Załącznik Nr 5 do SWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa i wdrożenie sprzętu informatycznego w ramach konkursu grantowego „Cyfrowa Gmina”

Projekt „Cyfrowa gmina” jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 - 2020

Spis treści

1. Wstęp

W ramach zadania wykonawca dostarczy sprzęty i oprogramowanie wyszczególnione w niniejszym dokumencie oraz dokona wdrożenia zgodnego z opisem w sekcji „Wdrożenie". Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich systemów opisanych w tym dokumencie):

a) Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej,
b) Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by nie były używane,
c) Sprzęt musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej,
d) Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów. Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa),
e) Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich,
f) Zamawiający dopuszcza realizację poszczególnych grup funkcjonalnych przez zespoły urządzeń pod następującymi warunkami:
   i. połączenie urządzeń będzie zrealizowane w sposób nie ograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),
   ii. łączna wielkość zestawu nie będzie przekraczać wymaganej wielkości urządzenia,
   iii. zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,
   iv. wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem,
   v. Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ±10%, 50Hz;

2. Osprzęt sieciowy

2.1 Serwer – 1 sztuki

Obudowa	• Typu Tower • Możliwość dokupienia dedykowanego przez producenta serwera zestawu do montażu w szafie RACK;
Płyta główna	• Jednoprocesorowa; • Wyprodukowana i zaprojektowana przez producenta serwera • Możliwość instalacji procesorów 8-rdzeniowych; • Zainstalowany moduł TPM 2.0 • 4 złącza PCI Express, w tym:

	○ 2 fizyczne złącza o prędkości x8 gen. 4; ○ 2 fizyczne złącza o prędkości x4; • 4 gniazda pamięci RAM; • 4 zintegrowane porty SATA z możliwością konfiguracji RAID 0, 1, 10 oraz wsparciem dla systemów z rodziny Windows i Linux • Wsparcie dla technologii: ○ Dual Channel ○ ECC
Procesory	• Procesor 6-rdzeniowy • architektura x86 • Taktowanie 3,2GHz • 12 MB pamięci cache
Pamięć RAM	• Min. 32 GB pamięci RAM • DDR4 Registered • 3200Mhz • Możliwość zainstalowania 128GB pamięci RAM
Dyski twarde i napędy	• Minimum 8 wnęk dla dysków twardych Hotplug 3,5”; • Zainstalowany napęd DVD-RW • Zainstalowane 2 szt. HDD SATA 2TB HOT PLUG 3.5”;
Kontrolery LAN	• Trwale zintegrowana karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 1Gbit Base-T;
Kontrolery I/O	• Zainstalowany kontroler RAID 0, 1, 10, 5
Porty	• Zintegrowana karta graficzna ze złączem VGA z tyłu serwera • 2 porty USB 3.2 na panelu przednim, w tym 1 port USB-C; • 4 porty USB 2.0 dostępne z tyłu serwera; • 2 porty USB 3.2 dostępne z tyłu serwera; • 2 porty USB 3.2 dostępne wewnątrz serwera • Opcjonalny port serial; • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;
Zasilanie, chłodzenie	• Dwa zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy nie większej niż 500W;
Zarządzanie	• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera; • Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: ○ Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; ○ Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do

	komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; ○ Dostęp poprzez przeglądarkę Web, SSH; ○ Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; ○ Zarządzanie alarmami (zdarzenia poprzez SNMP) ○ Możliwość przejęcia konsoli tekstowej ○ Opcjonalne przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) ○ Obsługa serwerów proxy (autentykacja) ○ Obsługa VLAN ○ Możliwość konfiguracji parametru Max. Transmission Unit (MTU) ○ Wsparcie dla protokołu SSDP ○ Obsługa protokołów TLS 1.2, SSL v3 ○ Obsługa protokołu LDAP ○ Integracja z HP SIM ○ Synchronizacja czasu poprzez protokół NTP ○ Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); • Możliwość zainstalowania dedykowanej (lub zintegrowanej) pamięci flash o pojemności minimum 16 GB; Pamięć umożliwiająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN oraz umożliwiającej możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. • Opcjonalna możliwość zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
Wspierane OS	• Microsoft Windows Server 2019, 2022

	• VMWare vSphere 7.0 • Suse Linux Enterprise Server 15 • Red Hat Enterprise Linux 8
Gwarancja	• 2 lat gwarancji producenta serwera w trybie onsite z gwarantowanym przyjazdem do miejsca użytkowania sprzętu certyfikowanego przez producenta pracownika serwisu do końca następnego dnia roboczego; • Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; • Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; • Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty);
Dokumentacja, inne	• Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy lub producenta; • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; • W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; • Możliwość wykonania aktualizacji BIOS z nośnika USB • Urządzenie zostanie dostarczone z szafą montażową stojącą o minimalny wymiarach[mm]: szerokość 600, głębokość 800, wysokość 1250

System operacyjny serwera	Ze względu na posiadane aplikacje Serwer będzie dostarczony wraz z oprogramowaniem Windows Server 2019 ESS 1-2CPU ROK lub nowszym

2.2 UTM – 1 sztuka

Wymagania Ogólne

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

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

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

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

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 24 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.
5. 7. 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 1.4 Gbps.
6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

13. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
14. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu.
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.

17. Element systemu realizujący funkcję Firewall musi integrować 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
    - Google Cloud Platform (GCP).
    - OpenStack.
    - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
    - Wsparcie dla IKE v1 oraz v2.
    - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
    - Obsługa protokołu Diffie-Hellman grup 19 i 20.
    - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
    - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
    - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
    - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
    - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
    - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
    - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
    - Routingu statycznego.
    - Policy Based Routingu.
    - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

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

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
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 powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

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

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

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. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

2.3 Przełącznik sieciowy 48 portów– 2 sztuki

- Minimum 48 portów 10BASE-T/100BASE-TX/1000BASE-T ze wsparciem dla trybów: full-duplex, half-duplex, automatycznej negocjacji (auto-negotiation)
- Minimum 4 porty 1GE SFP, pozwalające na instalację wkładek Gigabitowych (SFP)
- Automatyczne wykrywanie przeplotu (Auto MDIX) na portach 10/100/1000Base-T
- Przepustowość: minimum 104 Gbps oraz 75 Mpps.
- Tablica adresów MAC o wielkości minimum 32 000 pozycji
- Obsługa ramek Jumbo: minimum 9kb
- Przełącznik wyposażony w co najmniej jeden zasilacz 230V/AC.
- Obsługa standardu LACP (Link Aggregation Control Protocol)
- Tablica ARP minimum 4000 wpisów
- Tablica routingu nie mniejsza niż 4000 wpisów dla IPv4 i 1000 wpisów dla IPv6
- Minimum 1000 interfejsów VLAN
- Routing IPv4 – minimum: statyczny (minimum 4000 tras), RIPv1, RIPv2, OSPF
- Routing IPv6 – minimum: statyczny (minimum 1000 tras), RIPng, OSPFv3
- Obsługa VRRP i VRRP6
- Obsługa Policy Base Routing (PBR)
- Obsługa ruchu Multicast: PIM-DM, PIM-SM, PIM-DM dla IPv6, PIM-SM dla IPv6, PIM-SSM dla IPv6, IGMP v1/v2/v3, IGMP v1/v2/v3 Snooping; MLDv1/v2, MLD Snooping, Multicast VLAN
- Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
- Obsługa protokołu PVST lub równoważnego.
- Wsparcie dla protokołu typu Ethernet Ring Protection Switching (ERPS, G.8032 v1 i v2)
- Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 aktywnych sieci VLAN
- Obsługa IEEE 802.1ad QinQ
- Obsługa GVRP (GARP VLAN Registration Protocol) lub równoważny. Funkcja

pozwalająca na automatyczne tworzenie statycznych sieci VLAN na określonej grupie urządzeń. Stworzenie określonych sieci VLAN na jednym urządzeniu musi powodować ich autentyczne utworzenie na innych przełącznikach z tej samej grupy (urządzenia w grupie muszą być od siebie nie zależne, nie połączone ze sobą w stos).

- Funkcja Root Protection umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
- Funkcja BPDU Protection – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom
- Wsparcie dla funcji DHCP Relay, DHCP client oraz DHCP Snooping
- Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
- Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu)
- Obsługa standardu 802.1p – min. 8 kolejek na porcie
- Funkcja wyboru sposobu obsługi kolejek, minimum – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP lub równoważny.
- Funkcja mirroringu portów lokalnego i zdalnego: SPAN i RSPAN
- Obsługa funkcji logowania do sieci zgodna ze standardem IEEE 802.1x oraz autoryzacja po adresach MAC. Obsługa serwerów TACACS+ i RADIUS
- LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED
- Funkcja centralnego uwierzytelniania administratorów na serwerze RADIUS
- Obsługa funkcji Voice VLAN
- Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
- Port konsoli RS232 ze złączem RJ45
- Port USB 2.0
- Obsługa Syslog
- Obsługa sFlow
- Obsługa NTP (Network Time Protocol)
- Obsługa protokołów 802.3ah, 802.1ag oraz Y.1731
- Obsługa RMON (minimum grupy 1/2/3/9)
- Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter
- Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania).
- Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).
- Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany

aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

- Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego
- Wsparcie dla mechanizmu wykrywania linków jednokierunkowych typu DLDP (Device Link Detection Protocol) lub równoważnego
- Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych
- Minimalny zakres pracy od 0°C do +50°C
- Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
- Wysokość w szafie 19" – 1U
- Maksymalny pobór mocy nie większy niż 100 W (nie wliczając sekcji zasilania PoE)
- Ochrona przepięciowa, nie gorsza niż 1.5kV dla portów przełącznika oraz zasilaczy AC.
- Wymagany jest serwis gwarancyjny producenta świadczony przez minimum 5 lat.
- Gwarantowany czas naprawy sprzętu – 10 dni roboczych od momentu zgłoszenia i potwierdzenia wady przez producenta.

3. Osprzęt komputerowy

3.1 Monitor - 15 sztuk

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1	Ekran	23"
2	Typ matrycy	TFT
3	Technologia podświetlania	LED
4	Rozdzielczość	1920x1080(FHD)
5	Czas reakcji	5 ms
6	Kontrast statyczny	3000:1
7	Kąt widzenia poziomy/pionowy	178 stopni /178 stopni
8	Gniazda we/wy	1 x 15-pin D-Sub 1 x HDMI 1 x 3,5 mm minijack
9	Jasność	250 cd/m2
10	Certyfikaty	CE
11	Waga	Ponieważ sprzęt może być montowany na ścianie jego waga nie powinna przekraczać 4 kg bez podstawy

12	Inne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Wszystkie komponenty i podzespoły monitora muszą pochodzić od jednego producenta lub muszą być przez niego certyfikowane.

3.2 Skaner do dokumentów -1 sztuka

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1	Typ skanera	Skaner z podajnikiem
2	Funkcje	Skanowanie w czerni i kolorze
3	Technologia	CIS lub CCD
4	Interfejsy	USB, Ethernet, Wi-Fi
5	Rozdzielczość skanowania	600x600
6	Pojemność podajnika	80 arkuszy A4 80 g/m2
7	Obsługiwane rozmiary papieru	A4-A6, niestandardowe
8	Obsługiwane typy nośników	papier zwykły, papier gruby, wizytówki, karty plastikowe o grubości do 1.32 mm
9	Gramatura papieru	40-200g/m2
10	Rodzaj automatycznego podajnika dokumentów	skanowanie dwustronne jednoprzebiegowe
11	Szybkość skanowania jednostronnego (w czerni i kolorze)	min 40 str/min przy rozdzielczości 300 dpi
12	Szybkość skanowania dwustronnego (w czerni i kolorze)	min. 80 str/min. przy rozdzielczości 300 dpi
13	Wyświetlacz LCD typ	kolor, dotykowy 4,3''
14	Skanowanie do	min. pliku, obrazu, sieci,
15	Skanowane do	formatu min. PDF, JPEG i TIFF
16	Dodatkowe funkcje	min. usuwanie pustych stron, automatyczne prostowanie
17	Sterowniki	min. TWAIN, WIA, ISIS
18	Obciążenie miesięczne	min. 120 000 arkuszy
19	Gwarancja producenta	min. 3 lata

3.3 Zasilacz awaryjny UPS – 1 sztuka

UPS	
Parametr	**Wymagania minimalne**
Moc pozorna	min. 6000VA
Moc rzeczywista	min. 6000W
Technologia	on-line (VFI), podwójna konwersja
Sprawność max (dla VFI)	> 95 %
Typ obudowy	rack/tower
praca sieciowa	
Napięcie wejściowe	110V – 275V
Częstotliwość napięcia wejściowego	45 - 55Hz
Zakres napięcia wyjściowego	208 V AC / 220 V AC / 230 V AC / 240 V AC
Wartość napięcia wyjściowego ustawiana z panelu LCD	tak
Kształt napięcia wyjściowego	sinusoidalny
Czas przełączania sieć – UPS	0ms
Współczynnik odkształceń prądu wejściowego THDi	< 3%
praca bateryjna	
Napięcie wyjściowe	~230V ± 1%
Częstotliwość napięcia wyjściowego	50Hz/60Hz ± 1Hz
Kształt napięcia wyjściowego na pracy bateryjnej	sinusoidalny
Zabezpieczenie przeciwzwarciowe gniazd wyjściowych	Bezpiecznik automatyczny 20 A
Zabezpieczenie przeciążeniowe	elektroniczne
Akumulatory wewnętrzne w UPS lub w Modułach Bateryjnych	minimum 12V 9Ah; szczelne, bezobsługowe
Czas podtrzymania dla obciążenia 6000W	minimum 7 min
pozostałe	
Przeciążalność	100%＜obciążenie ≤105%: ciągłe 105%＜obciążenie ≤125%: 10 minut 125%＜obciążenie ≤150%: 30s >150% : 500m
Wejście zasilania	Listwa zaciskowa
Ilość i typ gniazd wyjściowych (w UPS lub przy wykorzystaniu zew PDU)	minimum 6x IEC 320 C13 (10 A) + 2x IEC 320 C19 (16A), listwa zaciskowa

Sygnalizacja	Wyświetlacz LCD (informacje wskazujące pracę sieciową, bateryjną, przeciążenie i ładowanie akumulatora). Diody LED informujące o pracy bateryjnej oraz stanie alarmowym.
Test baterii	Wymagana możliwość wykonania testu baterii do niskiego poziomu - możliwości całkowitego rozładowania baterii
Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych	Wymagana możliwość podłączenia minimum 6 zewnętrznych modułów bateryjnych
Interfejs komunikacyjny	RS232, USB, SNMP
Funkcjonalność karty SNMP	Wymagane wsparcie dla szyfrowania SSL oraz obsługa zasilacza UPS poprzez standardową bazę obiektów MIB lub zdefiniowaną przez użytkownika
Złącze EPO	wymagane NC
Styki bezpotencjałowe zamontowane na stałe w obudowie UPS	wymagany minimum 1x wejściowy i 1x wyjściowy
Możliwość pracy równoległej	wymagana możliwość połączenia minimum 3 jednostek
Wsporniki do montażu w szafie RACK	wymagane
Waga UPSa	do 15kg
Waga pojedynczego MODUŁU BATERYJNEGO (jeżeli występuje)	do 69kg
Wymiary UPS - wersja RACK	nie większe niż: wysokość 86mm; szerokość 438mm; głębokość 576mm
Wymiary MODUŁ BATERYJNY - wersja RACK (jeżeli występuje)	nie większe niż: wysokość 130mm; szerokość 438mm; głębokość 596mm
Łączna wysokość w szafie RACK 19" dla oferowanego zestawu	nie więcej niż 5U
Gwarancja	minimum 24 miesiące na elektronikę i 24 miesiące na akumulatory; Gwarancja realizowana wyłącznie przez autoryzowany serwis producenta
Serwis	autoryzowany serwis producenta zlokalizowany w Polsce.
	naprawa w maksymalnie 5 dni roboczych
	serwis realizowany w systemie door to door

Oprogramowanie	oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS dla Windows, Linux oraz systemów wirtualizacji VMware, Hyper-V, Citrix XenServer
	możliwość edycji nazw urządzeń na liście monitorowanych UPSów
	wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.
Certyfikaty producenta (załączyć do oferty)	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania;
	deklaracja CE producenta sprzętu
Oświadczenia / dokumenty	oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji
	karta katalogowa oferowanego sprzętu, wytyczne instalacyjne zawierające przynajmniej wymagania odnośnie zabezpieczeń i przekroi kabli zasilających.

4. Wdrożenie

Zamawiający dopuszcza przeprowadzenie wdrożenia w formie hybrydowej. Przy czym minimalna ilość dni jakie wykonawca powinien poświęcić na konfiguracje i podłączenie w siedzibie zamawiającego nie powinna być mniejsza niż 2 dni.

4.1 Firewall

a) Montaż urządzeń w szafie rack

b) Nadanie adresu IP

c) Konfiguracja dostępu SSH

d) Zmiana haseł dostępu

e) Aktualizacja oprogramowania do najnowszej możliwej wersji

f) Stworzenie reguł bezpieczeństwa

g) Konfiguracja routingu

i) Wdrożenie funkcjonalności DPI

j) Konfiguracja firewall, reguły przychodzące i wychodzące na podstawie obecnie działających usług

k) Konfiguracja ochrony przed malware, exploitami oraz stronami zawierającymi złośliwy kod

l) Wdrożenie PKI oraz konfiguracja polityki za pomocą których przeprowadzona zostanie dystrybucja certyfikatów, do realizowania deszyfracji SSL

m) Konfiguracja klienta VPN

n) Transfer wiedzy do klienta na temat obsługi zaproponowanej konfiguracji

4.2 Przełączniki sieciowe

a) Nadanie adresu IP

b) Konfiguracja dostępu SSH

c) Zmiana haseł dostępu

d) Skonfigurowanie stosów przełączników zgodnie z zaleceniami działu IT (ustawienia przełącznika master i backup)

e) Aktualizacja oprogramowania do najnowszej możliwej wersji

f) Uruchomienie protokół zapobiegania pętlą MSTP lub równoważny

g) Konfiguracja wysyłania logów do serwera logów

h) Konfiguracja funkcjonalności wykrywania telefonów IP, protokół LLDP lub równoważny

i) Uruchomienie protokołu DHCP Snooping lub równoważny

j) Konfiguracja VLANów na wszystkich urządzeniach

k) Konfiguracja access listy zgodnie z wymaganiami zamawiającego

l) Konfiguracja protokołu STP

m) Konfiguracja protokołu loop protect lub równoważny

n) Transfer wiedzy do klienta

4.3 Serwer

a) Instalacja dostarczonego sprzętu w szafie rack w siedzibie Zamawiającego

b) Podłączenie serwera fizycznego z posiadaną przez Zamawiającego infrastrukturą teleinformatyczną.

c) Konfiguracja:

   i. Konfiguracja dostarczonego serwera,
   ii. Konfiguracja wirtualizacji
   iii. Konfiguracja wirtualnych switchy (podział na 4 podsieci: BACKUP, DMZ, LAN, MGMT GUEST)

d) Przeniesienie baz danych oraz kluczowych aplikacji Zamawiającego na nowy system operacyjny.

e) Przeniesienie wszystkich niezbędnych aplikacji z punktu widzenia Zamawiającego wraz z testami poprawności działania po migracji na nowy system operacyjny.

f) Utworzenie lub migracja usług systemu operacyjnego:

vii. Utworzenie od podstaw usługi kontrolera domeny Windows.

viii. Migracja usługi DHCP - wymagane przeniesienie pełnej dotychczasowej konfiguracji dotyczącej zakresów, zasad i zastrzeżeń, wraz z zachowaniem dotychczasowego adresu IP. Migracja nie może wpłynąć na pracę użytkowników końcowych i infrastruktury sieciowo-serwerowej.

g) Transfer wiedzy do klienta

4.4 UPS

a) Instalacja dostarczonego sprzętu w szafie rack w siedzibie Zamawiającego

b) Podłączenie UPS-a z posiadaną przez Zamawiającego infrastrukturą teleinformatyczną.

4.5 Testy powdrożeniowe

Po dokonaniu całości wdrożenia należy:

a) przeprowadzić testy poprawności działania całej infrastruktury

b) przygotować dokumentację powykonawczą zawierająca listę dostarczonego sprzętu wraz z numerami seryjnymi i opisem konfiguracji poszczególnych elementów systemów

c) Ze względu na krytyczne aplikacje które będą dostępne z sieci publicznej, Wykonawca przeprowadzi testy podatności systemów (testy penetracyjne). Testy będą polegały na zdalnej enumeracji otwartych portów oraz weryfikacji bezpieczeństwa oprogramowania na nich nasłuchującego. Skanowanie obejmie:

- urządzenia dedykowane (embeded), na przykład routery i przełączniki;
- punkty styku z sieciami obcymi
- zbadanie podatności systemów Zamawiającego na ataki przeprowadzane z zewnątrz
- Ponadto Wykonawca przeprowadzi badanie bezpieczeństwa sieci systemów komputerowych, które pozwoli na:

- określenie błędów w konfiguracji skutkujących powstaniem podatności na atak;
- wskazanie nadmiernych uprawnień, niezgodnych z zasadami dobrych praktyk;

Badaniu będą podlegały następujące systemy:

- rodzina Microsoft Windows Server (do poziomu weryfikacji poprawek Windows Update włącznie);
- Linux 2.4.x, 2.6.x, 3.x.x;

Badanie zostanie zakończone raportem. Forma i zakres raportu musi być zaakceptowany przez dział informatyki.