URZĄD MARSZAŁKOWSKI
WOJEWÓDZTWA PODLASKIEGO
15-888 BIAŁYSTOK
ul. Kardynała Stefana Wyszyńskiego 1

Białystok, 06 sierpnia 2021 r.

BZP.272.19.2021

Wykonawcy
(uczestnicy postępowania)

Zamawiający informuje, iż w postępowaniu o udzielenie zamówienia publicznego pn. **„Rozwój e-usług Województwa podlaskiego”„ nr BZP.272.19.2021** wpłynęło pytanie, którego treść wraz z odpowiedzią przekazuję poniżej:

Pytanie nr 1:
Wykonawca wnosi o wyjaśnienie i zmianę postanowień SIWZ:
Informujemy Zamawiającego, że po zapoznaniu się z treścią postępowania oznaczonego znakiem BZP.272.19.2021 „Rozwój e-usług Województwa podlaskiego” prowadzonego przez Urząd Marszałkowski Województwa Podlaskiego, „Załącznik nr 1 e do OPZ Firewall średni_MŁomża” oraz „Załącznik nr 1 f do OPZ Firewall mały” po analizie opisu przedmiotu zamówienia i kontakcie z kluczowymi producentami rozwiązań z obszaru bezpieczeństwa sieci działającymi w Polsce lub posiadającymi swoje centrum serwisowe w Polsce, oświadczamy, że sposób w jaki został opisany przedmiot zamówienia w rażący sposób narusza przepisy art. 7 ust. 1 PZP i art. 29 ust. 1, 2 i 3 PZP i nie ma możliwości zaoferowania innych rozwiązań niż SOPHOS XGS2100 oraz SOPHOS XGS3300 który łącznie spełnia wyspecyfikowane przez Zamawiającego wymagania.
Poniżej wskazujemy którzy producencie np. nie wskazują publicznie wydajności firewall mierzonej jako ruch IMIX co powoduje rażące ograniczenie konkurencji:
Palo Alto - nie ma
Checkpoint - nie ma
Watchguard - nie ma
Fortigate - nie ma
Poza firmą Sophos, firma Stormshield podaje wydajność dla firewall IMIX, jednak tutaj również otrzymaliśmy potwierdzenie, że rozwiązania Stormshield nie spełniają łącznie wskazanych przez Zamawiającego wymagań.
W związku z powyższym wnioskujemy do Zamawiającego o dopuszczenie poniższych parametrów równoważności -co pozwoli Zamawiającemu uniknąć zawyżonych kosztów zakupu oraz korekty dofinansowania:

Czy Zamawiający dopuści rozwiązanie równoważne o parametrach równoważności:
Równoważność dla „Załącznik nr 1 e do OPZ Firewall średni_MŁomża”

Typ systemu ochrony
System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym.
Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część jako router, część jako bridge).

Wymagania systemowe
System ochrony powinien spełniać wymagania w niżej wymienionym zakresie.
Obsługa nielimitowanej ilości hostów w sieci chronionej.
Minimalna liczba i typ interfejsów fizycznych: 8x GE (IEEE 1000Base-T), 2x SFP GE (IEEE 1000Base-X), 2x USB 3.0 (Type-A), 1x Console (RJ-45 lub DB9) z możliwością rozbudowy o co najmniej 8 x GE (IEEE 1000Base-T lub IEEE1000Base-X).
Minimalna liczba i typ interfejsów wirtualnych: 512 (IEEE 802.1Q)
Minimalna liczba nowych połączeń na sekundę: 80 000
Minimalna liczba jednoczesnych połączeń: 1 500 000
Minimalna przepustowość Firewall: 29 000 Mbps
Minimalna przepustowość IPS: 14 000 Mbps
Minimalna przepustowość Web Proxy AV: 2 000 Mbps
Minimalna przepustowość IPSec: 3 000 Mbps
Minimalna liczba równoczesnych tuneli IPSec VPN: 1 000
Minimalna liczba równoczesnych tuneli SSL VPN:150
Przestrzeń dyskowa do celów logowania i raportowania o pojemności nie mniejszej niż 120 GB
PODSTAWOWE FUNKCJE SYSTEMU OCHRONY
Zarządzanie i utrzymanie
Rozwiązanie powinno być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI).
Wbudowany webowy graficzny interfejs użytkownika powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute.
Interfejs graficzny powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP.
Rozwiązanie powinno oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz protokołu SSH z autoryzacją za pośrednictwem kluczy.
Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
System powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności.
System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.
System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.
Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade).
System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.
Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora.
System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji.
Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej.
System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP.
Rozwiązanie powinno oferować wsparcie dla protokołów SNMP v1, v2 i v3 oraz co najmniej Netflow v5 (lub odpwiednik).

