minimum przez okres 36 miesięcy.

1. Przełącznik B - trzy sztuki

Muszą pracować jako jeden stos, dostępny pod jednym adresem IP.

Typ i liczba portów liniowych w ramach urządzenia:

Minimum 48 portów 10/100/1000

Minimum 8 portów 1/10GE na wkładki SFP/SFP+. Porty muszą obsługiwać prędkości 1Gbit/s oraz 10Gbit/s w zależności od zainstalowanej wkładki SFP/SFP+ lub kabla DAC.

Porty SFP/SFP+ muszą umożliwiać ich obsadzanie wkładkami – minimum 1000Base-SX, 1000BaseLX/LH, 1000Base-BX-D/U, 10Gbit-SR, 10Gbit-LR - zależnie od potrzeb Zamawiającego.

Minimalna wydajność przełączania ruchu 190Mpps (dla pakietów 64-bajtowych) oraz wymagana minimalna przepustowość matrycy 250Gb/s full duplex.

Musi zapewniać obsługę min. 12000 tras FIB IPv4.

Urządzenie musi obsługiwać minimum 16000 adresów MAC.

Przełącznik musi umożliwiać dodanie redundancji zasilania poprzez dodanie dodatkowego zasilacza wewnętrznego lub zewnętrznego.

Urządzenie musi posiadać min. 2GB pamięci DRAM i 2GB pamięci flash.

MTBF (Mean Time Between Failure) nie może być mniejszy niż 300000 godzin.

Urządzenie musi mieć możliwość pracy w trybach (wymagana rekonfiguracja lub zmiana oprogramowania, jeśli wymagane są licencje – należy je dostarczyć):

Jako samodzielny przełącznik.

Jako przełącznik zestackowany .

Jako wyniesiona karta liniowa przełącznika rdzeniowego – zgodnie ze standardem IEEE 802.1BR

Urządzenie musi obsługiwać minimum 4000 VLAN 802.1q.

Parametry fizyczne – możliwość montażu w szafie 19”, wielkość urządzenia nie może przekroczyć 1U

Urządzenie musi posiadać funkcjonalność łączenia w stosy z zachowaniem następującej parametrów:

Minimum 12 jednostek w stosie.

Stackowanie musi się odbywać po dedykowanych portach lub portach 10Gbps Ethernet.

Możliwość tworzenia połączeń EtherChannel LACP zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (Cross-stack EtherChannel) – minimum z 8 różnych przełączników w stosie jednocześnie.

Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9216 bajtów (Jumbo Frames)

Urządzenie musi wspierać mechanizm QinQ oraz Selective-QinQ. Funkcja QinQ musi umożliwiać tunelowanie ramek STP BPDU.

Wsparcie dla automatyzacji z wykorzystaniem ANSIBLE.

Zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet).

Obsługa protokołu NTP lub SNTP.

Musi zapewniać routing statyczny oraz dynamiczny: OSPFv2, OSPFv3, RIP, RIP-NG oraz zapewniać obsługę protokołów First-Hop Redundancy – VRRP. Licencje dla tej funkcji są wymagane na tym etapie postępowania.

Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping, PIM-SM, PIM-DM, PIM-SSM. Licencje dla tej funkcji nie są wymagane na tym etapie postępowania.

Wsparcie dla protokołów Per-VLAN Spanning-Tree, IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 250 instancji protokołu STP.

Wsparcie dla funkcji BPDU Guard oraz funkcji wykrywania i zabezpieczenia przed pętlami Layer 2.

Wsparcie dla funkcji Auto-MDI/MDI-X na portach 10/100/1000.

Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP Server oraz wspierać funkcję DHCP Helper.

Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad.

Przełącznik musi obsługiwać następujące mechanizmy bezpieczeństwa:

Minimum 3 poziomów dostępu administracyjnego.

Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL.

Obsługa funkcji Guest VLAN.

Obsługa Private VLAN.

Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.

Możliwość uwierzytelniania użytkowników w oparciu o portal www (WebAuth).

Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC.

Wymagana jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie

Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176.

Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6

Obsługa list kontroli dostępu (ACL).

Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection.

Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.

Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne) .

Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:

Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) .

Implementacja co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu WRR lub SRR lub innego podobnego dla obsługi tych kolejek.

Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).

Możliwość mapowania ruchu do określonych kolejek QoS z wykorzystaniem ACL.

Możliwość ograniczania pasma dostępnego na każdym porcie jednocześnie dla ruchu wychodzącego oraz przychodzącego za pomocą Shapingu lub Policingu.

Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP)

Obsługa protokołu UDLD.

Obsługa protokołu Ethernet Ring – Np. G.8032 lub REP lub inny równoważny.

Obsługa protokołu MVRP lub innego równoważnego (np. VTP).

Obsługa protokołu OpenFlow 1.3 lub nowszego dla współpracy z kontrolerem OpenFlow.

Obsługa VLAN Mapping.

