ZADANIE II. DOSTAWA, INSTALACJA I WDROŻENIE URZĄDZENIA FIREWALL UTM NOWEJ GENERACJI

1. Minimalne parametry urządzenia

1) **OBSŁUGA SIECI**
   - Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.

2) **ZAPORA (Firewall)**
   - Urządzenie musi posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.
   - Urządzenie musi być wyposażone w Firewall klasy Stateful Inspection.
   - Urządzenie musi obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
   - Urządzenie musi dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
   - Interfejs (GUI) do konfiguracji firewalla musi 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 etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
   - Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia.
   - Administrator musi mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u.

- Edytor reguł na firewallu musi posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).
- Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).

3) **INTRUSION PREVENTION SYSTEM (IPS)**

- System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
- Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy.
- Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
- Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
- Moduł IPS musi nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej.
- Urządzenie musi mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
- Administrator urządzenia musi 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.

4) **KSZTAŁTOWANIE PASMA (Traffic Shapping)**

- Urządzenie musi mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
- Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.

- Rozwiązanie musi umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).
- Urządzenie musi umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

5) **OCHRONA ANTYWIRUSOWA (AV)**

- Rozwiązanie musi zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
- Co najmniej jeden z dwóch skanerów antywirusowych musi być dostarczany w ramach podstawowej licencji.
- Administrator musi mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
- Administrator musi 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 odrzucenia.

6) **OCHRONA ANTYSPAM (AS)**

- Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
- Ochrona antyspam ma działać w oparciu o:
  - białe/czarne listy,
  - DNS RBL,
  - heurystyczny skaner.
- W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.
- Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

7) **WIRTUALNE SIECI PRYWANTE (VPN)**

- Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
- Odpowiednio kanały VPN można budować w oparciu o:
  - PPTP VPN,
  - IPSec VPN,
  - SSL VPN
  - SSL VPN musi działać w trybach Tunel i Portal.
- W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN
- współpracującego z oferowanym rozwiązaniem.
- Urządzenie musi posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
- Urządzenie musi posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
- Urządzenie musi umożliwiać tworzenie tuneli w oparciu o technologię Route Based.

8) **FILTR DOSTĘPU DO STRON WWW**

- Urządzenie musi posiadać wbudowany filtr URL.
- Filtr URL musi działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
- Administrator musi mieć możliwość dodawania własnych kategorii URL.
- Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.
- Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.
- Administrator musi posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:

- blokowanie dostępu do adresu URL,
- zezwolenie na dostęp do adresu URL,
- blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

- Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
- Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.
- Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.
- Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
- Urządzenie musi posiadać możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.
- Urządzenie musi posiadać możliwość włączenia pamięci cache dla ruchu http.

9) **UWIERZYTELNIANIE**

- Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:
  - lokalną bazę użytkowników (wewnętrzny LDAP),
  - zewnętrzną bazę użytkowników (zewnętrzny LDAP),
  - usługę katalogową Microsoft Active Directory.
- Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP.
- Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:
  - SSL,
  - Radius,
  - Kerberos.
- Urządzenie musi posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory.

- Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.
- Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.

10) **ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)**

- Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
- Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
  - równoważenie względem adresu źródłowego,
  - równoważenie względem połączenia.
- Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
- Urządzenie musi posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
- Urządzenie musi posiadać mechanizm statycznego trasowania pakietów.
- Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
- Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
- Rozwiązanie musi zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
- Rozwiązanie musi wspierać technologię Link Aggregation.

11) **POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA**

- Urządzenie musi posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.

- Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.
- Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.
- Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS
- Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.
- Urządzenie musi posiadać usługę DNS Proxy.

12) **ADMINISTRACJA URZĄDZENIEM**

- Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.
- Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową, a komunikacja musi być zabezpieczona za pomocą protokołu https.
- Komunikacja może odbywać się na porcie innym niż https (443 TCP).
- Urządzenie musi być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
- Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.
- Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową, a komunikacja musi być zabezpieczona za pomocą protokołu https.
- Urządzenie musi mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS).
- Rozwiązanie musi mieć możliwość eksportowania logów za pomocą protokołu IPFIX.
- Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.
- Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z

serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.

13) **RAPORTOWANIE**

- Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
- System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
- System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.
- System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów.
- System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu.
- W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
- Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy.

