**Załącznik nr 1.2**

OPIS PRZEDMIOTU ZAMÓWIENIA

**Część 2**

1. **Access Point – 3 sztuki.**

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
   1. Temperatura 0–50°C,
   2. Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać co najmniej następujące standardy:
   1. 2.4 GHz 802.11b/g/n/ax,
   2. 5 GHz 802.11a/n/ac/ax,
   3. 6 GHz 802.11ax/be
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.
5. Urządzenie musi być wyposażone w moduł BLE.
6. Urządzenie musi być wyposażone w co najmniej jeden interfejs Ethernet (RJ45) wspierający co najmniej szybkości 1G/2.5G/5.0G.
7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz. Maksymalne zużycie energii nie może przekraczać 17W przy wykorzystaniu wszystkich funkcji urządzenia.
8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
   1. Tunnel,
   2. Bridge,
   3. Mesh.
9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).
11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    1. MIMO – 2x2,
    2. Wymagana przepustowość dla poszczególnych modułów radiowych:
       1. min. 688 Mbps;
       2. min. 2882 Mbps;
       3. min. 5765 Mbps;
    3. Wymagana moc nadawania:
       1. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
       2. min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
       3. min. 22 dBm dla pasma 6GHz z możliwością zmiany co 1dBm
    4. Wsparcie dla kanałów 20/40/80/160/320MHz,
    5. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5dBi dla pasma 6GHz.
    6. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy.
    7. Każdy z modułów radiowych musi posiadać możliwość pracy jako dedykowany skaner.
12. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512
13. Funkcje dodatkowe:
    1. OFDMA UL i DL
    2. Spatial Reuse (BSS Coloring)
    3. UL-MU-MIMO
    4. DL-MU-MIMO
    5. Enhanced Target Wake Time (TWT)
    6. Wbudowany analizator widma
    7. Wbudowane mechanizmy WIPS/WIDS

Gwarancja oraz wsparcie:

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 36 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 24x7.

1. **Przełącznik sieciowy – 4 sztuki.**

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach:

Parametry fizyczne platformy:

* Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
* Zasilanie AC 230V.
* Wymagany - z możliwością wymiany w czasie pracy - redundantny zasilacz.
* Maksymalny pobór mocy: 185 W.
* Minimalny zakres temperatury pracy: 0-40ᵒC.

Interfejsy sieciowe – wymagania minimalne:

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 48 porty 10 GE SFP+.

b) 6 porty 40 GE QSFP+ lub 4 porty 100 GE QSFP28.

Zarządzanie:

* Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania.
* Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
* Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
* Wsparcie dla SNMP w wersjach 1-3
* Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
* Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
* Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
* Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
* Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
* Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
* Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe:

* Przepustowość urządzenia - min. 1750 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 1515 Mpps.
* Tablica adresów MAC o pojemności co najmniej 144 k wpisów.
* Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje:

* Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
* Obsługa Jumbo Frames.
* Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
* Agregacja portów zgodna ze standardem 802.3ad.
* Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
* Obsługa routingu statycznego.
* Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP.
* Port-mirroring.
* Uwierzytelnianie 802.1x na poziomie portu.
* Uwierzytelnianie 802.1x w oparciu o adres MAC.
* W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN).
* W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
* W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
* Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC:

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

* Centralne zarządzanie konfiguracją urządzenia.
* Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania.
* Centralne zarządzanie sieciami VLAN.
* Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u.
* Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
* Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
* Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
* Automatyczna detekcja i rekomendacje konfiguracji.
* Przesyłanie logów na zewnętrzny serwer syslog.
* Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
* Obsługa białych i czarnych list adresów MAC.
* Wykrywanie aplikacji komunikujących się w sieci.

1. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
2. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa:

* System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
* System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie:

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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 24x7.

Opisy do wymagań ogólnych:

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. **Przełączniki sieciowe – 5 sztuk.**

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach:

Parametry fizyczne platformy:

* Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
* Zasilanie AC 230V.
* Maksymalny pobór mocy: 10 W.
* Minimalny zakres temperatury pracy: 0-40ᵒC.

Interfejsy sieciowe – minimalne wymagania:

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 8 porty GE RJ-45.

b) 2 porty GE, SFP.

Zarządzanie:

* Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
* Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
* Wsparcie dla SNMP w wersjach 1-3
* Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
* Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
* Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
* Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
* Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
* Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
* Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe:

* Przepustowość urządzenia - min. 20 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 30 Mpps.
* Tablica adresów MAC o pojemności co najmniej 8 k wpisów.
* Opóźnienie wprowadzane przez przełącznik - poniżej 5 mikrosekund.

Wymagane funkcje:

* Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
* Obsługa Jumbo Frames.
* Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
* Agregacja portów zgodna ze standardem 802.3ad.
* Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
* Obsługa routingu statycznego.
* Port-mirroring.
* Uwierzytelnianie 802.1x na poziomie portu.
* Uwierzytelnianie 802.1x w oparciu o adres MAC.
* W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
* W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
* W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC:

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

* Centralne zarządzanie konfiguracją urządzenia
* Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
* Centralne zarządzanie sieciami VLAN.
* Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
* Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
* Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
* Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
* Automatyczna detekcja i rekomendacje konfiguracji.
* Przesyłanie logów na zewnętrzny serwer syslog.
* Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
* Obsługa białych i czarnych list adresów MAC.
* Wykrywanie aplikacji komunikujących się w sieci.

1. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
2. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa:

* System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
* System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie:

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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 24x7.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. **Przełączniki sieciowe – 1 sztuka.**

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach:

Parametry fizyczne platformy:

* Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
* Zasilanie AC 230V.
* Budżet mocy dla portów PoE min.: 370 W.
* Maksymalny pobór mocy bez budżetu dla PoE: 85 W.
* Minimalny zakres temperatury pracy: 0-40ᵒC.

Interfejsy sieciowe – wymagania minimalne:

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 24 porty GE RJ-45.

* W tym porty PoE w ilości co najmniej: 24, zgodne ze standardem: 802.3af oraz 802.3at.

b) 4 porty 10 GE SFP+.

Zarządzanie:

* Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
* Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
* Wsparcie dla SNMP w wersjach 1-3
* Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
* Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
* Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
* Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
* Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
* Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
* Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe:

* Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps.
* Tablica adresów MAC o pojemności co najmniej 32k wpisów.
* Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje:

* Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
* Obsługa Jumbo Frames.
* Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
* Agregacja portów zgodna ze standardem 802.3ad.
* Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
* Obsługa routingu statycznego.
* Port-mirroring.
* Uwierzytelnianie 802.1x na poziomie portu.
* Uwierzytelnianie 802.1x w oparciu o adres MAC.
* W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
* W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
* W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
* Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC:

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

* Centralne zarządzanie konfiguracją urządzenia
* Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
* Centralne zarządzanie sieciami VLAN.
* Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
* Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
* Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
* Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
* Automatyczna detekcja i rekomendacje konfiguracji.
* Przesyłanie logów na zewnętrzny serwer syslog.
* Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
* Obsługa białych i czarnych list adresów MAC.
* Wykrywanie aplikacji komunikujących się w sieci.

1. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
2. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa:

* System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
* System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie:

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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 24x7.

Opisy do wymagań ogólnych:

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. **Przełączniki sieciowe – 12 sztuk.**

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach:

Parametry fizyczne platformy:

* Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
* Zasilanie AC 230V.
* Budżet mocy dla portów PoE min.: 185 W.
* Maksymalny pobór mocy bez budżetu dla PoE: 55 W.
* Minimalny zakres temperatury pracy: 0-40ᵒC.

Interfejsy sieciowe – wymagania minimalne:

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 24 porty GE RJ-45.

* W tym porty PoE w ilości co najmniej: 12, zgodne ze standardem: 802.3af oraz 802.3at.

b) 4 porty 10 GE SFP+.

Zarządzanie:

* Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
* Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
* Wsparcie dla SNMP w wersjach 1-3
* Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
* Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
* Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
* Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
* Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
* Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
* Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe:

* Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps.
* Tablica adresów MAC o pojemności co najmniej 32k wpisów.
* Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje:

* Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
* Obsługa Jumbo Frames.
* Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
* Agregacja portów zgodna ze standardem 802.3ad.
* Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
* Obsługa routingu statycznego.
* Port-mirroring.
* Uwierzytelnianie 802.1x na poziomie portu.
* Uwierzytelnianie 802.1x w oparciu o adres MAC.
* W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
* W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
* W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
* Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC:

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

* Centralne zarządzanie konfiguracją urządzenia
* Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
* Centralne zarządzanie sieciami VLAN.
* Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
* Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
* Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
* Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
* Automatyczna detekcja i rekomendacje konfiguracji.
* Przesyłanie logów na zewnętrzny serwer syslog.
* Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
* Obsługa białych i czarnych list adresów MAC.
* Wykrywanie aplikacji komunikujących się w sieci.

1. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
2. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa:

* System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
* System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie:

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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 24x7.

Opisy do wymagań ogólnych:

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. **Przełącznik sieciowy – 11 sztuk.**

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach:

Parametry fizyczne platformy:

* Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
* Zasilanie AC 230V.
* Budżet mocy dla portów PoE min.: 370 W.
* Maksymalny pobór mocy bez budżetu dla PoE: 110 W.
* Minimalny zakres temperatury pracy: 0-40ᵒC.

Interfejsy sieciowe – minimalne wymagania:

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 48 porty GE RJ-45.

* W tym porty PoE w ilości co najmniej: 24, zgodne ze standardem: 802.3af oraz 802.3at.

b) 4 porty 10 GE SFP+.

Zarządzanie:

* Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
* Wsparcie dla SNMP w wersjach 1-3
* Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
* Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
* Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
* Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
* Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
* Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
* Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe:

* Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.
* Tablica adresów MAC o pojemności co najmniej 32k wpisów.
* Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje:

* Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
* Obsługa Jumbo Frames.
* Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
* Agregacja portów zgodna ze standardem 802.3ad.
* Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
* Obsługa routingu statycznego.
* Port-mirroring.
* Uwierzytelnianie 802.1x na poziomie portu.
* Uwierzytelnianie 802.1x w oparciu o adres MAC.
* W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
* W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
* W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
* Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC:

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

* Centralne zarządzanie konfiguracją urządzenia
* Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
* Centralne zarządzanie sieciami VLAN.
* Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
* Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
* Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
* Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
* Automatyczna detekcja i rekomendacje konfiguracji.
* Przesyłanie logów na zewnętrzny serwer syslog.
* Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
* Obsługa białych i czarnych list adresów MAC.
* Wykrywanie aplikacji komunikujących się w sieci.

1. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
2. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa:

* System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
* System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie:

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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 24x7.

Opisy do wymagań ogólnych:

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. **UTM – 2 sztuki.**

**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 5 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:**

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

1. **System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację 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 2xAC.**

**Parametry wydajnościowe:**

1. **W zakresie Firewall’a obsługa nie mniej niż 10 mln jednoczesnych połączeń oraz 380 tys. nowych połączeń na sekundę.**
2. **Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B.**
3. **Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 26 Gbps.**
4. **Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 35 Gbps.**
5. **Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 9 Gbps.**
6. **Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 6 Gbps.**
7. **Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 6 Gbps.**

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.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
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. Możliwość filtrowania zapytań DNS 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: adresy 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. System 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. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec 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).
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. System 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. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System 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. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System 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. System 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 usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. System 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. System 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. System 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 wieloskładnikowego.
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 wieloskładnikowego 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.

Testy wydajnościowe oraz funkcjonalne

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.

Serwisy i licencje

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

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

System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

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.
3. **Centralny system logowania.**

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 działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Interfejsy, Dysk:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 20 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 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:

a. Listę najczęściej wykrywanych ataków.

b. Listę najbardziej aktywnych użytkowników.

c. Listę najczęściej wykorzystywanych aplikacji.

d. Listę najczęściej odwiedzanych stron www.

e. Listę krajów , do których nawiązywane są połączenia.

f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
2. 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.
3. 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: 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.

1. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.

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.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

1. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje

1. Wsparcie: System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. **System centralnego zarządzania urządzeniami bezpieczeństwa oraz logowania.**

W ramach postępowania wymaganym jest dostarczenie systemu centralnego zarządzania oraz logowania i raportowania, przystosowanego do współpracy z systemem bezpieczeństwa sieciowego (np. NGFW).

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy lub komercyjnych platform działających w środowisku wirtualnym lub w postaci komercyjnej platformy/komercyjnych platform działających na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX, ESXi wersje: 5.5,6.0,6.5,6.7; Microsoft Hyper-V 2012, 2016; Citrix XenServer 6.0+; Open Source Xen 4.1+; KVM Redhat 6.5+, Amazon Web Services (AWS), Microsoft Azure, Google Cloud.

Interfejsy, Dyski:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 200 GB.

Parametry wydajnościowe:

1. System musi umożliwiać zarządzenie co najmniej 10 systemami bezpieczeństwa.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 10 systemów.
3. System musi być w stanie przyjmować minimum 2 GB logów na dzień.

