

Przełącznik sieciowy Typ I – 2 szt. (OT 1, OT 2, OT 3)

Parametry fizyczne:

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 30 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe:

- 24 porty GE RJ-45.
- 4 porty 10 GE SFP+ obsadzone wkładkami 10 GE SR.

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:

- 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..

<ul style="list-style-type: none"> ○ 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. <ul style="list-style-type: none"> ● Musi być możliwe redundantne połączenie z elementami zarządzającymi. ● Wraz ze sprzętem koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
<p>Gwarancja:</p> <ul style="list-style-type: none"> ● 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.
<p>Wymagania ogólne:</p> <ul style="list-style-type: none"> ● W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca wraz ze sprzętem 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.

Wymagania Ogólne

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

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

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

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery 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:
 - 5 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.

6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. 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.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
 - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
 - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
 - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łącz WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), 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. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. 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 chmurze.
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.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. 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.

4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

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

Logowanie

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

Testy wydajnościowe oraz funkcjonalne

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

Serwisy i licencje

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

- a) 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 [40] miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), dostawca wraz ze sprzętem przedłoży 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. Przed zawarciem umowy Wykonawca musi złożyć załączyc ~~do oferty~~ oświadczenie producenta że posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Access Point (4sztuki) (OT 6)

Urządzenie musi być w pełni kompatybilne, co ma wynikać z dokumentacji producenta, z kontrolerem sieci bezprzewodowej posiadanym przez Zamawiającego (funkcjonalność kontrolera sieci bezprzewodowej posiada klaster UTM Fortinet FortiGate 100F).

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:
 - a. Temperatura -20 – 45°C,
 - b. 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 dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
 - a. 2.4 GHz 802.11b/g/n,
 - b. 5 GHz 802.11a/n/ac.
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
5. Urządzenie musi być wyposażone w moduł BLE.
6. Urządzenie musi być wyposażone w jeden interfejs 10/100/1000 Base-TX. Należy dołączyć niezbędne okablowanie typu patchcord wymagane do podłączenia punktu dostępowego dopasowane i kompatybilne z istniejącą infrastrukturą Zamawiającego (zarówno od strony AP jak i przełącznika).
7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub zewnętrzny zasilacz.

8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
 - a. Tunnel,
 - b. Bridge,
 - c. Mesh.
9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
 - a. MIMO – 2x2,
 - b. Maksymalna przepustowość dla poszczególnych modułów radiowych:
 - i. 400 Mbps;
 - ii. 867 Mbps;
 - c. Wymagana moc nadawania:
 - i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
 - ii. min. 24 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
 - d. Wsparcie dla 802.11n 20/40Mhz HT,
 - e. Wsparcie dla kanałów 80MHz,
 - f. Anteny – 4 zewnętrzne dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.
 - g. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
 - h. Maksymalna deklarowana liczba klientów per moduł radiowy:
 - i. 512;
 - ii. 512;
12. Funkcje dodatkowe:
 - a. 802.11ac MU-MIMO Wave 2
 - b. Transmit Beam Forming (TxBF)
 - c. Low-Density Parity Check (LDPC) Encoding
 - d. Maximum Likelihood Demodulation (MLD)
 - e. Maximum Ratio Combining (MRC)
 - f. A-MPDU and A-MSDU Packet Aggregation

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta do dnia 30.06.2026r. , 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.

Przełącznik sieciowy typ II (2 sztuki) (OT 6)

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

Zamawiający jest w posiadaniu rozwiązania UTM, model FortiGate 60F. W ramach rozbudowy istniejącego systemu, której celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową, wymagany jest dostarczenie przełącznika w pełni kompatybilnego wg dokumentacji producenta z istniejącym rozwiązaniem Fortigate.

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: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymagany 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.
 - e) 4 porty 10 GE SFP+. Należy dołączyć do przełącznika 4 kompatybilne wkładki SFP+ MultiMode wraz odpowiednimi i kompatybilnymi do istniejącej instalacji okablowania strukturalnego Zamawiającego patchcordami optycznymi).

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.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
3. **Wraz ze sprzętem** 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 do dnia 30.06.2026, 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.

