OP.272.50.2022

Załącznik Nr 1b do SWZ - Szczegółowy opis przedmiotu zamówienia

Urządzenie klasy UTM/NGFW wraz z licencjami i wsparciem technicznym – 8 szt.

Wymagania minimalne:

1. Urządzenie posiada certyfikat bezpieczeństwa EU RESTRICTED oraz NATO RESTRICTED, CE (Conformité Européenne) - dołączyć wydruki certyfikatów do oferty lub podać bezpośrednie linki;
2. Producent urządzenia ma siedzibę na obszarze Unii Europejskiej,
3. W zakresie obsługi sieci:
    a. Urządzenie posiada wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak DHCP.
4. W zakresie zapory (Firewall):
    a. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
    b. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
    c. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
    d. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
    e. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP (Differentiated Services Code Point) nagłówka pakietu, przypisania kolejki QoS (Quality of Service), określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
    f. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
    g. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
    h. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
    i. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.

j. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

5. W zakresie Intrusion Prevention System (IPS):
    a. System detekcji i prewencji włamań IPS ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
    b. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
    c. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
    d. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
    e. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
    f. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
    g. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
    h. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
    i. Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci.
    j. Powyższy moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu.
6. W zakresie kształtowania pasma (Traffic Shapping):
    a. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
    b. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
    c. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
    d. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
7. W zakresie ochrona antywirusowa:
    a. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).

b. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
c. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
d. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

8. W zakresie ochrona antyspam:
    a. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
    b. Ochrona antyspam ma działać w oparciu o:
        i. białe/czarne listy,
        ii. DNS RBL,
        iii. Skaner heurystyczny.
    c. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
    d. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
9. W zakresie wirtualne sieci prywatne (vpn):
    a. urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
    b. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
        i. PPTP VPN,
        ii. IPSec VPN,
        iii. SSL VPN.
    c. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
    d. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
    e. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
    f. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
    g. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
10. W zakresie filtr dostępu do stron www:
    a. Urządzenie ma posiadać wbudowany filtr URL.
    b. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
    c. Administrator ma mieć możliwość dodawania własnych kategorii URL.
    d. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
        i. blokowanie dostępu do adresu URL,
        ii. zezwolenie na dostęp do adresu URL,

iii. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

e. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
f. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
g. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
h. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
i. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

11. W zakresie uwierzytelnianie:
    a. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
        i. lokalną bazę użytkowników (wewnętrzny LDAP),
        ii. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
        iii. usługę katalogową Microsoft Active Directory.
    b. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
    c. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
        i. SSL,
        ii. Radius,
        iii. Kerberos.
    d. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
    e. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
    f. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
12. W zakresie administracji łączami do internetu (ISP)
    a. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
    b. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
        i. równoważenie względem adresu źródłowego,
        ii. równoważenie względem połączenia.
    c. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
    d. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
    e. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
    f. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).

g. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

13. W zakresie routingu (trasowania):
    a. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
    b. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
    c. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
    d. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
14. W zakresie administracji urządzeniem:
    a. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
    b. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
    c. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
    d. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
    e. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
    f. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
    g. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
    h. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
    i. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
    j. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
        i. manualnego eksportu do pliku w dowolnym momencie czasu,
        ii. automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
    k. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
    l. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
15. W zakresie raportowania:
    a. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

b. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
c. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
d. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
e. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
f. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
g. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
h. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

16. W zakresie pozostałe usługi i funkcje:
    a. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
    b. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
    c. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
    d. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny.
    e. Urządzenie ma posiadać usługę DNS Proxy.
    f. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
17. W zakresie – pasywny skaner wnętrza sieci
    a. urządzenie posiada pasywny skaner wnętrza sieci, wychwytujący luki bezpieczeństwa w wykorzystywanym w sieci oprogramowaniu (audyt podatności),
    b. ma działać każdorazowo, gdy komputer z sieci LAN generuje ruch przechodzący przez urządzenie, ruch ten ma być weryfikowany pod kątem generujących go aplikacji,
    c. ma weryfikować czy wykryta aplikacja jest wrażliwa na ataki lub posiada inne luki bezpieczeństwa,
    d. ma prezentować szczegółową listę aplikacji sieciowych, pracujących na stacjach, jak np. Google Desktop, Firefox, Skype, aplikacje do multimediów (streamingu audio/video), programy antywirusowe, itp.
    e. poprzez wskazanie (kliknięcie) na aplikację powoduje wyświetlenie wszystkich komputerów, na których dany program został wykryty, a także pozwala sprawdzić wersję tej aplikacji,

f. ma możliwość wyszukiwania nieaktualnych wersje oprogramowania na stacjach roboczych i serwerach,
g. ma możliwość wysyłania automatycznych powiadomień o zagrożeniach wskazując zagrożone stacje robocze,
h. posiada pomoc, która wskazuje źródła z których można pobrać odpowiednie poprawki i aktualizacje, które przywrócą optymalny poziom bezpieczeństwa.

18. W zakresie gwarancja i serwis:
    a. Urządzenie ma być objęte co najmniej **12-miesięczną gwarancją producenta** na dostarczone elementy systemu
    b. Urządzenie ma posiadać licencję dla wszystkich funkcji/modułów bezpieczeństwa (włączając audyt podatności) **do dnia 31 października 2023 r.**
    c. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
19. W zakresie parametry sprzętowe:
    a. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
    b. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów.
    c. Liczba portów Ethernet 10/100/1000Mbps – min.8.
    d. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
    e. Przepustowość Firewall (1518 bajtów UDP) – minimum 2Gbps.
    f. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 1.6Gbps.
    g. Przepustowość filtrowania Antywirusowego – minimum 400Mbps.
    h. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 350Mbps.
    i. Maksymalna liczba tuneli VPN IPSec – minimum 50.
    j. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20.
    k. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 20.
    l. Obsługa interfejsów 802.11q (VLAN) – minimum 128
    m. Liczba równoczesnych sesji – minimum 200 000 i nie mniej niż 15 000 nowych sesji/sekundę.
    n. Urządzenie nie ma limitu na liczbę użytkowników.
    o. Liczba reguł filtrowania – minimum 4 096.
    p. Liczba tras statycznego routingu – minimum 512.
    q. Liczba tras dynamicznego routingu – minimum 10 000.