Funkcje systemu centralnego zarządzania

W ramach centralnego systemu zarządzenia muszą być realizowane co najmniej poniższe funkcje:

1. System musi posiadać system zarządzenia zmianami konfiguracji (WorkFlow, mechanizm audytu oraz porównania konfiguracji).
2. System musi dawać możliwość pełnej konfiguracji urządzeń, ze wszystkimi ich funkcjami składowymi.
3. System musi posiadać możliwość skonfigurowania godziny implementacji zmian (harmonogram dla instalowania zmian).
4. System musi przechowywać i implementować polityki bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej.
5. System musi wersjonować polityki w taki sposób, aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości.
6. System musi umożliwiać zarządzenie wersjami firmware’u oraz zapewniać centralną aktualizację oprogramowania.
7. System musi być w stanie wysłać tą samą konfigurację na wiele urządzeń.
8. System musi umożliwiać pracę wielu administratorów jednocześnie (system musi mieć możliwość blokady kontekstu urządzenia).
9. System musi być w stanie zarządzać wersjami baz sygnatur na urządzeniach oraz zdalnymi uaktualnieniami.
10. System musi zapisywać i zdalne wykonywanie skryptów na urządzeniach.
11. System musi monitorować w czasie rzeczywistym stan urządzeń (użycie CPU, RAM).
12. System musi automatyzować proces konfiguracji struktur VPN typu hub-and-spoke oraz full-mash.
13. Konfigurację powiadomień poprzez: e-mail, SNMP v1/v2c/v3 w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.

Funkcje logowania

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:

a. Listę najczęściej wykrywanych ataków.

b. Listę najbardziej aktywnych użytkowników.

c. Listę najczęściej wykorzystywanych aplikacji.

d. Listę najczęściej odwiedzanych stron www.

e. Listę krajów , do których nawiązywane są połączenia.

f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

Funkcja raportowania

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. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Funkcje korelacji

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.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, TACACS+, PKI.

1. System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i elementów zarządzania z perspektywy poszczególnych zarządzanych systemów.
2. System musi posiadać API które umożliwia zarządzenie urządzeniami podłączonymi do systemu za pomocą poleceń REST API.
3. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

Gwarancja oraz wsparcie

1. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
2. Wsparcie: System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. **System ochrony aplikacji webowych oraz API.**

System ochrony aplikacji webowych oraz API, którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. Powinien zostać dostarczony w postaci komercyjnej platformy programowej. Powinien zostać dostarczony w postaci komercyjnej platformy instalowanej w środowisku wirtualnym: VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Amazon Web Services (AWS) and Microsoft Azure, Google Cloud, Oracle Cloud. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych. W przypadku implementacji programowej dostawca musi zapewnić niezbędny odpowiednio zabezpieczony systemem operacyjny.

Architektura systemu

1. Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest, aby elementy systemu pracowały w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa.
2. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe oraz zastosowane w nich technologie pochodziły od jednego producenta. Nie dopuszcza się, aby elementy funkcji podstawowych zastosowanych w systemie były opracowane przez firmy trzecie.
3. Musi istnieć możliwość implementacji systemu w trybach: inline reverse proxy lub transparent.
4. Produkt nie może posiadać ograniczeń co do ilości chronionych aplikacji web.
5. Powinna istnieć możliwość zdefiniowania co najmniej 4 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu.
6. System powinien mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive i Active-Active.

Parametry fizyczne systemu

1. System realizujący funkcje podstawowe musi obsługiwać minimum:

* 4 interfejsów sieciowych
* Ilość wirtualnych procesorów: 2

1. Obsługa powierzchni dyskowej - minimum 1 TB.

Parametry wydajnościowe

1. Przepustowość dla ruchu http - min 100 Mbps.
2. Przepustowość dla ruchu https - min 50 Mbps.

Podstawowe funkcje systemu

System musi realizować co najmniej poniższe funkcje:

1. Obsługa protokołów: - http 1.1, http 2.0, http 3.0, FTP.
2. System musi posiadać możliwość automatycznego uczenia się działania aplikacji w zakresie:

* obserwacji i budowania profilu dla URL, parametrów, metod http, sesji https. Obserwacje powinny uczyć model matematyczny normalnych zachowań, który następnie umożliwi wykrywanie anomalii
* Wyuczony model matematyczny wykrywa odstępstwa od normy w obserwowanych elementach
* System automatycznie wykrywa zmiany po stronie aplikacji lub zachowania użytkowników i ponawia proces uczenia.
* Możliwe jest zdefiniowanie wyjątków, które nie będą brały udziału w uczeniu modelu matematycznego
* Musi istnieć możliwość strojenia czułości modelu wykrywającego anomalie przez administratora systemu. Poziom czułości musi być ustawiany globalnie dla aplikacji jak i na poziomie pojedynczych parametrów.

1. System musi posiadać funkcje ochrony komunikacji API wspieraną technologią uczenia maszynowego. Zakres wsparcia nie może być mniejszy niż:

* Uczenie modelu matematycznego w oparciu o widziany faktyczny ruch REST API
* Budowanie automatyczne schematu struktury API w oparciu o obserwowany ruch
* Ruch niezgodny z wyuczonym profilem uznawany jest za atak

1. System ochrony aplikacji musi być wyposażony w mechanizm wykrywania komunikacji pochodzącej od internetowych bot’ów. Wykrywanie musi być oparte co najmniej o następujące mechanizmy:

* Uczenie maszynowe: powinno działać w trybie nauki modelu matematycznego standardowego zachowania użytkowników. Po zebraniu informacji system powinien przejść do trybu ochrony, gdzie wykrycie zachowania odbiegającego od normy powinno skutkować uznaniem źródła za automat.

1. Podział obciążenia na wiele serwerów (loadbalancing) z mechanizmami weryfikacji stanu pracy serwerów. Wsparcie dla mechanizmów podziału obciążenia:

* Round Robin,
* Weighted Round Robin,
* Least Connection,

1. Wsparcie dla mechanizmów podtrzymania sesji w oparciu o:

* Source IP
* HTTP Header
* URL parameter
* Insert Cookie
* Rewrite Cookie
* Persistent Cookie
* Embedded Cookie
* ASP Session ID
* PHP Session ID
* JSP Session ID
* SSL Session ID

1. Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla TLS 1.1, TLS 1.2. TLS 1.3.
2. Możliwość analizy ruchu do aplikacji po protokołach HTTP/HTTPS w oparciu o zaimplementowane polityki bezpieczeństwa.
3. Ochrona aplikacji www przed takimi zagrożeniami jak:

* SQL and OS Command Injection
* Cross Site Scripting (XSS)
* Cross Site Request Forgery
* Outbound Data Leakage
* HTTP Request Smuggling
* Buffer Overflow
* Encoding Attacks
* Cookie Tampering / Poisoning
* Session Hijacking
* Broken Access Control
* Forceful Browsing /Directory Traversal
* Ochrona przed innymi zagrożeniami specyfikowanymi przez listę OWASP
* DoS w warstwie aplikacji
* Ochrona przed atakami typu Brute force
* Ochrona przed atakami clickjacking

