Numer postępowania DAZ/ZP/2/2017

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Nazwa zamówienia

Dostawa sprzętu teleinformatycznego.

2. Termin realizacji

Termin realizacji przedmiotu zamówienia 6 tygodni licząc od dnia zawarcia umowy z Wykonawcą.

3. Miejsce dostawy

Miejscem dostawy przedmiotu zamówienia jest siedziba Zamawiającego, tj. ul. ks. I. J. Skorupki 4, 00-546 Warszawa. W ramach dostawy Wykonawca zobowiązany jest również do wniesienia i rozładunku sprzętu do pomieszczenia znajdującego się na parterze budynku,10 metrów od drzwi wejściowych do siedziby Zamawiającego.

Definicje

System informatyczny – system rozumiany jako w pełni działające środowisko Zamawiającego, w skład którego wchodzi sprzęt teleinformatyczny, infrastruktura teleinformatyczna oraz działające w tych środowiskach oprogramowanie komputerowe;

Sprzęt teleinformatyczny – sprzęt telekomunikacyjny i informatyczny rozumiany jako wszelkie urządzenia służące do prawidłowego działania systemu informatycznego Zamawiającego np. urządzenia sieciowe, urządzenia bezpieczeństwa teleinformatycznego, urządzenia transmisji głosu i wideo, urządzenia służące do tworzenia i przechowywania kopii zapasowych danych oraz pozostałe urządzenia szeroko rozumianego sprzętu komputerowego;

Infrastruktura teleinformatyczna – infrastruktura sprzętowa posiadana i aktualnie użytkowana przez Zamawiającego rozumiana jako aktywne i pasywne urządzenia sieciowe, elementy okablowania strukturalnego budynku, elementy infrastruktury bezpieczeństwa (zapory sieciowe, IPS, urządzenia do szyfrowania transmisji danych itp.) oraz pozostałe urządzenia pracujące w sieci Zamawiającego;

W kontekście zamówienia Zamawiający posiada:

- Urządzenia aktywne sieci – przełączniki sieciowe (switch) HP 6600ml (wersja firmware K.15.17.0007), HP 5406zl (wersja firmware K.15.16.0011) i HP 2910al (wersja firmware W.15.14.0012),
- Zapory sieciowe Palo Alto PA-3020,
- Standardowe szafy „rack" 19",
- Okablowanie strukturalne miedziane kategorii 5e,
- Okablowanie szkieletowe oparte na kablach światłowodowych jednomodowych oraz wielomodowych.

Numer postępowania DAZ/ZP/2/2017

4. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa sprzętu teleinformatycznego do siedziby Zamawiającego, w celu rozbudowy istniejącej i działającej infrastruktury teleinformatycznej Zamawiającego oraz w celu zakupu nowych urządzeń przeznaczonych do pracy w obecnej infrastrukturze teleinformatycznej Zamawiającego.

Przedmiot zamówienia został podzielony na 3 części, jak niżej:

1) **Część zamówienia nr 1 – Dostawa urządzeń sieciowych:**
   a) dostawa przełączników sieciowych, modułów i kabli połączeniowych do przełączników sieciowych (w ramach rozbudowy infrastruktury teleinformatycznej Zamawiającego);
   b) dostawa bramek VoIP do obsługi urządzeń analogowych w infrastrukturze VoIP;
   c) dostawa zapory sieciowej (w ramach rozbudowy systemu zapory sieciowej Zamawiającego).

2) **Część zamówienia nr 2 – Dostawa sprzętu telekomunikacyjnego:**
   a) dostawa 200 sztuk aparatów telefonicznych obsługujących technologię VoIP.

3) **Część zamówienia nr 3 - Dostawa jednostki pamięci taśmowej:**
   a) dostawa biblioteki taśmowej.

