## Załącznik nr 2 do SIWZ

***Zestawienie parametrów techniczno-użytkowych przedmiotu zamówienia***

**CZĘŚĆ I ZAMÓWIENIA - DOSTAWA SPRZĘTU SIECIOWEGO**

Wymagane parametry są wartościami minimalnymi

|  |
| --- |
| 1. **SWITCH** – ilość **1 sztuka** |
| Producent (marka):…………………………………………………………………………………………….……………………………  Model:…………………………………………………………………………………………………………………………….  Kraj pochodzenia:……………………………………………………………………………………………………………  /*Wykonawca zobowiązany jest do podania nazwy producenta, modelu urządzenia i kraju pochodzenia*/ |

**Sprzęt musi być fabrycznie nowy, wyprodukowany w 2019 roku.**

**Wymagania ogólne**

1. Przełącznik powinien mieć budowę modułową umożliwiającą dostosowanie ilości i typu portów do potrzeb zamawiającego oraz przyszłą rozbudowę poprzez dołożenia lub zmianę modułów.

Przełącznik powinien umożliwiać posiadanie portów:

* 1. 288 portów gigabitowych miedzianych;
  2. 288 portów gigabitowych miedzianych PoE+;
  3. 288 portów SFP;
  4. 96 portów 10-gigabitowych SFP+;
  5. 96 portów miedzianych 1/2,5/5/10-gigabitowych z negocjacją prędkości oraz obsługą standardu PoE+;
  6. 24 portów 40-gigabitowych;
  7. lub kombinacji powyższych typów portów.

1. Obudowa wieżowa Rack o wysokości maksymalnie 7U umożliwiająca instalację w szafie 19", głębokość urządzenia nie większa jak 46 cm.
2. Przełącznik należy wyposażyć w stosowne moduły tak aby sumarycznie posiadał następującą konfigurację portów:
   1. 24 porty RJ-45 z autonegocjacją 10/100/1000 (IEEE 802.3 typu 10Base-T, IEEE 802.3u typu 100Base-TX, IEEE 802.3ab typu 1000Base-T); duplex 10Base-T/100Base-TX: pół lub pełny duplex; 1000Base-T - tylko pełny;
   2. 8 portów 10Gigabit Ethernet SFP+ z możliwością użycia wkładek WDM;
   3. 1 port szeregowy konsoli RJ45 lub USB;
   4. 1 port zarządzający RJ45 ethernet OOBM;
   5. Przynajmniej osiem wolnych slotów na dodatkowe moduły;
   6. Dostarczone urządzenie musi być obsadzone następującymi modułami: 6 szt. SFP+ 10G LC SM, 6 szt. SFP+ 1x 10G LC SM WDM, 6 szt. SFP 1G LC SM, 6 szt. SFP 1G LC MM oraz kable światłowodowe typu patchcord: 8 szt. SC/UPC-LC/UPC 9/125 dupleks dł. min 1.5 m, 8 szt. SC/UPC-LC/UPC simplex dł. Min 1.5 m, 8 szt. SC/UPC-LC/UPC MM 50/125 duplex dł. min 1.5m.
3. Przełącznik musi posiadać moduł zarządzający pełniący funkcję kontrolera całości oraz architekturę nie blokującą zdolną obsłużyć ruch ze wszystkich portów jednocześnie w obu kierunkach.
4. Moduł zarządzający musi umożliwiać redundancję i jego wymianę w przypadku uszkodzenia w trybie hot-swap. Przełącznik należy dostarczyć wraz z drugim redundantnym modułem zarządzającym (co powoduje zdublowanie portów konsolowego i OOBM).
5. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 2 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster).
6. Zarządzanie:
   1. CLI;
   2. WWW;
   3. telnet/ssh;
   4. pozapasmowe konsolowe (port szeregowy RS-232C - RJ45);
   5. dedykowany port Ethernet do zarządzania OOBM;
   6. możliwość scentralizowanego zarządzania zarówno przez dedykowane oprogramowanie producenta jak i chmurowo.
7. Warstwa przełączania – Layer 3.
8. Rozmiar tablicy adresów MAC- minimum 64000.
9. Tablica routingu:
   1. 10000 wpisów dla IPv4;
   2. 5000 wpisów dla IPv6;
10. Obsługa protokołów routingu:
    1. routing statyczny;
    2. RIP v1;
    3. RIP v2;
    4. OSPF;
    5. OSPFv3;
    6. VRRP;
    7. PIM-SM;
    8. PIM-DM;
    9. BGP;
    10. Virtual Router Redundancy Protocol (VRRP).
11. Prędkość magistrali: 1920 Gbps.
12. Przepustowość: 1140 Mpps.
13. Parametry jednostki centralnej przełącznika:
    1. Dual Core, taktowanie procesora minimum 1200MHz;
    2. Pamięć flash minimum 16MB;
    3. Pamięć SD minimum 1GB;
    4. Pamięć RAM minimum 4GB DDR3.
14. Opóźnienie poniżej 2.8 µs dla 1000 Mbit.
15. Bufor pakietów minimum 13 MB na moduł.
16. VLAN
    1. Pełna zgodność z IEEE 802.1Q;
    2. 4094 VLAN Ids;
    3. Do 4094 VLANów jednocześnie;
    4. Obsługa MAC forwarding table per vlan;
    5. Wsparcie dla IEEE 802.1ad Q-in-Q;
    6. Wsparcie dla VxLAN.
17. Funkcje wysokiej dostępności:
    1. Spanning Tree (802.1d);
    2. Rapid Convergence Spanning Tree (802.1w);
    3. Muliple Spanning Tree (802.1s);
    4. Rapid Per-VLAN Spanning Tree (RPVST+);
    5. GVRP and MVRP.
18. Agregacja portów zgodna z 802.3ad LACP:

Obsługa dystrybuowanych łączy agregowanych LACP – łączy agregowanych wychodzących z dwóch, różnych, niezależnych i oddzielnie zarządzanych (nie połączonych w stos) przełączników (tzw. Multi-chassis Link Aggregation, MLAG, MC-LAG, Distributed Trunking).

1. Funkje QoS:
   1. priorytetyzacja zgodna z 802.1p;
   2. Class of Service (CoS) priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port and DiffServ ToS;
   3. Layer 4 prioritization TCP/UDP;
   4. wsparcie dla 4 kolejek;
   5. rate-limiting;
   6. Voice VLAN;
   7. IP SLA for voice.
2. Monitorowanie:
   1. RMON 4 grupy statistics, history, alarm, events;
   2. SFLOW;
   3. XRMON.
3. Inne funkcje i funkcjonalności:
   1. LLDP;
   2. LLDP-MED;
   3. dual flash images;
   4. obsługa ramek typu Jumbo;
   5. iSCSI;
   6. DHCP snooping;
   7. DHCP Server;
   8. BPDU Guard;
   9. BPDU Protection;
   10. port isolation;
   11. wsparcie dla IPv4 i Ipv6;
   12. Tunneled node dla ruchu z AP;
   13. Zero Touch Provisioning;
   14. Access control lists (ACL);
   15. Dynamic ARP protection;
   16. Bidirectional Forwarding Detection (BFD);
   17. Unidirectional link detection (UDLD);
   18. 802.1AE MACsec.
4. Autentyfikacja użytkowników:
   1. IEEE 802.1X;
   2. Web-based authentication;
   3. Supports MAC-based authentication;
   4. RADIUS/TACACS+ suport.
5. Zasilanie z zasilaczy hot-swap. Przełącznik powinien posiadać cztery sloty na zasilacze i umożliwiać instalację zasilaczy o różnych mocach w zależności od zapotrzebowania na moc PoE. Przełącznik należy dostarczyć z dwoma zasilaczami minimum 1100W każdy. Zasilacze powinny spełniać normę 80Plus Gold.
6. Chłodzenie aktywne z przepływem powietrza w kierunku przód-tył obudowy. Wentylatory na wymiennym module hot-swap.
7. Przełącznik musi być przystosowany do środowiska pracy od 0°C do 45°C.
8. **Gwarancja i wsparcie techniczne producenta:**

**Lifetime zapewniające dostęp do poprawek i aktualizacji tak długo jak urządzenie jest od zaprzestania produkcji. Gwarancja wymiany wadliwego urządzenia także Lifetime w trybie NBD z wysyłką urządzenia na wymianę następnego dnia roboczego od zgłoszenia.**

1. Producent musi posiadać w ofercie jednorodny system zarządzania pozwalający na konfigurację, zarządzanie i monitoring wszystkimi wyspecyfikowanymi urządzeniami. System zarządzania nie jest przedmiotem postępowania, ale musi być dostępny na dzień składania oferty i dostawy.

