**Część 1:**

**1 szt Serwer NAS przeznaczony do archiwizacji danych**

Zamawiający wymaga dostarczenia **Serwera NAS przeznaczonego do archiwizacji danych (1 szt.)** spełniającego następujące parametry minimalne:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L.p. | Nazwa parametru | Wymagane minimalnie parametry techniczne | Producent/typ/model | Wartość |
| 1 | **Procesor** | Czterordzeniowy procesor o taktowaniu 2,0 GHz osiągający w teście PassMark w maju 2023 co najmniej 2600 punktów  |  |  |
|  |  |  |
| 2 | **Pamięć RAM** | min. 2 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 4 GB |  |  |  |
| 3 | **Przestrzeń dyskowa** | Wymaga się aby serwer NAS był wyposażony w 4 kieszenie na dyski twarde typu hot-swap  |  |  |  |
| 4 | **Dyski twarde** | Urządzenie musi być wyposażone w 4 dyski twarde SATA HDD 3.5” o pojemności min. 8 TB min 7100obr. 256Mb cache każdy. Średni czas do awarii (MTBF) musi wynosić min. 1 mln godzin. Dyski muszą być przystosowane do działania w trybie ciągłym 24/7 w macierzach dyskowych NAS. Urządzenie musi być wyposażone w dysk M.2 NVMe o pojemności min. 0.75 TB |  |  |  |
|  |  |  |
| 5 | **Porty zewnętrzne** | Minimum: |  |  |  |
| • 2 porty USB 3.2 |  |  |  |
| 6 | **Porty sieciowe** | • 2 porty 1GbE RJ45 |  |  |  |
| 7 | **Funkcja Wake on LAN/WAN** | Wymagane |  |  |  |
| 8 | **Obsługiwane protokoły sieciowe** | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |  |  |  |
| 9 | **Obsługiwane systemy plików** | Min.: |  |  |  |
| • Wewnętrzny: Btrfs, ext4 |  |  |  |
| • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT |  |  |  |
| 10 | **Gwarancja** | 2 lata na urządzenia główne |  |  |  |

**Część 2:**

**Przełączniki dostępowe - switch 52 portowy - 2szt.**

Zamawiający wymaga dostarczenia przełączników dostępowych **(2 szt.)** spełniających następujące parametry minimalne:

Wymaga się aby urządzenie jak i zainstalowane zasilacze oraz wentylatory były objęte wieczysta gwarancją producenta realizowaną w systemie door-to-door  przez serwis producenta.

Urządzenie powinno być objęte 90 dniową pomocą techniczną telefoniczną świadczoną przez producenta urządzenia. Dodatkowo producent winien zapewnić pomoc w formie czat pracujący minimum 8 godzin dziennie w dni robocze w języku polskim przez cały okres gwarancji.

Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii  wysłanie sprawnego urządzenia nie później niż na następny dzień roboczy przez cały okres gwarancji.

W celu realizacji warunków gwarancji oraz zachowania pełnej kompatybilności wszystkie urządzenia sieciowe aktywne w tym moduły SFP oraz SFP+ będące przedmiotem postępowania winny pochodzić od jednego producenta.

Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa parametru** | **Wymagane minimalnie parametry techniczne** | **Producent/typ/model** | **Cena jednostkowa** | **Wartość** |
| **1** | **Całkowita liczba portów:** | 52 |  |  |  |
| **2** | **Złącza:** | RJ-45 10/100/1000 Mbps x 48 szt. RJ-45 100/1000/10000 Mbps x 2 szt.SFP+ x 2 szt. |  |
| **3** | **Architektura sieci:** | 10 Gigabit Ethernet |  |
| **4** | **Funkcja PoE:** | wymagane |  |
| **5** | **Zarządzanie:** | DHCP, IGMP v1/v2/v3, SNMP, Syslog, Telnet |  |
| **6** | **Przepustowość [Gb/s]:** | min. 80 |  |
| **7** | **Obsługiwane standardy:** | IPv4, IPv6, PoE+ |  |
| **8** | **Bufor pamięci:** | 16 Mb |  |
| **9** | **Zasilanie:** | PoE, Sieciowe |  |
| **10** | **Wyposażenie:** | Kabel mini USB, Przewód RJ-45, Przewód zasilający |  |
| **11** | **Gwarancja:** | Dożywotnia |  |
| **12** | **Zarządzanie:** | DHCP, IGMP v1/v2/v3, SNMP, Syslog, Telnet |  |
| **13** | **QoS:** | wymagane |  |
| **14** | **Inne:** | Filtrowanie Adresów MAC, Funkcja DHCP, Funkcja VLAN, System zapobiegania atakom DoS |  |
| **15** | **Obsługiwane standardy:** | IPv4, IPv6, PoE+ (min. 400W) |  |
| **16** | **Warstwa przełączania:** | 3 |  |
| **17** | **Algorytm przełączania:** | Store and forward |  |
| **18** | **Szybkość przekierowań pakietów:** | 120 Mp/s |  |
| **19** | **Możliwość montażu w szafach RACK:** | Wymagane |  |
| **20** | **Rozmiar tablicy MAC:** | 16 k |  |