System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, w ramach webowego interfejsu graficznego urządzenia.
System powinien oferować możliwość integracji z centralnym systemem do zarządzania.
Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do dedykowanego serwera.
Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych.
Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.
Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego.
Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu on-cloud.
Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware).
System ochrony powinien umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive.
.
Zapora sieciowa, konfiguracja sieciowa oraz routing
Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection.
Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, użytkownik, grupa lub czas.
System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.
Polisy zapory powinny umożliwiać egzekwowanie ruchu dla poszczególnych sieci lub usług.
.
Rozwiązanie powinno pozwolić na definiowanie własnych polis NAT wraz z IP masquerading.
System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
System powinien zapewniać ochrona przed skanowaniem portów (portscan blocking).
System powinien zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).
Rozwiązanie powinno zapewniać obsługę routingu statycznego.
Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).
Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.
Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (bridge) oraz mostów zbudowanych z wielu portów (bridge).
System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.
System powinien oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP.
Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.
Rozwiązanie powinno umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów.
Rozwiązanie powinno oferować wsparcie dla Policy Based Routing oraz Multipath Rules.
Wymagane jest by rozwiązanie zapewniało obsługę dowolnych modemów USB 3G/LTE/UMTS pochodzących od dowolnego producenta.

Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).
System powinien zapewniać pełną obsługę usług DNS, DHCP oraz NTP.
Podstawowe kształtowanie pasma oraz limity ilości danych
System powinien zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników.
System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
Autoryzacja użytkowników
Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication.
Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont.
System powinien zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS, LDAP.
Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory.
Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowisku opartym o Windows Terminal Server.
System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.
Rozwiązanie powinno zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.
Rozwiązanie powinno oferować możliwość uwierzytelniania przez wbudowany Captive Portal.
Samoobsługowy portal dla użytkowników
Rozwiązanie powinno udostępniać plik instalacyjny agenta do autentykacji w sieci.
Rozwiązanie powinno udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).
Rozwiązanie powinno udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows.
Rozwiązanie powinno udostępniać plik z konfiguracją dla klientów SSL VPN dla innych systemów operacyjnych w tym dla Mac OS X, Linux, iOS, Android.
Rozwiązanie powinno umożliwiać zmianę nazwy użytkownika oraz hasła.
Podstawowe opcje VPN
System powinien zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:
Site-to-site VPN: IPSec, 256-bit AES/3DES, PFS, autoryzacja z użyciem klucza PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK)
Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
Klient IPSec VPN
Autoryzacja poprzez współdzielony klucz Pre-Shared Key (PSK), PKI (X.509), Smartcard, Token + XAUTH.
Szyfrowanie z użyciem AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (2048 bit), DH grupy 1/2/5/14, MD5 oraz SHA-256/384/512.
Wsparcie dla split-tunneling.
Wsparcie dla NAT-traversal.
Monitorowanie stanu połączenia.
OCHRONA SIECI
IPS
Moduł ochrony klasy IPS z bazą minimum 2000 sygnatur.
Rozwiązanie powinno zapewniać możliwość dodawania własnych sygnatur IPS.
Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.