1. Mechanizmy ochrony przed wyciekiem informacji poufnych.
2. Filtrowanie ruchu do aplikacji w oparciu o geo-lokalizację.
3. Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania.
4. Integracja z zewnętrznymi systemami uwierzytelniania dwu-składnikowego.
5. Wsparcie dla ochrony HTTP/1.1 i HTTP/2 oraz SSL offload dla HTTP/1.1 i HTTP/2 w trybie pracy reverse proxy.
6. Wsparcie dla ochrony cookie, w tym szyfrowania oraz sprawdzania flag „Secure" oraz „http only”.
7. Content routing na bazie parametrów http oraz certyfikatów X.509.
8. Ochrona przed Web Scraping.
9. Wsparcie dla kompresji danych oraz cache.
10. Publikacja aplikacji web oraz OWA z zastosowaniem mechanizmu single sign on (http basic, kerberos).
11. Wsparcie dla aplikacji wykorzystujących AJAX oraz JSON, XML, AMF3.
12. Ochrona przed atakami typu SLOW (Slowloris i podobne).
13. Możliwość selektywnego wyłączania blokowania ataków dla sygnatur oraz obszarów aplikacji. Dodanie wyjątków dla sygnatur na podstawie co najmniej:

* Metoda HTTP
* IP klienta
* Host
* URI
* Cały URL
* Parametr
* Cookie
* http Header
* JSON Elements

1. Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For”.
2. Możliwość konfigurowania własnych stron z informacjami o błędzie per polityka.
3. Sprawdzanie pól w nagłówkach http oraz samym protokole. Sprawdzanie długości payload’u HTML.
4. Wsparcie dla walidacji OpenAPI, JSON i XML.
5. Blokowania „Illegal XML Format” oraz „Illegal JSON Format”.
6. Możliwość wysłania odszyfrowanego przez system ruchu do innego systemu celem dalszej analizy.
7. Przydzielanie różnych certyfikatów dla różnych nazw domenowych.
8. Możliwość tworzenia i wykorzystanie skryptów do obsługi ruchu.
9. Ochrona przed atakami MiTB (Man-in-the-Browser) z wykorzystaniem mechanizmów typu Anti-keylogger, Obfuscate.
10. Możliwość zapewnienia, że wewnętrzna struktura katalogów aplikacji internetowej nie zostanie ujawniona osobom niepożądanym.
11. Możliwość tworzenia wirtualnej kolejki (waiting room) przy przekroczeniu ilości liczby aktywnych połączeń.

Wymagane funkcje dodatkowe

1. Kontrola antywirusowa dla komunikacji http realizowana na firewall’u aplikacyjnym lub zewnętrznym systemie w oparciu o protokół icap. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
2. W ramach postępowania wymaganym jest dostarczenie licencji upoważniającej do współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
3. Skaner aplikacji WWW realizowany bezpośrednio na firewall’u aplikacyjnym lub zewnętrznym systemie (w przypadku zewnętrznego systemu skanującego – musi istnieć możliwość importu wyników skanowania do systemu WAF oraz na tej podstawie konfiguracji polityk ochrony). W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji dla co najmniej 50 aplikacji.
4. Ochrona przed podmianą strony WWW realizowana bezpośrednio na firewall’u aplikacyjnym lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji dla co najmniej 50 aplikacji.
5. Dekodowanie Base64 oraz CSS.
6. Domyślne szablony ochrony co najmniej dla MS Exchange, MS SharePoint i WordPress.
7. Uwierzytelnianie użytkowników w oparciu o protokół SAML.
8. Rozpoznawanie prawidłowo zalogowanych użytkowników do chronionej aplikacji.
9. Wsparcie dla CAPTCHA i Real Browser Enforcement do weryfikacji użytkowników.
10. Budowa rankingu punktowego lub określanie poziomu zagrożenia dla ruchu z możliwością określenia progów dla akcji: kwarantanna czasowa.
11. Możliwość uruchomienia ADFSProxy oraz stworzenia polityki w celu sprawdzania ruchu do serwerów ADFS, ich ochrony pod kątem botów oraz ataków DoS.
12. Możliwość znakowania przez administratorów systemu za pomocą znaczników (flag) lub komentarza zdarzeń zalogowanych przez urządzenie w celu późniejszej ich analizy.
13. Ochrona przed botami dla: strony internetowej, aplikacji mobilnej, interfejsu API - przy zastosowaniu funkcji biometrycznych.
14. Cross-Origin Resource Sharing (CORS) protection.
15. System musi pozwalać na weryfikacje nazwy użytkownika i hasła w ramach mechanizmów ochrony przed wykorzystywaniem skompromitowanych poświadczeń. W ramach postepowania muszą zostać dostarczone niezbędne do uruchomienia tej funkcji licencje.
16. Dostawca musi dostarczyć usługę monitorowania logów bezpieczeństwa pochodzących z oferowanego systemu w trybie 24/7, w wypadku wystąpienia incydentów bezpieczeństwa wynikających z analizy logów dostawca wykonuje oceny krytyczności zdarzenia i informuje zamawiającego o wystąpieniu zdarzenia adekwatnie do wagi wraz z rekomendacją dalszego postepowania
17. System musi pozwalać na identyfikacje i agregację alertów bezpieczeństwa z wykorzystaniem algorytmów uczenia maszynowego ze wszystkich chronionych aplikacji w zrozumiałe incydenty bezpieczeństwa poprzez dedykowany zewnętrzny portal.

Zarządzanie

1. Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, API.
2. Element systemu pełniący funkcję Web Application Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: packet capture.
3. Powinna istnieć możliwość zdefiniowania co najmniej 5 lokalnych kont administracyjnych.
4. Możliwość przechowywania lokalnie na urządzeniu do 10 plików konfiguracyjnych.

Logowanie i Raportowanie

1. System musi zapewniać lokalne logowanie oraz raportowanie - w oparciu o zestaw predefiniowanych wzorców raportów.
2. Możliwość logowania do zewnętrznego serwera syslog i SIEM.
3. Obsługa powiadomień o zdarzeniach systemowych, incydentach bezpieczeństwa mailem oraz z wykorzystaniem komunikatorów takich jak np. Teams.
4. Powiadomienia o zdarzeniach systemowych oraz incydentach bezpieczeństwa za pośrednictwem trapów SNMP.
5. Możliwość włączenia logowania per reguła w polityce.
6. Możliwość maskowania w logach pól wrażliwych.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub wykonane przez producenta testy nie starsze niż 6 miesięcy.

Sygnatury, subskrypcje

1. Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie aktualizowane zgodnie ze zdefiniowanych harmonogramem.
2. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:

* Kontrolę antywirusową, sygnatury ochrony dla aplikacji www, bazy reputacyjne adresów IP, usługa identyfikacji i korelacji alertów bezpieczeństwa przy użyciu sztucznej inteligencji, bazy skompromitowanych poświadczeń oraz dostęp do usługi sandbox na okres 36 miesięcy.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opis przedmiotu zamówienia (nie techniczny, tylko ogólny):

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Machine Learning - wykorzystująca mechanizmy sztucznej inteligencji w celu wychwytywania anomalii oraz zaawansowanych ataków. Funkcja powinna umożliwiać automatyczne dostrajanie mechanizmów ochrony (bez ingerencji administratora) w miarę zmieniającego się profilu zabezpieczanej aplikacji.