Wsparcie dla AAA z wykorzystaniem serwerów Tacacs oraz RADIUS.

Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli

Urządzenie musi posiadać port konsoli szeregowej RJ 45 oraz port Ethernet typu out-of-band – do zarządzania.

Urządzenie musi być wyposażone w port USB umożliwiający podłączenie pamięci flash z konfiguracją i obrazem.

Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie fizycznym, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego z wykorzystaniem funkcji ERSPAN (warstwa 3 ISO/OSI – tunelowanie kopii ruchu poprzez sieć IP) oraz RSPAN (warstwa 2 ISO/OSI – zdalny VLAN).

Musi być obsługiwana funkcja dzięki której przełącznik wykona upload swojego pliku konfiguracyjnego na zdalny serwer TFTP/SCP po otrzymaniu odpowiednich pakietów SNMP Write. Musi istnieć dodatkowe zabezpieczenie tej funkcji hasłem (np. enable) lub możliwość definiowana listy zaufanych serwerów TFTP/SCP.

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). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją.

Wszystkie licencje dla opisanych funkcji muszą być dostarczone razem z urządzeniami.

Wymagane jest, aby przełączniki posiadały gwarancję producenta minimum przez okres 36 miesięcy z zachowaniem poniższych warunków:

bezpłatne aktualizacje firmware,

wymianę uszkodzonego komponentu z wysyłką następnego dnia roboczego od uznania awarii,

dostęp do bazy wiedzy producenta,

dostęp do TAC producenta (otwieranie tzw. case’ów) – brak limitu otwierania zgłoszeń w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware,

realizacja serwisu w porozumieniu z producentem – tzw. Partner Support. Podmiot realizujący wsparcie musi posiadać certyfikat certyfikowanego partnera serwisowego wydany przez producenta urządzeń. Serwis musi być świadczony w języku Polskim.

Kabel SFP+ DAC –12 szt.

Kabel typu SFP+ (obie końcówki) zgodny z urządzeniami dostarczanymi w ramach tego postępowania.

Prędkość transmisji – 10Gbps.

Kabel typu Active DAC.

Długość kabla – 1 metr.

Kabel objęty gwarancją producenta minimum 36 miesięcy z reżimem wymiany Następny Dzień Roboczy.

Wkładka SFP+ 10G LR – 4 szt. (Zależne od światłowodu jaki tam jest).

Wkładka typu SFP+ zgodna z urządzeniami dostarczanymi w ramach tego postępowania.

Wkładka musi pracować na włóknach Single-Mode (G.652) na odległość nie mniejszą niż 10KM zgodnie ze standardem 10GBaseLR – 10Gbps.

Wkładka musi posiadać złącze LC/PC.

Wkładka musi pracować w zakresie temperatur od 0 to 60\*C.

Wkładka musi obsługiwać diagnostykę cyfrową – DDMi/DOM.

Wkładka musi być objęta gwarancją producenta minimum 36 miesięcy z reżimem wymiany Następny Dzień Roboczy.

1. Firewall – dwie sztuki

Wymagania podstawowe.

Rozwiązanie powinno prezentować informacje o globalnych atakach i zagrożeniach, jak również o atakach ukierunkowanych dla danego sektora.

Proponowane rozwiązanie powinno mieć możliwość pobierania i korelowania informacji o zagrożeniach z wielu źródeł, co najmniej takich jak: stacje końcowe, systemy zabezpieczeń typu firewall, zewnętrzne listy i feedy.

Rozwiązanie powinno pozwalać na wyświetlenie szeregu informacji o danym pliku złośliwym, co najmniej takich jak: czy należy do danej rodziny zagrożeń, czy jest powiązane z kampanią, jakie są jego cechy charakterystyczne, co najmniej: informacje o nawiązywanych połączeniach, wysyłanych zapytaniach DNS, pobieranych plikach, wprowadzanych zmianach w rejestrze.

Proponowane rozwiązanie powinno w sposób automatyczny nadawać priorytety i wagi poszczególnym zdarzeniom w celu identyfikacji unikalnych i krytycznych zdarzeń i IOC (Indicators of Compromise).

Poszczególne cechy charakterystyczne danego złośliwego pliku powinny mieć możliwość bycia oznaczanym za pomocą tagów. Tagi powinny być w sposób automatyczny przypisywane do próbek spełniających dane wymagania. Tagi powinny być dostarczane przez dostawcę rozwiązania w postaci tagów publicznie dostępnych dla wszystkich użytkowników; użytkownicy powinni mieć również możliwość tworzenia własnych tagów, widocznych tylko dla nich (tagi prywatne) oraz współdzielonych z innymi użytkownikami. Powinna istnieć możliwość wygenerowania alarmu w oparciu o typ tagu, jeśli zdarzenie nim oznaczone pojawi się w sieci klienta.

Rozwiązanie powinno umożliwiać sprawdzenie czy w sieci klienta miały miejsce wybrane zdarzenia powiązane z zagrożeniami poprzez integrację z firewallami za pomocą interfejsu API.