4.1. Wymagania stawiane wszystkim częściom przedmiotu zamówienia

1) Wszystkie elementy składowe dostarczonego sprzętu teleinformatycznego muszą być fabrycznie nowe, oryginalnie zapakowane i pochodzić z autoryzowanego źródła przeznaczonego do dystrybucji na terytorium Unii Europejskiej;
2) Sprzęt teleinformatyczny musi współpracować z istniejącą infrastrukturą teleinformatyczną Zamawiającego:
3) Wykonawca dostarczy niezbędne elementy montażowe i połączeniowe do infrastruktury Zamawiającego wynikające z funkcji i parametrów dostarczanego sprzętu teleinformatycznego;
4) Dostarczone urządzenia nie mogą być wyprodukowane przed dniem 1 stycznia 2016 roku;
5) Sprzęt teleinformatyczny musi być wyposażony w najnowszą wersję oprogramowania wewnętrznego (firmware), dostępną w dniu dostawy do Zamawiającego.

5. Szczegółowy opis poszczególnych części zamówienia

5.1. Część zamówienia nr 1 – Dostawa urządzeń sieciowych:

a) Dostawa przełączników sieciowych, modułów oraz kabli połączeniowych do przełączników sieciowych (w ramach rozbudowy infrastruktury teleinformatycznej Zamawiającego)

Przedmiotem zamówienia jest dostawa 7 sztuk przełączników sieciowych, 2 sztuk modułów do przełączników HP PROCURVE 5406zl, 14 sztuk modułów SFP 1G, 16 sztuk modułów SFP+ 10G (w tym 2 zapasowe moduły) wraz z 24 szt. kablami połączeniowymi do przełączników sieciowych, w ramach rozbudowy istniejącej infrastruktury teleinformatycznej Zamawiającego.

Posiadana przez Zamawiającego infrastruktura oparta jest na przełącznikach sieciowych firmy HP PROCURVE 2910al - przełączniki piętrowe oraz HP PROCURVE 5406zl – przełączniki core'owe.

Przełączniki:

Dostarczone przełączniki muszą spełniać co najmniej następujące wymagania funkcjonalne:

- musi posiadać 48 portów sieciowych „48 x 10/100/1000 (PoE+)";
- musi posiadać 4 porty SFP+ „4 x 1 Gigabit / 10 Gigabit SFP+ (uplink)";
- musi mieć możliwość montażu w szafie rack 19";
- wymagane jest aby wszystkie dostarczone przełączniki były obsługiwane w zakresie monitoringu i zarządzania przez posiadane przez Zamawiającego oprogramowanie do zarządzania infrastrukturą sieciową PCM w wersji 3. W szczególności wymagane jest wsparcie w zakresie: wykrywania urządzeń i prezentacji ich topologii, alarmów, serwera syslog, archiwizacji, przywracania i porównywania konfiguracji, aktualizacji oprogramowania, konfiguracji VLAN, konfiguracji ACL, konfiguracji QoS. Dopuszcza się aktualizację do najnowszej wersji oprogramowania zarządzającego, przy czym zachowana musi być powyższa funkcjonalność zarówno dla nowego jak i już posiadanego sprzętu.

Moduły:

Dostarczone moduły muszą pozwolić na połączenie z nowo dostarczonymi przełącznikami piętrowymi połączeniami światłowodowymi 10Gbit/s od przełącznika głównego Zamawiającego (HP 5406zl) i 1Gbit/s od przełącznika zapasowego Zamawiającego (HP 5406zl) - w przełącznikach Zamawiającego są wolne sloty na moduły).

Dostarczone moduły Gbic muszą być dedykowane do pracy w dostarczonych urządzeniach/modułach zapewniające prędkości transmisji 10Gbit/s od przełącznika głównego i 1Gbit/s od przełącznika zapasowego.

Wykaz urządzeń w ramach dostawy przedstawia Tabela nr 1.

Tabela nr 1.