Rozbudowa urządzenia UTM FGT-80F– 1 szt. (OT 7, OT 8)

Zamawiający posiada urządzenie UTM firmy Fortinet FG-80F w ramach postępowanie wymagane jest dostarczenie następujących usług i funkcjonalności:

- wsparcie serwisowe na poziomie 24x7 w trybie Next Business Day na okres 24 miesięcy
- forticloud na 24 miesiące
-

Zadania wykonawcy

Usługi wdrożenia konfiguracji FortiSwitch oraz FortiAP (firewall Fortigate):

1. Przegląd i analiza obecnej konfiguracji posiadanego firewall Fortigate.
 2. Uruchomienie dedykowanego interfejsu zarządzającego przełącznikami FortiSwitch oraz FortiAP.
 3. Dodanie odpowiednich sieci VLAN zgodnie z wytycznymi Zamawiającego.
 4. Konfiguracja nowych polityk bezpieczeństwa dla sieci WLAN.
 5. Konfiguracja uwierzytelniania dla produkcyjnej sieci WLAN opartego o istniejącą Domenę Windows.
 6. Konfiguracja, wdrożenie analogicznej do posiadanej dekrypcji SSL dla sieci produkcyjnej WLAN.
 7. Konfiguracja polityk bezpieczeństwa (URL Filtering, antywirus, kontrola aplikacji, IPS) zgodnie z dobrymi praktykami dla sieci WLAN gościnnej oraz produkcyjnej.
 8. Stworzenie optymalnych profili IDS/IPS pod kątem ruchu przychodzącego i wychodzącego zgodnie z charakterystyką systemów docelowych dla nowych sieci.
 9. Utworzenie reguł komunikacyjnych dla istniejących sieci VLAN z siecią WLAN zgodnie z wytycznymi Zamawiającego
 10. Szkolenie z obsługi systemu i konfiguracji dla administratora
- Dodatkowe wymagania:
- Wykonawca winien posiadać status partnera producenta oferowanego przez siebie rozwiązania,
 - usługi instalacji i konfiguracji rozwiązania musi dokonywać specjalista posiadający certyfikat danego producenta poświadczający kompetencje w zakresie instalacji i konfiguracji.

Usługi wdrożenia, konfiguracji i instalacji przełączników:

- fizyczny montaż przełączników w szafach rack i instalacja okablowania zgodnie z wytycznymi Zamawiającego,
 - podłączenie okablowania do urządzeń klienckich i połączenie przełączników z Firewall oraz między sobą za pomocą łączy optycznych MM 10Gbit. Wykonawca zapewnia konieczne akcesoria do połączenia (odpowiednie patchcordsy miedziane i optyczne oraz wkładki optyczne kompatybilne z istniejącą infrastrukturą strukturalną Zamawiającego).
 - Reorganizacja istniejących połączeń sieci zgodnie z dobrymi praktykami zapewniającymi wysoką dostępność, wydajność, bezpieczeństwo oraz skalowalność,
 - integracja zarządzania przełącznikami w interfejsie Firewall.
 - Konfiguracja i optymalizacja protokołów transportu pod kątem wykorzystywanego pomiędzy systemami w sieci wykorzystującymi usługi disaster-recovery,
- Dodatkowe wymagania:
- Wykonawca winien posiadać status partnera producenta oferowanego przez siebie rozwiązania,
 - usługi instalacji i konfiguracji rozwiązania musi dokonywać specjalista posiadający certyfikat danego producenta poświadczający kompetencje w zakresie instalacji i konfiguracji.

Usługi wdrożenia i konfiguracji punktów dostępowych sieci bezprzewodowej:

- fizyczny montaż punktów dostępowych i instalacja okablowania zgodnie z wytycznymi Zamawiającego, podłączenie zasilaczy PoE pomiędzy przełącznikami a AP
- podłączenie okablowania do urządzeń klienckich i połączenie przełączników z Firewall oraz między sobą za pomocą łączy optycznych MM 10Gbit. Wykonawca zapewnia konieczne akcesoria do połączenia (odpowiednie patchcordsy miedziane i optyczne oraz wkładki optyczne kompatybilne z istniejącą infrastrukturą strukturalną Zamawiającego).
- Reorganizacja sieci zgodnie z dobrymi praktykami zapewniającymi wysoką dostępność, wydajność, bezpieczeństwo oraz skalowalność,
- integracja zarządzania punktami dostępowymi w interfejsie Firewall.
- połączenie z kontrolerem sieci Wifi i konfiguracja kontrolera zgodnie z dobrymi praktykami zapewniającymi wysoką dostępność, wydajność, bezpieczeństwo oraz skalowalność, integracja z Firewall i analizerm logów.

- wykonanie powdrożeniowego badania sieci wifi zawierającego reprezentację graficzną dla badanego obszaru zawierającego następujące informacje:

- siła sygnału podstawowego dla określonego pasma sieci wifi (Primary signal Strenght)
- siła sygnału zapasowego dla określonego pasma sieci wifi (Secondary signal strenght)
- stosunek sygnału do szumu (SNR)
- zmierzony szum otoczenia (Noise)
- Zakłócenia kanałowe - Channel Interference
- wykryte inne interferencje (Interferers)
- ścieżki pomiarowe