Rozwiązanie powinno oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów.
System powinien generować alerty w przypadku wykrycia ataku.
ATP
System ochrony powinien zapewniać wykrywanie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control.
Clientless VPN
Udostępnianie zasobów w postaci usług RDP, VNC, SSH, Telnet, FTP, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji.
OCHRONA I KONTORLA WEB ORAZ APLIKACJI
Ochrona i kontrola Web
Rozwiązanie powinno działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.
Moduł pozwalający na wykrycie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control (ATP).
System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.
System powinien oferować możliwość uruchomienia drugiego niezależnego silnika antywirusowego.
Rozwiązanie powinno automatyczne odpytywać bazy producenta (on-cloud) w trybie rzeczywistym.
Rozwiązanie powinno zapewniać skanowanie plików.
Rozwiązanie powinno oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. walidacją certyfikatów.
System powinien oferować funkcję Web cache dla ograniczenia zużycia pasma.
System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.
Rozwiązanie powinno zapewniać filtrowanie plików Activex, apletów , cookies.
System powinien zapewniać możliwość emulacji skryptów JavaScript.
Rozwiązanie powinno oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.
Rozwiązanie powinno zawierać kategoryację stron www i umożliwiać tworzenie własnych kategorii stron www.
Rozwiązanie powinno zapewniać możliwość blokowanie wysyłania treści poprzez HTTP i HTTPS.
Rozwiązanie powinno umożliwiać blokadę stron HTTPS.
Rozwiązanie powinno blokować anonimowe proxy działające poprzez HTTP i HTTPS.
Rozwiązanie powinno umożliwiać definiowanie polityk dostępu do internetu w oparciu o harmonogramy dzienne/tygodniowe/miesięczne/roczne dla użytkowników i grup użytkowników.
System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator powinien mieć możliwość edytowania treści komunikatu i dodania logo organizacji.
Ochrona i kontrola aplikacji
Rozwiązanie powinno oferować bazę danych opisująca co najmniej 300 aplikacji.
Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji.
Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
Rozwiązanie powinno umożliwiać blokowanie:
- aplikacji, które pozwalają na transfer plików (np. P2P).
- komunikatorów internetowych, przynajmniej Skype, Gadu-gadu.
- proxy uruchamianych poprzez przeglądarki internetowe.
- streaming media (radio internetowe, Youtube, Vimeo).
Rozwiązanie powinno umożliwiać szczegółową kontrolę dostępu do Facebooka.,.

Kształtowanie pasma dla Web i Aplikacji
Rozwiązanie powinno oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron.
Rozwiązanie powinno zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.
Rozwiązanie powinno oferować możliwość gwarantowania pasma.
OCHRONA I KONTROLA EMAIL
Ochrona i kontrola Email
Rozwiązanie powinno oferować możliwość wyboru trybu pracy: Transparent Email Proxy.
System powinien umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S.
Rozwiązanie powinno zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.
System powinien umożliwiać uruchomienie drugiego niezależnego silnika antywirusowego.
Rozwiązanie powinno automatyczne odpytywać bazy producenta (on-cloud) w trybie rzeczywistym.
Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur zagrożeń.
System powinien zapewniać wykrywanie, blokowanie i skanowanie załączników.
Rozwiązanie musi umożliwiać ustawienie określonego przez administratora rozmiaru dla analizy Sandbox.
System powinien wykrywać próby phishingu przez analizę adresów URL zamieszczanych w treści wiadomości.
System powinien oferować mechanizm analizy ruchu szyfrowanego TLS dla SMTP, POP.
Rozwiązanie powinno współpracować z co najmniej dwoma bazami RBL.
Rozwiązanie powinno umożliwiać tworzenie białych i czarnych list adresów IP i email.
Rozwiązanie powinno zapewniać wykrywanie spamu niezależnie od stosowanego języka.
OCHRONA SERWERÓW APLIKACYJNYCH WEB
WAF
Rozwiązanie powinno oferować ochronę przed SQL injection.
Rozwiązanie powinno oferować ochronę przed Cross-site scripting.
System powinien zapewniać inspekcję ruchu HTTP.
System powinien umożliwiać uruchomienie drugiego niezależnego silnika antywirusowego.
OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY
On-cloud Sandboxing
Dodatkowy moduł ochrony klasy on-cloud Sandbox.
Rozwiązanie umożliwiające dodatkową inspekcję plików dokumentów w tym .doc, .docx, .docm, .rtf.
Rozwiązanie umożliwiające dodatkową inspekcję plików .pdf.
Rozwiązanie umożliwiające dodatkową inspekcję plików archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z.
System zapewniający dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows i MacOS.
System powinien oferować szczegółowe raporty.
LOGOWANIE I RAPORTOWANIE
Logowanie i raportowanie
System musi umożliwiać składowanie oraz archiwizację logów za pomocą wbudowanego i bezpłatnego mechanizmu.
System powinien gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.