Lp.	Nazwa towaru *	Kod towaru*	Ilość (sztuki)
1.	Przełącznik sieciowy Aruba 2930F 48G PoE+ 4SFP+ Switch	JL256A	7
2.	Moduł GBIC HPE X132 10G SFP+ LC SR Transceiver	J9150A	16
3.	Moduł GBIC HPE X121 1G SFP LC SX Transceiver	J4858C	14
4.	Moduł HPE 8-port 10GbE SFP+ v2 zl Module	J9538A	1
5.	Moduł HPE 24-port SFP v2 zl Module	J9537A	1
6.	Kable światłowodowe „Patchcord multimode 1m LC-SC"	-	24

* Zamawiający dopuszcza zaoferowanie rozwiązania równoważnego do przedstawionego w Tabeli nr 1.

Warunki gwarancyjne: dostarczony sprzęt sieciowy musi być objęty minimum 36 miesięcznym okresem gwarancyjnym w miejscu eksploatacji tzw. „on-site".

*** w przypadku zaoferowania rozwiązania równoważnego Zamawiający oczekuje rozwiązania spełniającego poniższe minimalne wymagania funkcjonalne:**

Opis równoważności dla urządzenia w pkt 1 Tabeli nr 1 – kod: JL256A	
Rodzaj urządzenia	Przełącznik - 48 porty - L3 - wieżowy
Rodzaj obudowy	Montowany w szafie rack 1U
Podtyp	Gigabit Ethernet
Porty	48 x 1000Base-T - RJ-45 - PoE+ 4 x Gigabit / 10Gbit LAN - SFP+ 1 x szeregowo (konsola)
Gniazda rozszerzeń	1 (całkowity) / 1 (wolna) x gniazdo rozszerzające
Ilość zainstalowanych modułów (maks)	0 (zainstalowane) / 4 (maks.)
Zasilanie przez Ethernet	PoE+
Wykonanie	Przepustowość:110 Mpps Zdolność przełączania:170 Gbps Opóźnienie (1 Gbps):max 4.0 µs Opóźnienie (10 Gbps):max 2.0 µs
Pojemność	Wielkość ramki Jumbo:9220 Wpisy w tabeli routingu IPv4:10000 Wpisy w tabeli routingu IPv6:5000
Wielkość tablicy adresów MAC	32K wpisów
Protokół routingu	OSPF,RIP,RIP-1,RIP-2,BGP,IGMPv2,IGMP,OSPFv2,static IP routing,IGMPv3,OSPFv3,routing statyczny IPv4,routing statyczny IPv6,RIPng,MLD,CIDR
Protokół zdalnego zarządzania	SNMP 1,SNMP 2,RMON 1,SNMP,Telnet,SNMP 3,SNMP 2c,SSH,SSH-2,CLI,XRMON
Algorytm kodowania	MD5,SSL
Metoda identyfikacji	RADIUS,PAP,CHAP,TACACS,TACACS+
Cechy	Sterowanie przepływem, możliwy pełen dupleks, obsługa DHCP, obsługa BOOTP, obsługa ARP, obsługa VLAN, nasłuchiwanie IGMP, obsługa Syslog, obsługa DiffServ, obsługa IPv6, obsługa SNTP, sFlow, obsługa protokołu Spanning Tree (STP), obsługa protokołu Multiple Spanning Tree Protocol (MSTP), obsługa list dostępu (ACL), Quality of Service (QoS), obsługa Jumbo Frames, serwer DHCP, STP Root Guard, Uni-Directional Link Detection (UDLD), obsługuje LLDP, Link Aggregation Control Protocol (LACP), Management Information Base (MIB), MAC address lockout, dynamiczna ochrona ARP, ochrona DHCP, Dynamic VLAN Support (GVRP), Multiple VLAN Registration Protocol (MVRP), Neighbor Discovery Protocol (NDP), Class of Service (CoS), Type of Service (ToS), obsługuje OpenFlow,