1. **Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów programowych.**
2. W ramach postępowania powinny zostać dostarczone co najmniej 50 tokeny programowe współpracujące z posiadanym przez Zamawiającego urządzeniem FortiGate, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów oraz w ramach połączeń VPN typu client-to-site.
3. Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile.
4. Dla tokenów na system iOS i Android wymaga się:
5. aktywacji z systemu firewall FortiGate
6. generowania kodu (cyfr) co 30 lub 60 sekund,
7. możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne),
8. ochrony dostępu poprzez konfigurowalny kod PIN,
9. **System klasy PAM.**

Wymagania funkcjonalne dla systemu

1. Zapewnienie wysokiego poziomu bezpieczeństwa danych i poufności informacji
2. Wsparcie dla szyfrowania danych w transmisji i przechowywaniu haseł i kluczy
3. Elastyczność w zakresie skalowania infrastruktury w celu obsługi zwiększonego obciążenia
4. System musi posiadać Mechanizmy failover i redundancji, aby zapewnić ciągłość działania w przypadku awarii serwera lub innego komponentu
5. System PAM musi posiadać przyjazny interfejs graficzny (GUI) umożliwiający łatwe zarządzanie kontami uprzywilejowanymi i monitorowanie działań użytkowników.
6. Integracja z technologią ZTNA (Zero Trust Network Access) oraz możliwość działania jako punkt wymuszania dla ZTNA
7. Musi istnieć możliwość sprawdzania silnikiem antywirusowym przesyłanych podczas sesji plików. Kontrola musi być realizowana co najmniej dla transferu plików poprzez web (Web SFTP, Web SAMBA) oraz SCP.
8. Automatyczne blokowanie niebezpiecznych poleceń za pomocą profilu filtrowania SSH. System musi monitorować komendy wydawane przez operatora sesji.
9. System PAM powinien być dostarczony jako urządzenie na utwardzonym przez jednego producenta systemie operacyjnym w formie gotowego i pełnego rozwiązania
10. Rozwiązanie musi być dostępne w formie zarówno urządzeń wirtualnych (*virtual appliance*), jak i sprzętowych. Dla wirtualizacji musi być wspierany co najmniej hypervisor VMWare oraz KVM.
11. Działanie PAM musi pozwalać na obsługę połączeń bezpośrednich jak i proxy.
12. Możliwość obsługi niestandardowych protokołów chociażby poprzez dedykowane wyzwalacze (*custom application launcher*)
13. Możliwość ostrzegania użytkowników o nagrywaniu w celu zapewnienia zgodności z wymaganiami RODO.
14. System PAM w wersji wirtualnej musi obsługiwać moduł vTPM (*Virtual Trusted Platform Module*) dla przechowywania kluczy prywatnych użytkowników.
15. PAM musi obsługiwać mechanizm awaryjnego dostępu do zaszyfrowanych haseł przechowywanych w systemie na zasadzie procedury „glass breaking”. Wszystkie działania w tym trybie muszą być logowane celem możliwości przeprowadzenia audytu.
16. System musi automatycznie nagrywać obraz podczas uruchomienia procedury awaryjnej (glass breaking)
17. Automatyczna zmiana hasła konta po poprawnym zalogowaniu
18. Wsparcie dla zaplanowanej zmiany haseł według harmonogramu
19. Możliwość tworzenia procedury żądania dostępu do haseł i zatwierdzania takich żądań poprzez konfigurowalną ilość administratorów
20. Ustawienie dedykowanego dostępu do skonfigurowanego hasła dla jednego administratora. W tym stanie dostęp jest ograniczony tylko dla jednego użytkownika uprzywilejowanego.
21. Wymagane jest wsparcie dla algorytmów szyfrowania SSH o wysokiej sile
22. Zaawansowany protokół uwierzytelniania RDP, w tym CredSSP i TLS
23. Kontrola dostępu oparta na rolach (RBAC)
24. Kontrola uprawnień oparta na użytkownikach oraz grupach użytkowników
25. Kontrola profili dostępowych w formie polityk
26. Wsparcie dla Disaster Recovery
27. Użytkownik uprzywilejowany musi mieć możliwość pracy co najmniej w następujących trybach:
    1. Agentowy – dostępne wszystkie funkcjonalności. Agent musi być dostępny bezpłatnie
    2. Bezagentowo, za pomocą przeglądarki internetowej wraz z dedykowanym rozszerzeniem. Metoda ta musi umożliwiać uzupełnianie haseł przez PAM oraz nagrywanie sesji
    3. Bezagentowo, za pomocą przeglądarki internetowej bez dodatkowych rozszerzeń.

Uwierzytelnianie

1. Obsługa uwierzytelniania użytkowników za pomocą certyfikatów
2. Możliwość korzystania z lokalnej bazy danych użytkowników
3. Obsługa uwierzytelniania wieloskładnikowego opartego na SAML
4. Obsługa OIDC (openID Connect), SAML
5. Obsługa wielu połączeń SAML SP
6. Możliwość integracji z istniejącymi usługami uwierzytelniania, w nie mniejszym zakresie niż Active Directory, LDAP, radius.
7. Wsparcie dla integracji z istniejącymi systemami zarządzania tożsamościami
8. Możliwość obsługi większej liczby kont uprzywilejowanych w miarę rozwoju organizacji
9. Dostęp do zasobów użytkowników uprzywilejowanych musi również obejmować możliwości blokady w oparciu o dodatkowe parametry:
   1. Kontrola dostępu oparta na adresie źródłowym IP użytkownika
   2. Ograniczanie dostępu oparte na harmonogramie użytkownika
   3. Kontrola dostępu do docelowego serwera oparta o przypisane tagi ZTNA (stan stacji, z której następuje połączenie jest badany przez mechanizmy ZTNA)

Licencjonowanie

1. Oprogramowanie musi być objęte kompletną licencją producenta na całe rozwiązanie. Nie dopuszcza się dodatkowych wymagań licencyjnych dla systemu operacyjnego, bazy danych, oprogramowania serwera WWW lub podobnych.
2. Nie dopuszcza się licencjonowania ilości zasobów, do których realizowany jest nadzorowany dostęp.
3. Nie dopuszcza się licencjonowania ilości zajętego miejsca na dysku przez nagrania sesji.
4. Licencja systemu musi pozwalać na jednoczesne podłączenie się co najmniej 5 aktywnych użytkowników do monitorowanych zasobów.
5. Licencja musi pozwalać na użytkowanie rozwiązania co najmniej w okresie obowiązywania zakontraktowanej gwarancji wsparcia technicznego.