**2 szt Moduł SFP+ 1x 10 Gbps LC MM, 300 m, TX:850nm, DDMI zgodny z zaproponowanym Switch z pozycji powyżej**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | Nazwa Parametru | Wymagane minimalne parametry techniczne | Producent/typ/model | Cena jednostkowa | Wartość |
| **1** |  **Port** | 1x 10 Gbps LC MM |  |  |  |
| **2** | **Długość fali TX** | 850 nm |  |  |  |
| **3** | **Długość fali RX** | 850 nm |  |  |  |
| **4** | **Zasięg portu** | 300 m |  |  |  |
| **5** | **Okablowanie portu** | 50/125, 62,5/125 |  |  |  |
| **6** | **DMI** | wymagane |  |  |  |
| **7** | **Typ modułu** | SFP+ |  |  |  |
| **8** | **Okres gwarancji** | minimum 1 rok |  |  |  |

**Przewody Światłowodowe SC**

Wymaga się dostarczenia 4 szt. światłowodów o długości min. 1m kompatybilnych z modułem SFP+ wymienionym powyżej z możliwością podłączenia do patchpanela światłowodowego z gniazdami SC.

**Część 3:**

**1szt Router UTM z funkcją firewall z licencją na 3 lata**

Zamawiający wymaga dostarczenia **Routera UTM (1 szt.)** spełniającego następujące parametry minimalne:

# **Wymagania Ogólne**

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły 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 – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

# **Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
* 6 portami Gigabit Ethernet RJ-45.
1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

# **Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 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 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 750 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 650 Mbps.

# **Funkcje Systemu Bezpieczeństwa:**

W ramach systemu ochrony są 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.
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. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są 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. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

# **Polityki, Firewall**

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje 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 istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
* Amazon Web Services (AWS).
* Microsoft Azure.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

# **Połączenia VPN**

1. Rozwiązanie umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* 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.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.
1. Rozwiązanie umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie rozwiązanie zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

# **Routing i obsługa łączy WAN**

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

# **Funkcje SD-WAN**

1. Rozwiązanie umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

# **Zarządzanie pasmem**

1. Rozwiązanie Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Rozwiązanie daje możliwość określania pasma dla poszczególnych aplikacji.
3. Rozwiązanie pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. Rozwiązanie zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

# **Ochrona przed malware**

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. Rozwiązanie umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. Rozwiązanie umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. Rozwiązanie dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. Rozwiązanie współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. Rozwiązanie zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

# **Ochrona przed atakami**

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Rozwiązanie chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. Rozwiązanie zapewnia 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).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

# **Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

# **Kontrola WWW**

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

# **Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall umożliwia 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. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

# **Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

# **Logowanie**

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

# **Certyfikaty**

Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.