	zabezpieczenie procesora centralnego, Internet Control Message Protocol (ICMP), ICMP Router Discovery Protocol (IRDP), Virtual Extensible LAN (VXLAN), Management Information Base (MIB) II
Zgodność z normami	IEEE 802.1D,IEEE 802.1Q,IEEE 802.1p,IEEE 802.3af,IEEE 802.3x,IEEE 802.3ad (LACP),IEEE 802.1w,IEEE 802.1x,IEEE 802.1s,IEEE 802.1ad,IEEE 802.1v,IEEE 802.1ab (LLDP),IEEE 802.3at,IEEE 802.3az,IEEE 802.1AX
RAM	1 GB DDR3 SDRAM
Pamięć fleszowa	4 GB
Warunki gwarancyjne	dostarczony sprzęt sieciowy musi być objęty minimum 36 miesięcznym okresem gwarancyjnym w miejscu eksploatacji tzw. „on-site”.
Zarządzanie infrastrukturą	wymagane jest aby wszystkie dostarczone przełączniki były obsługiwane w zakresie monitoringu i zarządzania przez posiadane przez Zamawiającego oprogramowanie do zarządzania infrastrukturą sieciową PCM w wersji 3. W szczególności wymagane jest wsparcie w zakresie: wykrywania urządzeń i prezentacji ich topologii, alarmów, serwera syslog, archiwizacji, przywracania i porównywania konfiguracji, aktualizacji oprogramowania, konfiguracji VLAN, konfiguracji ACL, konfiguracji QoS. Dopuszcza się aktualizację do najnowszej wersji oprogramowania zarządzającego, przy czym zachowana musi być powyższa funkcjonalność zarówno dla nowego jaki i już posiadanego sprzętu. Dostosowanie oprogramowania PCM (lub jego zaktualizowanej wersji) do obsługi dostarczonego sprzętu sieciowego leży po stronie Wykonawcy.

Opis równoważności dla urządzenia w pkt 2 Tabeli nr 1 – kod: J9150A	
Typ interfejsu:	SFP+
Szybkość przesyłania danych:	10000 Mbit/s
Złącze światłowodowe:	LC
Standardy komunikacyjne:	IEEE 802.3ae
Maksymalny dystans transferu:	300 m
Długość fali:	850 nm
Typ przewodu:	Multi-mode

Opis równoważności dla urządzenia w pkt 3 Tabeli nr 1 – kod: J4858C	
Typ interfejsu:	SFP
Szybkość przesyłania danych:	1000 Mbit/s
Złącze światłowodowe:	LC
Standardy komunikacyjne:	1000BASE-SX

Maksymalny dystans transferu:	550 m
Typ przewodu:	Multi-mode

Opis równoważności dla urządzenia w pkt 4 Tabeli nr 1 – kod: J9538A
Moduł rozbudowy pasujący i działający w przełącznikach HP 5406zl, wyposażony w 8 portów SFP+ 10GbE.

Opis równoważności dla urządzenia w pkt 5 Tabeli nr 1 – kod: J9537A
Moduł rozbudowy pasujący i działający w przełącznikach HP 5406zl wyposażony w 24 porty SFP.

Warunki gwarancyjne dla urządzeń równoważnych: dostarczony sprzęt sieciowy musi być objęty minimum 36 miesięcznym okresem gwarancyjnym w miejscu eksploatacji tzw. „on-site".

b) Dostawa bramek VoIP do obsługi urządzeń analogowych w infrastrukturze VoIP

Przedmiotem zamówienia jest dostawa 7 sztuk (jeden model) bramek analogowych VoIP FXS (Foreign eXchange Subscriber). Dostarczony sprzęt umożliwi wykorzystanie posiadanych urządzeń tj. analogowych aparatów telefonicznych i urządzeń faksowych Zamawiającego w infrastrukturze telefonii VoIP Zamawiającego.