Monitorowanie i raportowanie

1. Możliwość monitorowania aktywności użytkowników z kontami uprzywilejowanymi.
2. Generowanie szczegółowych raportów audytowych w celu analizy i śledzenia działań użytkowników

Gwarancja i wsparcie techniczne

Gwarancja wsparcia technicznego i dostępności aktualizacji oprogramowania w celu utrzymania systemu w aktualnym i bezpiecznym stanie musi być zapewniona na okres 36 miesięcy.

1. **Wdrożenie zakupionych rozwiązań wraz z szkoleniem.**

**OPIS USŁUG**

1. Montaż urządzeń aktywnych
   1. Instalacja urządzeń w szafach rack
   2. Udrożnienie komunikacji pomiędzy szafami a punktami centralnymi (nie dotyczy położenia nowych kabli światłowodowych).
   3. Zapewnienie pokrycia switchy na warstwie access do wszystkich urządzeń końcowych za pomocą okablowania.
2. Zarządzanie urządzeniami typu switch
   1. Switche instalowane w siedzibie zamawiającego mają być skonfigurowane do zarządzania z konsoli NGFW
   2. Switche w ramach konfiguracji muszą mieć zaimplementowane polityki NAC na portach w min. zakresie: filtrowanie po MAC, vendorze, systemie operacyjnym, modelu
   3. Switche muszą zostać skonfigurowane tak aby urządzenie nieautoryzowane nie otrzymywało dostępu do segmentu i usług w sieci Zamawiającego
   4. Switche CORE zainstalowane w obu serwerowniach muszą zostać skonfigurowane do pracy w trybie wysokiej dostępności z NGFW, obsługiwać protokół MCLAG (Zamawiający zapewni dostępność włóknień światłowodowych)
   5. Wszystkie swiche typu access podłączone za pomocą światłowodu i wkładek SFP+ muszą być skonfigurowane do pracy z prędkością 10Gbit/s. Tam, gdzie jest to technicznie możliwe, za pomocą dwóch linków do dwóch odrębnych switch-a CORE.
3. Segmentacja sieci
   1. Zaplanowanie – przygotowanie nowych segmentów sieci (vlan)
   2. Uzgodnienie segmentów (vlan) z Zamawiającym (uwzględnienie aspektów bezpieczeństwa oraz wydajności)
   3. Konfiguracja segmentów sieci z uwzględnieniem najlepszych praktyk w zakresie cyber bezpieczeństwa, w tym obowiązkowo odseparowanie sieci biurowej, systemów serwerowych, systemu kopii zapasowych, urządzeń medycznych i sieci gościnnej).
   4. Zamawiający wymaga wsparcia inżyniera w procesie przeadresowania serwerów używanych na terenie szpitala.
   5. Zamawiający wymaga wsparcia w podłączaniu komputerów, serwerów oraz systemów biznesowych do nowych segmentów sieci utworzonych w ramach projektu.
   6. Zamawiający wymaga wsparcia w diagnostyce problemów z podłączeniem serwerów, komputerów i innych urządzeń (w tym urządzeń medycznych) do nowej sieci zamawiającego.
   7. Zamawiający wymaga przygotowania dokumentacji segmentacji sieci
   8. Zamawiający wymaga udokumentowania sposobu autoryzacji grup urządzeń przy pomocy polityk NAC na switchach dostępowych.
   9. Przetestowanie skuteczności zabezpieczeń sieciowych i przygotowanie protokołu i odbioru (min. test powinien zawierać scenariusz podłączenia nieautoryzowanego urządzenia oraz próby nieautoryzowanej komunikacji pomiędzy segmentami sieci)
4. Bezpieczeństwo komunikacji między segmentami sieci
   1. Opracowanie zasad tworzenia polityk firewall z uwzględnieniem:
      1. Nazewnictwa polityk
      2. Wyboru interfejsów i zakresów adresów
      3. Stosowania profili bezpieczeństwa w zakresie: AV, WebFilter, DNS filter, Application Control, IPS
      4. Stosowania głębokiej inspekcji SSL lub DNS Filtering
      5. Grupowania polityk
      6. Oznaczania zmian
   2. Zbudowanie polityk w zakresie ruchu pomiędzy segmentami
      1. Na bazie monitoringu komunikacji, doprecyzowanie otwarć komunikacji do niezbędnego zakresu portów i usług
      2. Wdrożenie reguły minimalnego niezbędnego dostępu.
      3. Monitoring komunikacji musi trwać nie krócej niż czas trwania projektu tak aby na bieżąco dostosować reguły to potrzeb biznesowych zamawiającego
      4. Audyt konfiguracji polityk (realizowany przez uprawnionego audytora ISO27001, ISO22301), zawierający weryfikację zgodności konfiguracji z dokumentacją.
5. Urządzenia typu firewall
   1. Muszą zostać prawidłowo skonfigurowane w celu wymiany automatycznej obiektów takich jak pojedyncze adresy hostów, grupy hostów, ustawienia z systemami do logowania zdarzeń, autentykacji.
   2. Muszą mieć skonfigurowane przez wykonawcę filtr ochrony przed złośliwym oprogramowaniem, IDS/IPS, Filtrowanie kategorii treści w zakresie ruchu z sieci lokalnej, DMZ do Internetu
   3. Muszą mieć zmienione wszystkie domyślne hasła
   4. Muszą mieć wyłączone nieużywane porty, usługi oraz konta.
   5. Muszą mieć ograniczony dostęp do portu MGM poprzez funkcje trustedhosts oraz silne uwierzytelnienie wyłącznie dla uprawnionych osób zabezpieczone 2FA
   6. Muszą mieć wdrożony automatyczny mechanizm kopiowania konfiguracji urządzenia do repozytorium konfiguracji przed zalogowaniem administratora.
   7. Muszą mieć wdrożony automatyczny mechanizm kopiowania konfiguracji w cyklu raz dziennie.
   8. Kopie zapasowe konfiguracji muszą być przetestowane pod kątem odtworzenia. Musi być przygotowana procedura odtworzeniowa a same kopie w muszą być odmiejscowione.
   9. Przeprowadzenie testów bezpieczeństwa skuteczności zabezpieczeń (test skuteczności protekcji AV w komunikacji sieciowej, blokowania nieautoryzowanej treści, zatrzymania komunikacji wykorzystującą podatność w hoście)
6. Automatyzacja security
   1. Wdrożenie i integracja z wszystkimi NFGW zamawiającego systemu korelacji logów i zdarzeń
   2. Przygotowanie cyklicznych raportów obrazujących bezpieczeństwo sieci zamawiającego
   3. Przygotowanie na bazie monitoringu zdarzeń zestawu wektorów ataku najczęściej występujących w sieci oraz przygotowanie mechanizmów automatyzujących reakcje na zdefiniowane ataki w min. stopniu: alert, wdrożenie działania np. blokada ruchu do czasu obsługi przez administratora.
   4. Wymaga się skonfigurowania profili komunikacji zapewniających wysyłanie alertów na określone z adresy e-mail wskazane przez zamawiającego
   5. Wymaga się skonfigurowania mechanizmów wspierających proces rejestrowania incydentów i zdarzeń w zakresie sieci w dedykowanym systemie do korelacji logów i obsługi zdarzeń
   6. Wymaga się skonfigurowania konektora LDAP do lokalnej domeny zamawiającego celem umożliwienia logowania przy pomocy grup, kont domenowych.
   7. Należy skonfigurować lokalne konto emergency na wypadek utraty usług ActiveDirectory z polityką trustedhost umożliwiającą logowanie z wybranego segmentu i adresu IP.
   8. Należy skonfigurować alert związany z logowaniem, próbą logowania na konta z grupy emergency
7. Zarządzanie konfiguracją Firewall
   1. Wdrożenie systemu do centralnego zarządzania NFGW na wskazanym przez zamawiającego hyperwizorze
   2. Podłączenie wszystkich NGFW do systemu centralnego zarządzania
   3. Zbudowanie mechanizmu wersjonowania i backup-u konfiguracji w trybie automatycznym
   4. Zbudowanie procesu automatyzacji podnoszenia urządzeń do wskazanej wersji firmware w zaplanowanych oknach czasowych