# **Testy wydajnościowe oraz funkcjonalne**

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

# **Serwisy i licencje**

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

b)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

# **Gwarancja oraz wsparcie**

1. Gwarancja: Rozwiązanie jest objęte serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# **Opisy do wymagań ogólnych**

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lp. | Nazwa Parametru | Wymagane minimalne parametry techniczne | Producent/typ/model |  | Wartość |
| **1** | **Rodzaj urządzenia** | Firewall |  |  |
| **2** | **Porty** | 2 x WAN 10/100/1000/1 DMZ 5 x LAN 10/100/1000 |
| **3** | **Przepustowość IPS** | 1.4 Gb/s |
| **4** | **Przepustowość NGFW** | 1 Gb/s |
| **5** | **Przepustowość Threat Protection** | 700 Mb/s |
| **6** | **Przepustowość Firewalla (1518/ 512/ 64 bajty pakiety UDP)** | 10/ 10/ 6 Gb/s |
| **7** | **Opóźnienie zapory (64 bajtowe pakiety)** | 3.3 μs |
| **8** | **Przepustowość zapory (liczba pakietów na sekundę)** | 9 Mpps |
| **9** | **Sesje równoległe (TCP)** | 700 000 |
| **10** | **Nowe sesje na sekundę (TCP)** | 35 000 |
| **11** | **Firewall Policies** | 5 000 |
| **12** | **Przepustowość IPsec VPN (512 bajtów)** | 6.1 Gb/s |
| **13** | **Tunele IPsec typu Brama-Brama** | 200 |  |  |
| **14** | **Tunele IPsec typu Klient-Brama** | 500 |
| **15** | **Przepustowość SSL-VPN** | 405 Mb/s |
| **16** | **Liczba użytkowników SSL-VPN (zalecana)** | 200 |
| **17** | **SSL Inspection Throughput (IPS, avg. HTTPS)** | 700 Mb/s |
| **18** | **SSL Inspection CPS (IPS, avg. HTTPS)** | 400 |
| **19** | **Ilość Sesji SSL Inspectio (IPS, avg. HTTPS)** | 55 000 |
| **20** | **Przepustowość kontroli aplikacji (HTTP 64K)** | 1.8 Gb/s |
| **21** | **Przepustowość CAPWAP (HTTP 64 KB)** | 8 Gb/s |
| **22** | **Konfiguracje wysokiej dostępności** | Active/Active, Active/Passive, Clustering |
|  | **Funkcjonalności** | Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.  |
| **23** | **Licencja i wsparcie techniczne**  | **Wymaga się dostarczenia licencji na oprogramowanie na minimum 3 lata i wsparciem 24/7** |
| **24** | **Gwarancja** | Producenta |

**Część 4:**

**Kontroler WiFi zgodny z rozwiązaniami Unifi Ubiquiti 2szt**

Zamawiający wymaga dostarczenia **Kontrolera WiFi (2 szt.)** spełniającego następujące parametry minimalne:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lp. | Nazwa parametru | Wymagane minimalnie parametry techniczne | Producent/typ/model | Cena jednostkowa | Wartość |
| **1** | **Złącza:** | Gigabit Ethernet, Podświetlenie LED, Wbudowany port USB |  |  |  |
| **2** | **Przeznaczenie:** | Do elementów sieciowych |
| **3** | **Gwarancja** | minimum 12 miesięcy |
| **4** | **Rodzaj** | Kontroler WiFi |
| **5** | **Kompatybilność** | Urządzenie musi być zgodne z rozwiązaniami firmy Ubiquiti Networks ze względu na rozbudowę posiadanej infrastruktury |

 **Access-point zgodny z rozwiązaniami Unifi Ubiquiti – 10 szt.**

Zamawiający wymaga dostarczenia **urządzeń Access-point (10 szt.)** spełniającego następujące parametry minimalne:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lp. | Nazwa parametru | Wymagane minimalnie parametry techniczne | Producent/typ/model | Cena jednostkowa | wartość |
| **1** | **Producent** | Urządzenie musi być zgodne z rozwiązaniami firmy Ubiquiti Networks ze względu na rozbudowę posiadanej infrastruktury |  |  |  |
| **2** | **WIFI 2,4 GHz** | Wymagane  |
| **3** | **WIFI 5 GHz** | Wymagane |
| **4** | **Obsluga VLAN** | wymagane |
| **5** | **Maksymalna szybkość przesyłania danych (5 GHz)** | 867 Mbit/s   |
| **6** | **Prędkość transferu danych przez Ethernet LAN** | 10,100,1000 Mbit/s   |
| **7** | **Maksymalny zakres wewnętrzny (pomieszczenie)** | min 175 m   |
| **8** | **Szyfrowanie / bezpieczeństwo** | AES,TKIP,WEP,WPA,WPA-PSK,WPA2   |
| **9** | **Ilość portów Ethernet LAN (RJ-45)** | 1   |
| **10** | **Zasilanie** | POE |
| **11** | **Zestaw do montażu ściennego/sufitowego** | wymagane  |

**Część 5:**

**Zasilacz awaryjny UPS 10000VA – 1szt.**

Zamawiający wymaga dostarczenia **Zasilacza awaryjnego UPS (1 szt.)** spełniającego następujące parametry minimalne opisane poniżej.