|  |
| --- |
| 1. **SYSTEM BEZPIECZEŃSTWA SKŁADAJĄCY SIĘ Z DWÓCH URZĄDZEŃ PRACUJĄCYCH W KLASTRZE HA** – ilość **1 sztuka** |
| Producent (marka):…………………………………………………………………………………………….……………………………  Model:…………………………………………………………………………………………………………………………….  Kraj pochodzenia:……………………………………………………………………………………………………………  /*Wykonawca zobowiązany jest do podania nazwy producenta, modelu urządzenia i kraju pochodzenia*/ |

**Sprzęt musi być fabrycznie nowy, wyprodukowany w 2019 roku.**

## Zakup kontynuacji usług wsparcia i gwarancji producenta oraz licencji funkcji bezpieczeństwa dla urządzeń zabezpieczających usługi i sieci komputerową (firewall sprzętowe pracujące w klastrach) wraz z dostawą licencji i ich kompletną instalacją na pracującym sprzęcie Zamawiającego.

# Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

# Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

# Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:

* 10 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 2 gniazdami SFP+ 10 Gbps.

1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. 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.

1. Dostarczone urządzenie musi być obsadzone następującymi modułami: 2 szt. SFP+ 10G LC SM, 2 szt. SFP+ 1x 10G LC SM WDM, 4 szt. SFP 1G LC SM, 4 szt. SFP 1G LC MM oraz kable światłowodowe typu patchcord: 6 szt. SC/UPC-LC/UPC 9/125 dupleks dł. min 1.5 m, 4 szt. SC/UPC-LC/UPC simplex dł. Min 1.5 m, 6 szt. SC/UPC-LC/UPC MM 50/125 duplex dł. min 1.5m

# Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 8 mln jednoczesnych połączeń oraz 390.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 36 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 15 Gbps.
4. Wydajność szyfrowania IPSec VPN: nie mniej niż 20 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 10 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 7 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 8 Gbps.

# Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
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.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

# Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

# Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

* Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu 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.

1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

# Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

* Routingu statycznego.
* Policy Based Routingu.
* Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

1. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

# Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

# Kontrola Antywirusowa

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. 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.

# Ochrona przed atakami

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 6500 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.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

# Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

# Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

# Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

# Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

# Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
3. Musi istnieć możliwość logowania do serwera SYSLOG.

# Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.
* ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
* ICSA dla funkcji SSL VPN.

# Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. 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 na okres [12] miesięcy.

# Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. [12] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

|  |
| --- |
| 1. **CENTRALNY SYSTEM LOGOWANIA, REJESTRACJI I KORELACJI** – ilość **1 sztuka** |
| Producent (marka):…………………………………………………………………………………………….……………………………  Model:…………………………………………………………………………………………………………………………….  Kraj pochodzenia:……………………………………………………………………………………………………………  /*Wykonawca zobowiązany jest do podania nazwy producenta, modelu urządzenia i kraju pochodzenia*/ |

**Sprzęt musi być fabrycznie nowy, wyprodukowany w 2019 roku.**

# Wymagania Ogólne

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

# Interfejsy, Dysk, Zasilanie:

1. System musi dysponować co najmniej:

* 2 portami Gigabit Ethernet RJ-45.

1. Rozwiązanie musi dysponować powierzchnią dyskową min. 4 TB.

# Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 100 GB logów na dzień.
2. System musi być w stanie przeanalizować minimum 3000 logów na sekundę.
3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 150 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

# Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
4. Listę najczęściej wykrywanych ataków.
5. Listę najbardziej aktywnych użytkowników.
6. Listę najczęściej wykorzystywanych aplikacji.
7. Listę najczęściej odwiedzanych stron www.
8. Listę krajów , do których nawiązywane są połączenia.
9. Listę najczęściej wykorzystywanych polityk Firewall.
10. Informacje o realizowanych połączeniach IPSec.
11. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
12. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
13. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

# Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

# Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

* Malware.
* Aplikacje sieciowe.
* Email.
* IPS.
* Traffic.
* Systemowe: utracone połączenie VPN, utracone połączenie sieciowe.

# Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
3. System musi umożliwiać definiowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

# Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

UWAGA: Podane parametry sprzętu i elementów zamówienia, są wartościami minimalnymi wymaganymi przez zamawiającego. Wykonawca zobowiązany jest podać w nazwy producenta nazwy, modelu urządzenia i kraju pochodzenia oferowanego sprzętu.

………………………, dn. ……………………. ……………………………………………………

podpis(y) osoby(osób) uprawnionej(nych)

do reprezentacji wykonawcy