System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. Skali.
System powinien zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.
System powinien zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).
Rozwiązanie powinno umożliwiać wysyłanie raportów via email.
Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.
System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym dla wszystkich lub indywidualnego łącza.
System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych
Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.
System powinien pozwalać ustalić okres retencji danych dla poszczególnych kategorii informacji.
POZOSTAŁE
Certyfikaty
CE, Common Criteria EAL4+
Subskrypcje
Oferta musi zawierać subskrypcje dla wszystkich wymaganych modułów na okres nie krótszy niż 36 miesięcy
Gwarancja i wsparcie
Wsparcie techniczne w trybie 8x5 na okres nie krótszy niż
Gwarancja na sprzęt na okres nie krótszy niż 36 miesięcy
Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji.
Równoważność dla „Załącznik nr 1 f do OPZ Firewall mały”
ARCHITEKTURA SYSTEMU OCHRONY
Typ systemu ochrony
System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym.
Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część jako router, część jako bridge).
Wymagania systemowe
System ochrony powinien spełniać wymagania w niżej wymienionym zakresie.
Obsługa nielimitowanej ilości hostów w sieci chronionej.
Minimalna liczba i typ interfejsów fizycznych: 6x GE (IEEE 1000Base-T), 2x GE (IEEE 1000Base-X), 2x USB 3.0 (Type-A), 1x Console (RJ-45 lub DB9)
Minimalna liczba i typ interfejsów wirtualnych: 350 (IEEE 802.1Q)
Minimalna liczba nowych połączeń na sekundę: 25 000
Minimalna liczba jednoczesnych połączeń: 500 000
Minimalna przepustowość Firewall: 7 000 Mbps
Minimalna przepustowość IPS: 3 000 Mbps
Minimalna przepustowość Web Proxy AV: 900 Mbps
Minimalna przepustowość IPSec: 1 000 Mbps
Minimalna liczba równoczesnych tuneli IPSec VPN: 500
Minimalna liczba równoczesnych tuneli SSL VPN: 100
Zintegrowany dysk SSD do celów logowania i raportowania o pojemności nie mniejszej niż 120 GB.
PODSTAWOWE FUNKCJE SYSTEMU OCHRONY

Zarządzanie i utrzymanie
Rozwiązanie powinno być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI).
Wbudowany webowy graficzny interfejs użytkownika powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute.
Interfejs graficzny powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP.
Rozwiązanie powinno oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz protokołu SSH z autoryzacją za pośrednictwem kluczy.
Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
System powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności.
System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.
System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.
Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade).
System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.
Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora.
System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji.
Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej.
System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP.
Rozwiązanie powinno oferować wsparcie dla protokołów SNMP v1, v2 i v3 oraz co najmniej Netflow v5 (lub odpwiednik).
System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, w ramach webowego interfejsu graficznego urządzenia.
System powinien oferować możliwość integracji z centralnym systemem do zarządzania.
Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do dedykowanego serwera.
Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych.
Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.
Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego.
Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu on-cloud.
Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware).

System ochrony powinien umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive.

.

Zapora sieciowa, konfiguracja sieciowa oraz routing

Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection.

Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, użytkownik, grupa lub czas.

System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.

Polisy zapory powinny umożliwiać egzekwowanie ruchu dla poszczególnych sieci lub usług.

.

Rozwiązanie powinno pozwolić na definiowanie własnych polis NAT wraz z IP masquerading.

System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection).

System powinien zapewniać ochrona przed skanowaniem portów (portscan blocking).

System powinien zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).

Rozwiązanie powinno zapewniać obsługę routingu statycznego.

Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).

Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.

Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (bridge) oraz mostów zbudowanych z wielu portów (bridge).

System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.

System powinien oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP.

Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.

Rozwiązanie powinno umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów.