Rozwiązanie powinno dostarczać dodatkowe informacje (dotyczące co najmniej pasujących tagów, powiązanych sesji, wyników analizy pliku), na temat zdarzeń w sieci klienta z poziomu GUI firewalla.

Rozwiązanie powinno mieć możliwość eksportowania informacji o wybranych zagrożeniach w formacie CSV w postaci list zawierających co najmniej: zapytania HTTP oraz DNS, informacje o zmianach w kluczach rejestrów, informacje o nawiązanych sesjach, a także metadane SHA256, SHA1 oraz MD5 dla wybranych plików.

Rozwiązanie powinno mieć umożliwiać tworzenia nowych mechanizmów ochrony poprzez eksportowanie informacji o zagrożeniach w postaci list adresów IP, zapytań DNS oraz URL z możliwością zaimportowania do list blokujących na firewallu.

Rozwiązanie powinno umożliwiać integrację z systemami firm trzecich za pomocą API. Poprzez API, rozwiązanie powinno wspierać zapytania w formacie STIX (Structured Threat Indicator eXpression).

System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.

System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 900 Mbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 600 Mbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 120 000 jednoczesnych połączeń.

System zabezpieczeń firewall musi być wyposażony w co najmniej 4 porty Ethernet 10/100/1000, 8 portów 1Gbps SFP.

Interfejsy sieciowe systemu zabezpieczeń firewall muszą działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA.

Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a system zabezpieczeń firewall musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).

System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Interfejsy sieciowe pracujące w trybie transparentnym, L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN.

System zabezpieczeń firewall musi obsługiwać nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.

System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).

Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).

System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.

System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.

Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 900 Mbit/s.

Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).

Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.

Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.

System firewall dać się skonfigurować tak aby mógł pracować jako para HA, możliwość konfiguracji w trybie pracy passiv/active i active/active.

System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.

System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.

System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.

System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.

System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików.

System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.

System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.

System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.

System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.

System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

Wymagane jest, aby Firewall posiadały gwarancję producenta minimum przez okres 36 miesięcy.

**Wymagania podstawowe identyfikacja użytkowników**

System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.

System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.

System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku, gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.

Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.

Wymagania ochrony IPS, AV, anty-spyware, URL, zero-day

System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL.

System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.

System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.

System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.

System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).

System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.

System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.

System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany.

System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.

**Wymagania dodatkowe NAT, DoS, IPSEC VPN, SSL VPN, QoS**

System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.

System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.

System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.

System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.

System zabezpieczeń firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną). Musi istnieć możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci.

System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0.

System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.

System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.

System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.

**Wymagania zarządzanie i raportowanie**

Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.

System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.

System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian, których są autorami.

System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.

System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).

Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.

System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.

System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).

System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 240GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.

System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.

System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.

System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.

System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.

System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.

System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.

System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.

System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.

System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.

Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym.

1. Zasilacz awaryjny (UPS).

UPS 6kVA.

Moc znamionowa (kVA/kW): 6kVA/5.4kW.

Technologia: On-line podwójna konwersja z korekcją współczynnika mocy (PFC).

Napięcie znamionowe: 200/208/220/230/240V 1:1.

Zakres napięcia wejściowego: 176-276V bez obniżenia mocy (pomiędzy 100–276V przy obniżeniu mocy) 1:1.

Napięcie wyjściowe/THDu: 200/208/220/230/240V +/– 1%; THDU <2%.

Zakres częstotliwości wejściowej/THDi 40-70Hz, 50/60Hs automatyczny wybór, standardowo konwerter częstotliwości, THDi < 5%.

Sprawność: do 94% w trybie online, 98%w trybie podwyższonej sprawności.

Współczynnik szczytu/prąd zwarciowy: 90A.

Wartości przeciążeniowe: 102–110% : 120s, 110–125%: 60s, 125–150%: 10s, >150%: 500ms.

Obudowa: możliwość montażu w szafie rack, szyny w komplecie.

Zarządzanie akumulatorami: metoda ładowania z kompensacją temperaturową (wybór użytkownika), automatyczny test baterii, ochrona przed głębokim rozładowaniem, automatyczne rozpoznawanie podłączonych jednostek modułów baterii zewnętrznych.

Interfejs użytkownika: Wielojęzyczny graficzny wyświetlacz LCD.

Gniazda komunikacyjne: 1 sieciowa karta komunikacyjna, 1 port USB, 1 port szeregowy RS232 (porty USB i RS232 nie mogą być używane jednocześnie), 4 styki beznapięciowe (DB9), 1 blok miniaturowych zacisków do zdalnego załączania/wyłączania i 1 do zdalnego wyłączania, 1 port do pracy równoległej DB15.

Poziom hałasu: <45dB.

Certyfikaty: CE, raport CB (TUV), UL.

Minimum 36 miesięcy gwarancji producenta.