Bramki analogowe VoIP FXS muszą spełniać następujące wymogi techniczne i bezpieczeństwa wynikające z konfiguracji systemu teleinformatycznego Zamawiającego, w szczególności muszą:

1. posiadać 16 portów analogowych FXS RJ11 oraz 1 port analogowy 50-pinowy Telco,
2. posiadać interfejs sieciowy 10M/100M/1000Mbps,
3. obsługiwać kodeki G.711, G723.1, G.726, G729 A/B,
4. obsługiwać połączenia faksowe zgodnie z ITU T.38 Grupy 3 do 14.4kbps, z możliwością automatycznego przełączenia na G.711,
5. obsługiwać protokół 802.1p,
6. obsługiwać protokół 802.1q,
7. mieć możliwość usuwania echa G.168,
8. posiadać sygnalizacja SIP po UDP/TCP/TLS,
9. posiadać automatyczną konfigurację po protokołach TFTP, http, HTTPS,
10. posiadać 16 kont SIP (Session Initiation Protocol) z możliwością niezależnego skonfigurowania konta dla każdego portu analogowego,
11. posiadać możliwość zarządzania przez wbudowany serwis WWW (HTTPS), TR-069 (protokół zarządzający CPE (Customer Premise Equipment) WAN),
12. posiadać możliwość montażu w 19" szafie rack.

Warunki gwarancyjne: Dostarczone bramki muszą być objęte minimum 24 miesięcznym okresem gwarancyjnym.

c) dostawa zapory sieciowej (w ramach rozbudowy systemu zapory sieciowej)

Przedmiotem zamówienia jest dostawa 1 sztuki zapory sieciowej (firewall) wraz z usługą co najmniej 3 letniej subskrypcji dostępu do bazy zagrożeń oraz co najmniej 3 letnim wsparciem technicznym dla urządzenia w celu rozbudowy istniejącej infrastruktury teleinformatycznej Zamawiającego.

Numer postępowania DAZ/ZP/2/2017

Posiadane przez Zamawiającego urządzenia zapór sieciowych oparte są na produktach firmy Palo Alto, w związku z tym Zamawiający w celu utrzymania spójności platformy (systemu do zarządzania zaporami) planuje rozbudowę systemu zapory sieciowej przez doposażenie w urządzenie Palo Alto Networks PA-220 lub równoważną**.
Poprzez spójność platformy, Zamawiający rozumie, dostępność dla posiadanych zapór sieciowych i nowego urządzenia zapory sieciowej wspólnej platformy do zarządzania tymi urządzeniami.

Wykaz urządzeń w ramach dostawy przedstawia Tabela nr 2.

Tabela nr 2.

Lp.	Nazwa towaru**	Kod towaru**	Liczba (sztuki)
1.	Urządzenie Palo Alto Networks PA-220	PA-220	1
2.	Usługa Threat prevention subscription 3-year prepaid, PA-220	-	1
3.	Usługa Partner enabled premium support 3-year prepaid, PA-220	-	1

**Zamawiający dopuszcza zaoferowanie rozwiązania równoważnego w stosunku do wykazanego w Tabeli nr 2

Warunki gwarancyjne: Dostarczona zapora sieciowa musi być objęta minimum 36 miesięcznym wsparciem technicznym producenta.

<u>W przypadku zaoferowania rozwiązania równoważnego Zamawiający oczekuje rozwiązania spełniającego poniższe minimalne wymagania funkcjonalne:</u>**

1) Wymagania podstawowe

System zabezpieczeń firewall musi być dostarczony jako dedykowane 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 500 Mbps dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 150 Mbps dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 64 000 jednoczesnych połączeń.
System zabezpieczeń firewall musi być wyposażony w co najmniej 8 portów Ethernet 10/100/1000.
System zabezpieczeń firewall musi 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 urządzenia musi być ustalany w konfiguracji interfejsu sieciowego a system 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. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.
System zabezpieczeń firewall musi obsługiwać nie mniej niż 3 wirtualne routery posiadające odrębne tabele routingu i umożliwiające 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 500 Mbps.
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 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 powinien posiadać 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.