Rozwiązanie powinno oferować wsparcie dla Policy Based Routing oraz Multipath Rules.

Wymagane jest by rozwiązanie zapewniało obsługę dowolnych modemów USB 3G/LTE/UMTS pochodzących od dowolnego producenta.

Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).

System powinien zapewniać pełną obsługę usług DNS, DHCP oraz NTP.

Podstawowe kształtowanie pasma oraz limity ilości danych

System powinien zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników.

System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.

Autoryzacja użytkowników

Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication.

Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont.

System powinien zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS, LDAP.

Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory.

Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowisku opartym o Windows Terminal Server.
System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.
Rozwiązanie powinno zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.
Rozwiązanie powinno oferować możliwość uwierzytelniania przez wbudowany Captive Portal.
Samoobsługowy portal dla użytkowników
Rozwiązanie powinno udostępniać plik instalacyjny agenta do autentykacji w sieci.
Rozwiązanie powinno udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).
Rozwiązanie powinno udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows.
Rozwiązanie powinno udostępniać plik z konfiguracją dla klientów SSL VPN dla innych systemów operacyjnych w tym dla Mac OS X, Linux, iOS, Android.
Rozwiązanie powinno umożliwiać zmianę nazwy użytkownika oraz hasła.
Podstawowe opcje VPN
System powinien zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:
Site-to-site VPN: IPSec, 256-bit AES/3DES, PFS, autoryzacja z użyciem klucza PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK)
Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
Klient IPSec VPN
Autoryzacja poprzez współdzielony klucz Pre-Shared Key (PSK), PKI (X.509), Smartcard, Token + XAUTH.
Szyfrowanie z użyciem AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (2048 bit), DH grupy 1/2/5/14, MD5 oraz SHA-256/384/512.
Wsparcie dla split-tunneling.
Wsparcie dla NAT-traversal.
Monitorowanie stanu połączenia.
OCHRONA SIECI
IPS
Moduł ochrony klasy IPS z bazą minimum 2000 sygnatur.
Rozwiązanie powinno zapewniać możliwość dodawania własnych sygnatur IPS.
Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.
Rozwiązanie powinno oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów.
System powinien generować alerty w przypadku wykrycia ataku.
ATP
System ochrony powinien zapewniać wykrywanie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control.
Clientless VPN
Udostępnianie zasobów w postaci usług RDP, VNC, SSH, Telnet, FTP, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji.
OCHRONA I KONTORLA WEB ORAZ APLIKACJI
Ochrona i kontrola Web
Rozwiązanie powinno działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.
Moduł pozwalający na wykrycie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control (ATP).
System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.

System powinien oferować możliwość uruchomienia drugiego niezależnego silnika antywirusowego.
Rozwiązanie powinno automatyczne odpytywać bazy producenta (on-cloud) w trybie rzeczywistym.
Rozwiązanie powinno zapewniać skanowanie plików.
Rozwiązanie powinno oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. walidacją certyfikatów.
System powinien oferować funkcję Web cache dla ograniczenia zużycia pasma.
System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.
Rozwiązanie powinno zapewniać filtrowanie plików Activex, apletów , cookies.
System powinien zapewniać możliwość emulacji skryptów JavaScript.
Rozwiązanie powinno oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.
Rozwiązanie powinno zawierać kategoryację stron www i umożliwiać tworzenie własnych kategorii stron www.
Rozwiązanie powinno zapewniać możliwość blokowanie wysyłania treści poprzez HTTP i HTTPS.
Rozwiązanie powinno umożliwiać blokadę stron HTTPS.
Rozwiązanie powinno blokować anonimowe proxy działające poprzez HTTP i HTTPS.
Rozwiązanie powinno umożliwiać definiowanie polityk dostępu do internetu w oparciu o harmonogramy dzienne/tygodniowe/miesięczne/roczne dla użytkowników i grup użytkowników.
System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator powinien mieć możliwość edytowania treści komunikatu i dodania logo organizacji.
Ochrona i kontrola aplikacji
Rozwiązanie powinno oferować bazę danych opisująca co najmniej 300 aplikacji.
Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji.
Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
Rozwiązanie powinno umożliwiać blokowanie:
- aplikacji, które pozwalają na transfer plików (np. P2P).
- komunikatorów internetowych, przynajmniej Skype, Gadu-gadu.
- proxy uruchamianych poprzez przeglądarki internetowe.
- streaming media (radio internetowe, Youtube, Vimeo).
Rozwiązanie powinno umożliwiać szczegółową kontrolę dostępu do Facebooka.,.
Kształtowanie pasma dla Web i Aplikacji
Rozwiązanie powinno oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron.
Rozwiązanie powinno zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.
Rozwiązanie powinno oferować możliwość gwarantowania pasma.
OCHRONA I KONTROLA EMAIL
Ochrona i kontrola Email
Rozwiązanie powinno oferować możliwość wyboru trybu pracy: Transparent Email Proxy.
System powinien umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S.
Rozwiązanie powinno zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.
System powinien umożliwiać uruchomienie drugiego niezależnego silnika antywirusowego.
Rozwiązanie powinno automatyczne odpytywać bazy producenta (on-cloud) w trybie rzeczywistym.
Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur zagrożeń.