Zamawiający wymaga od dostawcy dostarczenia, podłączenia w wyznaczonym przez Zamawiającego miejscu, skonfigurowania i uruchomienia urządzenia oraz przeprowadzenia szkolenia dla wskazanych pracowników Zamawiającego.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp. | Nazwa parametru | Wymagane minimalne parametry techniczne | Producent/typ/model | Wartość |
| **1** | Moc pozorna [VA] | 10000VA (10kVA) |  |  |
| **2** | Moc czynna [W] | 9000W  |
| **3** | Typ UPS | Online 3/3 |
| **4** | Napięcie  | Sinusoidalne |
| **5** | Złącze bateryjne | TAK |
| **6** | Akumulatory na wyposażeniu | Tak |
| **7** | Moduł zarządzania SNMP | Wymagany  |
| **8** | Typ baterii | 12V / 9Ah |
| **9** | Złącze TERMINAL | TAK |
| **10** | Złącza komunikacyjne | RS232,USB, RJ45 (Ethernet) |
| **11** | Kompatybilność z zasilaczami z aktywnym PFC | Wymagana |
| **12** | Ochrona przed przeciążeniem | Wymagana(minimum bezpiecznik i wewnętrzny ogranicznik prądu) |
| **13** | Filtr EMI/RFI | Wymagany |
| **14** | Układ przeciwprzepięciowy (Dżule) | Wymagany, minimum 440 |
| **15** | Funkcja EPO (Awaryjne wyłączenie) | Tak |
| **16** | Dołączone oprogramowanie do zarządzania | Wymagane, obsługa platform Windows, Linux, Vmware |
| **17** | Zarządzanie przez sieć | Wymagane dostarczenie karty zarządzającej HTTPS/SNMP, umożliwiającej m.in. kontrolę i monitoring stanu i kondycji zasilacza UPS, parametrów zasilania na wejściu i wyjściu, powiadamianie o zdarzeniach związanych z zasilaniem, możliwość zaplanowania automatycznego włączenia, wyłączenia lub restartu zasilacza UPS, log zdarzeń.  |
| **18** | Slot inteligentny | TAK |
| **19** | Gwarancja  | Producenta minimum 2 lata |
| **20** | Konstrukcja / montaż  | Dopuszcza się wersje montażu rack, tower i wolnostojące. W przypadku wersji rack wymaga się dostarczenia niezbędnych elementów do montażu urządzenia  |

**Zasilacz awaryjny 2000VA – 1 szt.**

Zamawiający wymaga dostarczenia **Zasilacza awaryjnego UPS (1 szt.)** spełniającego następujące parametry minimalne:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp. | Nazwa parametru | Wymagane minimalnie parametry techniczne | Producent/typ/model | wartość |
| 1 | Moc pozorna [VA]: | min.2000 |  |  |
| 2 | Moc skuteczna [W]: | min.1400 |
| 3 | Sygnalizacja pracy: | Wyświetlacz LCD |
| 4 | Topologia: | Line-interactive |
| 5 | Zabezpieczenia: | Przeciwprzepięciowe, Przeciwzwarciowe, Termiczne |
| 6 | Czas podtrzymania (średni) [min]: | 5,00 |
| 7 | Czas podtrzymania przy 100% obciążeniu [min]: | 1,00 |
| 8 | Czas podtrzymania przy 50% obciążeniu [min]: | 10,00 |
| 9 | Czas przełączania [ms]: | max 6 |
| 10 | Liczba gniazd wyjściowych: | 5,00 |
| 11 | Napięcie wejściowe [V]: | 220/230/240 |
| 12 | Napięcie wyjściowe [V]: | 230,00 |
| 13 | Wyposażenie: | Kabel zasilający |
| 14 | Funkcje  | Wymagana funkcja AVR |
| 15 | Gwarancja |  Producenta, minimum 2 lata |