2) 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. Funkcjonalność musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.
System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z nagłówka X-Forwarded-For 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 musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.

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

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 modułu IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność 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 funkcjonalność 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 funkcjonalność automatycznego przeglądania logowanych informacji oraz wyciągania 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 posiadać funkcjonalność wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.

4) 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 funkcjonalność 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 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.

5) 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 32 GB. 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 musi 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.

6) Wymagania gwarancyjne i serwisowe

Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym.
Gwarancja, wsparcie producenta oraz subskrypcja definicji antywirusowych i IPS na 3 lata

7) W przypadku rozwiązania równoważnego Zamawiający oczekuje pełnej integracji urządzenia z funkcjonującymi w sieci teleinformatycznej Zamawiającego zaporami sieciowymi (Palo Alto) oraz przeprowadzenie w siedzibie Zamawiającego co najmniej dwudniowego (8 godzin) szkolenia dla 2 administratorów z zakresu konfiguracji dostarczonego urządzenia w terminie wyznaczonym przez Zamawiającego po zrealizowanej przez Wykonawcę dostawie.
8) **Warunki gwarancyjne dla rozwiązania równoważnego:** Dostarczona zapora sieciowa musi być objęta minimum 36 miesięcznym wsparciem technicznym producenta.

5.2. Część zamówienia nr 2 – Dostawa sprzętu telekomunikacyjnego

a) dostawa 200 sztuk aparatów telefonicznych obsługujących technologię VoIP

Przedmiotem Części 2 zamówienia jest dostawa 200 sztuk (jeden model) aparatów telefonicznych w technologii Voice over IP wraz z kablami połączeniowymi.

Dostarczone aparaty telefoniczne stanowić będą podstawę nowego systemu telefonii stacjonarnej, mającego zastąpić obecne rozwiązanie oparte na systemowej centrali telefonicznej.

Aparaty telefoniczne muszą spełniać następujące wymogi techniczne i bezpieczeństwa wynikające z konfiguracji systemu informatycznego Zamawiającego, a w szczególności muszą:

1. obsługiwać co najmniej 6 kont SIP,
2. posiadać wbudowany przełącznik sieciowy GigabitEthernet umożliwiający połączenie stacji roboczej z siecią LAN poprzez aparat telefoniczny jednym przewodem sieciowym,
3. obsługiwać protokół 802.1q,
4. obsługiwać protokół 802.1p,
5. obsługiwać protokół 802.3af,

6. posiadać automatyczną konfiguracja z wykorzystaniem protokołów TFTP, HTTP, HTTPS,
7. obsługiwać protokół 802.1x w trybie EAP-PEAPv0/MSCHAPv2 i konfiguracji sieci wykorzystującej między innymi przełączniki sieciowe **HP ProCurve 2910al** (wersja firmware W.15.14.0012) oraz MS Network Policy Server (NPS),
8. posiadać możliwość dołączenia opcjonalnego modułu sekretarskiego - zwiększającego liczbę dodatkowych programowalnych przycisków,
9. wszystkie dostarczone telefony muszą być w tej samej kolorystyce, dopuszczalne przez Zamawiającego kolory telefonów: czarny, odcienie szarości;

Warunki gwarancyjne: Dostarczone aparaty telefoniczne muszą być objęte minimum 24 miesięcznym okresem gwarancyjnym.