System powinien zapewniać wykrywanie, blokowanie i skanowanie załączników.
Rozwiązanie musi umożliwiać ustawienie określonego przez administratora rozmiaru dla analizy Sandbox.
System powinien wykrywać próby phishingu przez analizę adresów URL zamieszczanych w treści wiadomości.
System powinien oferować mechanizm analizy ruchu szyfrowanego TLS dla SMTP, POP.
Rozwiązanie powinno współpracować z co najmniej dwoma bazami RBL.
Rozwiązanie powinno umożliwiać tworzenie białych i czarnych list adresów IP i email.
Rozwiązanie powinno zapewniać wykrywanie spamu niezależnie od stosowanego języka.
OCHRONA SERWERÓW APLIKACYJNYCH WEB
WAF
Rozwiązanie powinno oferować ochronę przed SQL injection.
Rozwiązanie powinno oferować ochronę przed Cross-site scripting.
System powinien zapewniać inspekcję ruchu HTTP.
System powinien umożliwiać uruchomienie drugiego niezależnego silnika antywirusowego.
OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY
On-cloud Sandboxing
Dodatkowy moduł ochrony klasy on-cloud Sandbox.
Rozwiązanie umożliwiające dodatkową inspekcję plików dokumentów w tym .doc, .docx, .docm, .rtf.
Rozwiązanie umożliwiające dodatkową inspekcję plików .pdf.
Rozwiązanie umożliwiające dodatkową inspekcję plików archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z.
System zapewniający dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows i MacOS.
System powinien oferować szczegółowe raporty.
LOGOWANIE I RAPORTOWANIE
Logowanie i raportowanie
System musi umożliwiać składowanie oraz archiwizację logów za pomocą wbudowanego i bezpłatnego mechanizmu.
System powinien gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.
System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. Skali.
System powinien zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.
System powinien zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).
Rozwiązanie powinno umożliwiać wysyłanie raportów via email.
Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.
System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym dla wszystkich lub indywidualnego łącza.
System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych
Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.
System powinien pozwalać ustalić okres retencji danych dla poszczególnych kategorii informacji.
POZOSTAŁE

Certyfikaty
CE, Common Criteria EAL4+
Subskrypcje
Oferta musi zawierać subskrypcje dla wszystkich wymaganych modułów na okres nie krótszy niż 36 miesięcy
Gwarancja i wsparcie
Wsparcie techniczne w trybie 8x5 na okres nie krótszy niż
Gwarancja na sprzęt na okres nie krótszy niż 36 miesięcy
Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji.

Odpowiedź:
Zamawiający nie dopuszcza zaproponowanych przez Wykonawcę wymagań. Szczegółowe wymagania w tym zakresie opisano w OPZ.

W przypadku rozbieżności pomiędzy treścią SWZ, a treścią udzielonych wyjaśnień lub zmian SWZ, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.

z up. MARSZAŁKA WOJEWÓDZTWA
Marian Malinowski
Dyrektor Biura Zamówień Publicznych
/podpisano elektronicznie/