   5. Konfiguracja możliwości przetestowania planowanej zmiany konfiguracji NGFW w wirtualnym środowisku systemu do centralnego zarządzania NGFW
   6. Kopie zapasowe konfiguracji systemu centralnego zarządzania urządzeniami NFGW muszą być przetestowane pod kątem odtworzenia.
   7. Musi być przygotowana procedura odtworzeniowa systemu, wykonywane kopie zapasowe muszą być odmiejscowione.
8. Sieć WiFi
   1. Zaprojektowanie sieci bezprzewodowej WiFi dla strefy administracyjnej
   2. Wdrożenie warstwy bezpieczeństwa w oparciu o lokalne kontrolery domeny i natywną usługę NPS. Należy skonfigurować poziom szyfrowania WPA3-Enterprise. Konfiguracja jednego SSID z mechanizmem dynamicznego lokowania klienta w odpowiednim vlan-ie na podstawie atrybutów z RADIUS-a
   3. Skonfigurowanie sieci WIFI dla urządzeń niewspierających WPAx-Enterprise z adekwatnymi ograniczeniami w komunikacji, z dedykowanym segmentem sieci
   4. Zaprojektowanie sieci bezprzewodowej WiFi dla gości, poziom szyfrowania min. WPA2 z obsługą sieci 2.4GHz
   5. Wykonanie odpowiednich otwarć komunikacji w ten sposób, aby zapewnić separacje sieci szpitalnych od sieci gość
9. Wdrożenie protekcji poczty
   1. Konfiguracja protekcji SPF, DMARC, DKIM w zakresie domeny cmkarpacz.pl w systemie ochrony poczty
   2. Stworzenie polityk protekcji antyspamowej, antywirusowej, anty-phishingowej z uwzględnieniem protekcji linków przekazywanych w wiadomościach mailowych
   3. Konfiguracja backup-u poczty na zasób sieciowy NAS z wyłączeniem maili przekraczających ustaloną wielkość załącznika (maile takie są odrzucane)
   4. Konfiguracja protekcji backup-u poczty zapewniającą ochronę przed działaniem szkodliwego oprogramowania szkodliwego z rodziny ransomware
   5. Kopie zapasowe konfiguracji systemu protekcji kopii muszą być przetestowane pod kątem odtworzenia, musi być przygotowana procedura odtworzeniowa a same kopie w jednej generacji muszą być odmiejscowione.
   6. W przypadku poczty dostępnej z sieci publicznej dostęp musi być poprzedzony dwuskładnikowym uwierzytelnieniem.
   7. Przeprowadzenie testów skuteczności wdrożonych zabezpieczeń. W tym obowiązkowo bezpiecznapoczta.cert.pl
   8. Przetestowanie obowiązkowego stosowania drugiego składnika.
   9. Przygotowanie raportu o aktualizacji sygnatur systemu bezpieczeństwa pocztowego.
10. Wdrożenie systemu dostępu zdalnego w celu separacji podmiotów zewnętrznych i administratorów od systemów krytycznych.
    1. Przygotowanie kont użytkowników – zintegrowanie logowania z Active Directory (protokół LDAP).
    2. Konfiguracja serwerów docelowych w liczbie co najmniej 10 szt. w zakresie:
       1. Konfiguracji protokołów dostępu
       2. Konfiguracja cyklicznej zmiany poświadczeń
       3. Konfiguracja sejfu na dane uwierzytelniające
    3. Konfiguracja profili bezpieczeństwa filtrujących dane.
    4. Konfiguracja flow akceptacyjnych dla wybranych serwerów umożliwiających akceptację wybranych inicjowanych sesji zdalnych.
    5. Konfiguracja agentów w celu możliwości korzystania z natywnych aplikacji dostępu zdalnego.
11. Migracja dotychczasowych NGFW do nowych lokalizacji (dwie lokalizacje).
    1. Przeniesienie konfiguracji z istniejących urządzeń NGFW na nowe urządzenia.
    2. Uwzględnienie wymagań konfiguracyjnych zawartych w punkcie „urządzenia typu firewall” powyżej.
12. Wdrożenie systemu ochrony serwisów WEB-owych
    1. Inwentaryzacja aplikacji webowych i API wymagających ochrony WAF w organizacji.
    2. Instalacja WAF w formie maszyny wirtualnej na hyperwizorze zamawiającego
    3. Podłączenie do sieci, skonfigurowanie interfejsów sieciowych i adresacji IP
    4. Konfiguracja dostępu administracyjnego (GUI i CLI) z wykorzystaniem konektora LDAP, kont domenowych, reguł ograniczeń sieciowych – trusted host
    5. Skonfigurowanie trybu pracy WAF-a
    6. Konfiguracja reguł routingu ruchu przez WAF-a do aplikacji backendowych
    7. Konfiguracja adekwatnych dla aplikacji zabezpieczeń i reguł WAF, implementacja reguł: blokowanie ataków SQL injection, XSS, itp.
    8. Konfiguracja dla określonych usług wykrywania i blokowania anomalii i ataków zero-day (Virtual Patching)
    9. Konfiguracja alertów i notyfikacji bezpieczeństwa.
    10. Uruchomienie rejestrowania zdarzeń i raportowania incydentów.
    11. Analiza logów i dostosowywanie polityk w oparciu o obserwacje, monitorowanie stanu systemu i wydajności w całym okresie trwania projektu
    12. Przeprowadzenie testów penetracyjnych i testów działania w sieci produkcyjnej
    13. Dopasowanie reguł i polityk w celu minimalizacji false positive i zapewnienia wydajności
    14. Szkolenia personelu odpowiedzialnego za bezpieczeństwo aplikacji
13. Wsparcie serwisowe w zakresie infrastruktury w okresie trwałości projektu
    1. Usługa aktualizacji firmowane w sytuacji braku wsparcia dotychczasowego oprogramowania lub na żądanie zamawiającego.
    2. Usługa przeglądu konfiguracji, aktualizacji zgodnie z najlepszymi praktykami, zaleceniami producenta na żądanie zamawiającego.
    3. Modyfikacje konfiguracji na żądanie i w uzgodnieniu z zamawiającym.
    4. Komunikacja podatności dotyczących infrastruktury sieciowej (w tym w szczególności firewall NGFW) – informowanie o podatnościach mających wpływ na bezpieczeństwo sieci zamawiającego.
    5. Przegląd logów w kontekście wykrywania anomalii, błędów, utraty pojemności kluczowych komponentów
    6. Wsparcie serwisowe w okresie trwania projektu (36 miesięcy) w wymiarze: 4 dni miesięcznie.
    7. w/w usługi w punkcie „wsparcie serwisowe w zakresie infrastruktury” znajdą się w umowie serwisowej podpisanej z wykonawcą.
14. Szkolenia
    1. Szkolenie w formie warsztatowej z systemu analizy i raportowania logów – 1 dzień roboczy
    2. Szkolenie w formie warsztatowej z zarządzania przełącznikami
    3. Szkolenie w formie warsztatowej z zarządzania firewall za pomocą konsoli centralnego zarzadzania.
    4. Szkolenie z zakresu zarządzania bezpieczeństwem poczty.
    5. Szkolenie z zakresu zarządzania ochroną serwisów WEB
    6. Ze wszystkich szkoleń należy przygotować imienne certyfikaty potwierdzające zakres, datę wykonania i uczestnictwo wybranych osób na szkoleniach.
15. Dokumentacja
    1. Zamawiający wymaga przygotowania pełnej dokumentacji nowo powstałego środowiska z uwzględnieniem istniejącej infrastruktury sieciowej/serwerowej, AD, Oracle, SAN, systemów medycznych.
    2. Zamawiający wymaga opracowanie dokumentu zawierającego wymagania dotyczące podziału sieci wraz ze sposobem implementacji – dla zakupu sprzętu, oprogramowania oraz usług wdrożeniowych.
    3. Zamawiający wymaga rozrysowania połączeń sieciowych fizycznych (warstwa 2, oraz logicznych (warstwa 3) z uwzględnieniem segmentacji sieci powstałej podczas projektu.
    4. Zamawiający wymaga przygotowania dokumentacji opisu sposobu ochrony poczty wraz z dokumentacją istniejącej konfiguracji.