5.3. Część zamówienia nr 3 – Dostawa nowej biblioteki taśmowej

Przedmiotem Części 3 zamówienia jest dostawa 1 sztuki biblioteki taśmowej spełniającej poniższe minimalne parametry i wymagania, w szczególności dostarczona biblioteka taśmowa musi:

1. posiadać 24 „sloty” na kasety w dwóch magazynkach po 12 szt.;
2. posiadać 1 „mailslot”;
3. posiadać 1 napęd LTO-7;
4. posiadać możliwość obsługi 2 napędów LTO-7;
5. posiadać standard zapisu: LTO-7;
6. posiadać rodzaj obudowy do montażu w szafie RACK wysokość max. 2U;
7. posiadać typ interfejsu 8Gb Fibre Channel (LC);
8. posiadać interfejs zarządzający Ethernet;
9. posiadać całkowitą pojemność urządzenia 144 TB (nieskompresowana) / 360 TB (skompresowana);
10. obsługiwać kasety taśmowe (odczyt i zapis): LTO-6, LTO-7;
11. posiadać możliwość zarządzania przez stronę www oraz przez panel LCD;
12. posiadać zasilanie AC 120/230 V (50/60 Hz);
13. być wyposażona w komplet kabli połączeniowych/zasilających min. 1,5m, FC min. 2m;
14. posiadać w zestawie 2 kasety czyszczące;
15. posiadać w zestawie 48 kaset LTO-7;
16. posiadać komplet naklejek z kodami kreskowymi dla LTO-7 (min. 100 szt.) + naklejki na kasety czyszczące;

Warunki gwarancyjne: Dostarczona biblioteka taśmowa musi być objęta minimum 36 miesięcznym okresem gwarancyjnym w miejscu eksploatacji tzw. „on-site”.

---

6. ROZWIĄZANIE RÓWNOWAŻNE

6.1. Wszędzie tam, gdzie przedmiot zamówienia został opisany przez wskazanie nazw znaków towarowych, patentów lub pochodzenia a także norm, Zamawiający dopuszcza zaoferowanie przez Wykonawcę rozwiązania równoważnego.

Wszystkie materiały, urządzenia, elementy wyposażenia przedstawione w przedmiotowej dokumentacji i opisane przez wskazanie znaków towarowych, patentów lub pochodzenia a także norm, należy traktować jako rozwiązania przykładowe o modelowych: parametrach technicznych i użytkowych, właściwościach charakterystycznych i właściwościach estetycznych, standardach określonych dla materiałów, urządzeń, elementów wyposażenia oraz warunków gwarancyjnych i serwisowych.

6.2. Przez rozwiązanie równoważne dla wyspecyfikowanego przedmiotu zamówienia rozumie się taki, który w sposób poprawny współpracuje z infrastrukturą teleinformatyczną Zamawiającego, a jego zastosowanie nie wymaga żadnych nakładów (finansowych, programistycznych sprzętowych) związanych z dostosowaniem infrastruktury teleinformatycznej Zamawiającego lub rozwiązania równoważnego oraz realizuje wszystkie funkcje i posiada wszystkie cechy określone w SIWZ.
Dopuszcza się zastosowanie rozwiązań „równoważnych" polegających na zastosowaniu innych materiałów, urządzeń, elementów wyposażenia niż podane w dokumentacji pod warunkiem zapewnienia wszystkich parametrów, właściwości i standardów oraz warunków gwarancyjnych i serwisowych nie gorszych niż określonych w opisie przedmiotu zamówienia oraz SIWZ.

6.3. W przypadku, gdy Wykonawca zaoferuje rozwiązanie równoważne, zobowiązany jest wykazać jego równoważność w stosunku do opisanego przedmiotu zamówienia.

6.4. W celu potwierdzenia, że oferowane rozwiązanie równoważne odpowiada wymaganiom określonym w SIWZ, Zamawiający wymaga złożenia przez Wykonawcę oświadczenie o którym mowa w SIWZ oraz stosownych dokumentów, potwierdzających spełnianie wszystkich wymagań określonych w opisie przedmiotu zamówienia i SIWZ.

6.5. W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy systemu informatycznego Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem systemu informatycznego Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie systemu informatycznego Zamawiającego również po odinstalowaniu oprogramowania równoważnego.