**Część 6:**

**Komputer all in one - 12szt.**

Zamawiający wymaga dostarczenia **komputerów typu All-in-One (12 szt.)** spełniających następujące parametry minimalne:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lp. | Nazwa parametru | Wymagane minimalnie parametry techniczne | Producent/typ/model | Cena jednostkowa | Wartość |
| **1** | **Dane techniczne** |  |  |  |
|  | **Gwarancja**  | Min. 2 lata  |
|  | **Rodzaj** | All in One |
| **2** | **Wyświetlacz** |
|  | **Przekątna ekranu** | 23 cali |
|  | **Rozdzielczość** | 1920 x 1080 |
|  | **Powłoka ekranu** | antyrefleksyjna |
| **3** | **Procesor** |
|  | **Wynik w teście CPU BenchMark (w pkt)** | minimum 20000 |
| **4** | **Karta graficzna** |
|  | **Złącza karty graficznej** | 1 x HDMI out |
| **5** | **Pamięć** |
|  | **Ilość pamięci RAM** | 16 GB |
|  | **Rodzaj pamięci RAM** | SO-DIMM DDR4  |
| **6** | **Dysk twardy** |
|  | **Typ dysku 1** | SSD |
|  | **Pojemność dysku** | 512 GB |
|  | **Interfejs dysku 1** | M.2 (PCIe) NVMe |
| **7** | **Oprogramowanie** |
|  | **System operacyjny** | Windows 11 Pro |
| **8** | **Płyta główna** |
|  | **Złącza**  | 1 x HDMI in, 1 x RJ45, 2 x USB, 2 x USB 3.2, 1 x USB 3.2 Gen 2 (Typ-C), audio |
| **9** | **Obudowa** |
|  | **Waga całkowita** | maksymalnie 8 kg |
| **10** | **Pozostałe cechy** |
|  | **Karta sieciowa** | 10/100/1000 |
|  | **Standard łączności bezprzewodowej** | Bluetooth |
|  | Wi-Fi 6 (802.11 a/b/g/n/ac/ax) |
|  | **Akcesoria w komplecie** | klawiatura, mysz |
|  | **Szyfrowanie** | szyfrowanie TPM 2.0 |
|  | **Dodatkowe informacje** | Wymagana wbudowana/dołączona do zestawu kamera internetowa |

**Monitor 27”**

Zamawiający wymaga dostarczenia **monitora 27” (1 szt.)** spełniających następujące parametry minimalne:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lp. | Nazwa parametru | Wymagane minimalne parametry techniczne | Producent/typ/model | Cena jednostkowa | wartość |
| **1** | Przekątna ekranu:  | 27" |  |  |  |
| **2** | Powłoka matrycy:  | Matowa |
| **3** | Rodzaj matrycy:  | LED |
| **4** | Typ ekranu:  | Płaski |
| **5** | Rozdzielczość ekranu:  | 1920 x 1080 (FullHD) |
| **6** | Format obrazu:  | 16:09 |
| **7** | Częstotliwość odświeżania ekranu: min.  | 75 Hz |
| **8** | Czas reakcji:  | 1ms |
| **9** | Liczba wyświetlanych kolorów:  | 16,7 mln |
| **10** | Technologia ochrony oczu:  | Redukcja migotania (Flicker free), Filtr światła niebieskiego |
| **11** | Kąt widzenia w pionie:  | 178 stopni |
| **12** | Złącza:  | VGA (D-sub) - 1 szt., HDMI - 1 szt. |
| **13** | Wyjście audio / Wejście audio lub COMBO | wymagane  |
| **14** | AC-in (wejście zasilania) | 1 szt. |
| **15** | Głośniki:  | Tak, min.,2 x 2W |
| **16** | Obrotowy ekran (PIVOT):  | Tak |
| **17** | Regulacja wysokości (Height):  | Tak |
| **18** | Regulacja kąta pochylenia (Tilt):  | Tak |
| **19** | Regulacja kąta obrotu (Swivel):  | Tak |
| **20** | Możliwość montażu VESA:  | TAK |
| **21** | Kolor:  | czarny |
| **22** | Dołączone akcesoria:  | Kabel zasilający, Kabel HDMI |