WYMAGANIA STAWIANE WYKONAWCY

1. Posiada niezbędną wiedzę i doświadczenie,

Opis sposobu dokonywania oceny spełniania tego warunku:

Niniejszy warunek zostanie uznany za spełniony, jeżeli Wykonawca:

1. posiada wdrożony i certyfikowany przez akredytowana jednostkę certyfikującą System Zarządzania Bezpieczeństwem Informacji ISO 27001: 2023
2. posiada status partnera oferowanego rozwiązania od co najmniej 6 lat
3. przedstawi co najmniej 9 dokumentów (lub w przypadku braku możliwości ich przedstawienia oświadczenie Wykonawcy) potwierdzających prawidłowe wdrożenie rozwiązań objętych przedmiotem zamówienia, przy czym:

* Co najmniej trzy z nich dotyczą wdrożeń rozwiązania typu Next Generation Firewall (NGFW), a ich wartość to co najmniej 100.000,00zł brutto każda,
* Co najmniej trzy z nich dotyczą rozwiązania protekcji poczty elektronicznej, a ich wartość wynosi co najmniej 70.000,00zł brutto każda.
* Co najmniej dwa z nich dotyczą rozwiązania klasy: system analizy logów i korelacji zdarzeń dedykowanych dla NGFW,
* Co najmniej jedno dotyczy rozwiązania PAM
* -Co najmniej cztery z ww. wdrożeń zostały przeprowadzone w szpitalach

1. Dysponowanie osobami zdolnymi do wykonania zamówienia

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy wykażą, że dysponują lub będą dysponować, który będzie uczestniczyć w wykonaniu zamówienia, spełniającymi następujące wymagania:

Kierownik projektu

- 1 osoba posiadająca następujące kwalifikacje i doświadczenie zawodowe:

* wykształcenie wyższe
* Certyfikat potwierdzający wiedzę z zakresu zarządzania projektami – Prince2 Practitioner lub równoważny
* Certyfikat CISM, CISA lub CISSP
* posiada co najmniej 3-letnie doświadczenie kierowania projektami w zakresie usług objętych przedmiotem zamówienia

Eksperci:

Jako zespół posiadają następujące certyfikaty:

- certyfikat CISM lub równoważny – co najmniej 1 osoba

- certyfikat CISA lub równoważny -co najmniej 1 osoba

- certyfikat CEH lub równoważny – co najmniej 1 osoba

- certyfikat OSCP lub równoważny – co najmniej 1 osoba

- certyfikat CISSP lub równoważny -co najmniej 1 osoba

- certyfikat CompTIa Security + lub równoważny- co najmniej 1 osoba

- certyfikat Comptia CySA+ lub równoważny- co najmniej 1 osoba

- certyfikat audytora wiodącego Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001:2023 wydany przez akredytowaną jednostkę certyfikującą lub równoważny – co najmniej 3 osoby

- certyfikat audytora wiodącego Systemu Zarządzania Ciągłością Działania wydany przez akredytowaną jednostkę certyfikującą lub równoważny – co najmniej 3 osoby

Jako certyfikat równoważny zamawiający rozumie posiadanie certyfikatów analogicznych do zakresu wskazanych certyfikatów tj. dotyczących analogicznej dziedziny merytorycznej, analogicznego stopnia poziomu kompetencji, analogicznego poziomu doświadczenia zawodowego wymaganego dla otrzymania danego certyfikatu itp.

1. znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie Przedmiotu Zamówienia.

Opis sposobu dokonywania oceny spełniania tego warunku:

Niniejszy warunek zostanie uznany za spełniony, jeżeli wykonawca wykaże, że jest ubezpieczony od odpowiedzialności cywilnej na kwotę 1 mln zł.