14) **PARAMETRY SPRZĘTOWE**

- Urządzenie musi być wyposażone w dysk o pojemności co najmniej 320 GB.
- Wymagana liczba portów Ethernet 10/100/1000Mbps – minimum 8.
- Wymagana liczba portów światłowodowych 1Gbps pozwalających na użycie wkładek SX/LX – min. 2.
- Urządzenie musi mieć możliwość zainstalowania minimum jednej karty rozszerzeń z 8 interfejsami Ethernet 10/100/1000Mbps lub 4 światłowodowymi interfejsami 1Gbps lub 2 światłowodowymi interfejsami 10 Gbps,
- Przepustowość Firewalla – min. 10 Gbps,
- Przepustowość Firewalla wraz z włączonym systemem IPS – min. 7 Gbps,

- Przepustowość filtrowania Antywirusowego – min. 1,6 Gbps,
- Minimalna przepustowość tunelu VPN przy szyfrowaniu AES - 2 Gbps,
- Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 1000,
- Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 150,
- Maksymalna liczba VLAN nie może być mniejsza niż 256,
- Liczba równoczesnych sesji - min. 1 000 000 i nie mniej niż 40 000 nowych sesji/sekundę,
- Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive,
- Urządzenie musi być nielimitowane na użytkowników.

2. Wymagania dotyczące wdrożenia

1) **Wymagania ogólne**

- Wdrożenie nowego urządzenia ma na celu wymianę starej zapory sieciowej UTM Zamawiającego *Zyxel ZyWall USG 1000.*
- Wykonawca jest zobowiązany do wykonania instalacji i konfiguracji wymaganego urządzenia w dedykowanym pomieszczeniu serwerowni Zamawiającego, które jest wyposażone w niezbędną infrastrukturę sieciową, system zasilania awaryjnego i klimatyzację oraz szafę 42 U przeznaczoną na wykonanie wszelkich prac instalacyjnych stanowiących przedmiot zamówienia.

2) **Wymagany zakres prac wdrożeniowych**

- Wykonawca jest zobowiązany do wykonania wszelkich prac instalacyjnych dla nowego urządzenia, przeniesienia konfiguracji starej zapory sieciowej do nowego urządzenia i odtworzenia wszystkich połączeń fizycznych LAN/WAN.
- Przeniesienie konfiguracji powinno obejmować:
  - konfigurację LAN/WAN, w tym adresację IP urządzenia, VLAN-y (ilość - 5), trasy dla routingu statycznego (ilość - 10), polityka routowania (ilość - 13), usługi typu DHCP (ilość - 3), NAT (mapowane porty - ilość 10), VPN (ilość - 3), certyfikaty (ilość - 3), Radius (ilość - 1).
  - wszystkie aktywne reguły firewalla dla ruchu przychodzącego i wychodzącego (ilość

- 50 reguł) oraz wszystkie powiązane z nimi obiekty, typu: adresy (ilość - 113), grupy adresów (ilość - 20), numery portów (ilość - 130), grupy portów (ilość - 35), harmonogramy dla dostępu zdalnego (ilość - 3), użytkownicy (ilość - 6).

- Wykonawca musi dostarczyć urządzenie ze wszystkimi wymaganymi licencjami dla FW+IPS, VPN, filtr URL, AV i AS na okres minimum 1 roku.
- Wykonawca musi zapewnić gwarancję producenta na urządzenie wraz ze wsparciem serwisowym NBD 8x5 (czas reakcji - następny dzień roboczy od momentu zgłoszenia) na okres 24 miesięcy.
- Przeprowadzenie w siedzibie Zamawiającego szkolenia dla 2 administratorów urządzenia.

3) **Czas prowadzenia prac wdrożeniowych**

- Zamawiający nie dopuszcza możliwości wyłączenia dostępu do sieci w czasie od poniedziałku do piątku w godzinach 7:30 -15:30.
- Prace wymagające wyłączenia elementów infrastruktury sieciowej, należy wykonywać po godzinach pracy Zamawiającego lub w weekendy. Prace takie należy uzgadniać z pracownikami Wydziału Informatyki i Łączności z minimum dwudniowym wyprzedzeniem.

4) **Dodatkowe wymagania**

- Urządzenie musi być dostarczone w stanie fabrycznie nowym, wolnym od wad technicznych, prawnych i formalnych zwłaszcza w zakresie licencji i uprawnień do aktualizacji oprogramowania. Sprzęt nie może być wcześniej zarejestrowany na żadnego innego klienta w bazie klientów producenta sprzętu.
- Zamawiający wymaga przed podpisaniem protokołu odbioru sprzętu zażądać oświadczenia producenta na podstawie numerów seryjnych, że oferowany sprzęt jest nowy i pochodzi z legalnego kanału dystrybucyjnego producenta. Jeśli sprzęt nie spełnia tych warunków Zamawiający odstąpi od umowy z winy Oferenta.
- Serwis urządzenia musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta.