Załącznik nr 6 do SIWZ

Część 6 zamówienia – sprzęt sieciowy Z.5

I. UTM typ 1 – 5 szt.

Lokalizacja – miejsce dostawy/ montażu/uruchomienia:

Zespół Szkół w Hucie Dąbrowie -1szt
Zespół Szkół w Okrzei - 1szt.
Szkoła Podstawowa w Krzywdzie - 1szt.
Szkoła Podstawowa w Radoryżu Kościelnym. - 1szt.
Szkoła Podstawowa w Radoryżu Smolanym - 1szt

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. Powinna istnieć możliwość dedykowania 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.

Interfejsy, Dyski:

1. System realizujący funkcję Firewall musi dysponować minimum 14 portami Gigabit Ethernet RJ-45, 2 gniazdami SFP 1 Gbps.
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.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1,2 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.

2. Przepustowość Stateful Firewall: nie mniej niż 4 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 800 Mbps.
4. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA1: nie mniej niż 2,5 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 1,5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem AES256-SHA1) dla ruchu http – minimum 300 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, IMAP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Analiza ruchu szyfrowanego protokołem SSL.
10. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
11. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. 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.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

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 Diffiego-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.
3. Dla modułów: IPSec VPN oraz SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. Klient VPN musi umożliwiać weryfikację stanu bezpieczeństwa stacji zdalnej.
4. Rozwiązanie powinno zapewniać funkcjonalność VTEP (VXLAN Tunnel End Point)

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.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

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.

Kontrola Antywirusowa

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. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. 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.

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 2800 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, Botnet.
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, phishing, spam, Dynamic DNS, proxy avoidance.
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. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

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.

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. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie:

1. System musi mieć możliwość logowania 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 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 certyfikaty:

- ICSA lub EAL4 dla funkcji Firewall
- ICSA lub NSS Labs dla funkcji IPS
- ICSA dla funkcji: SSL VPN, IPSec VPN

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 24 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 8x5.

II. UTM typ 2 – 2 szt.

Lokalizacja – miejsce dostawy/ montażu/uruchomienia:

Szkoła Podstawowa w Fiukówce - 1szt.
Szkoła Podstawowa w Woli Okrzejskiej - 1szt.

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. Powinna istnieć możliwość dedykowania 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.

Interfejsy, Dyski:

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.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1,2 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 3 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 500 Mbps.
4. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA1: nie mniej niż 2 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 1400 Mbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 180 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem AES256-SHA1) dla ruchu http – minimum 300 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, IMAP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Analiza ruchu szyfrowanego protokołem SSL.
10. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
11. 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.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. 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.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

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 Diffiego-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.

3. Dla modułów: IPSec VPN oraz SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. Klient VPN musi umożliwiać weryfikację stanu bezpieczeństwa stacji zdalnej.
4. Rozwiązanie powinno zapewniać funkcjonalność VTEP (VXLAN Tunnel End Point)

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.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

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.

Kontrola Antywirusowa

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. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. 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.

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 2800 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, Botnet.
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, phishing, spam, Dynamic DNS, proxy avoidance.
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. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

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.

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. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie:

1. System musi mieć możliwość logowania 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 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 certyfikaty:

- ICSA lub EAL4 dla funkcji Firewall
- ICSA lub NSS Labs dla funkcji IPS
- ICSA dla funkcji: SSL VPN, IPSec VPN

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 24 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 8x5.

III. Licencja UTM typ 1 –5 szt.

Lokalizacja – miejsce dostawy/ montażu/uruchomienia:

Zespół Szkół w Hucie Dąbrowie -1szt
Zespół Szkół w Okrzei - 1szt.
Szkoła Podstawowa w Krzywdzie - 1szt.
Szkoła Podstawowa w Radoryżu Kościelnym. - 1szt.
Szkoła Podstawowa w Radoryżu Smolanym - 1szt

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów dla urządzenia klasy UTM zaproponowanego w ofercie. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres min. 24 miesięcy.

IV. Licencja UTM typ 2 –2 szt.

Lokalizacja – miejsce dostawy/ montażu/uruchomienia:

Szkoła Podstawowa w Fiukówce - 1szt.
Szkoła Podstawowa w Woli Okrzejskiej - 1szt.

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów dla urządzenia klasy UTM zaproponowanego w ofercie. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres min. 24 miesięcy.

V. Kontroler – 5 szt.

Lokalizacja – miejsce dostawy/ montażu/uruchomienia:

Zespół Szkół w Hucie Dąbrowie -1szt
Zespół Szkół w Okrzei - 1szt.
Szkoła Podstawowa w Krzywdzie - 1szt.
Szkoła Podstawowa w Radoryżu Kościelnym. - 1szt.
Szkoła Podstawowa w Radoryżu Smolanym - 1szt

Kontroler sieci bezprzewodowej obsługujący punkty dostępowe i klientów WiFi, wyposażony w oprogramowanie umożliwiające scentralizowane zarządzanie siecią bezprzewodową, automatyczną konfigurację AP, a także pracą sieci WLAN. Platforma obsługuje minimalnie 10 punktów dostępowych. Kontroler sieciowy musi być kompatybilny z punktem dostępowym. Kontroler powinien zostać dostarczony z licencją na obsługę min. 10 punktów dostępowych.
Kontroler musi spełniać następujące wymagania:

- zarządzać centralnie wszystkimi punktami dostępowymi,
- umożliwiać zbieranie informacji o poszczególnych stacjach roboczych podłączonych do punktów dostępowych zarządzanych przez kontroler bezpośrednio z interfejsu WWW kontrolera (adres MAC, stan uwierzytelnienia stacji, przydzielony adres IP),
- umożliwiać uzyskanie informacji na temat obciążenia poszczególnych kanałów radiowych,
- umożliwiać zbieranie informacji na temat innych punktów dostępowych będących w zasięgu propagowanej sieci,
- zapewniać przydział użytkowników do VLAN-ów (IEEE 802.1Q) na podstawie informacji przesyłanej w atrybutach Access-Accept protokołu RADIUS,
- pozwalać na definiowanie co najmniej 6 profili SSID, zapewniając możliwość zdefiniowania różnych metod szyfrowania lub jego wyłączenie dla każdego z SSID oraz rozdziału ruchu do odrębnych VLANów (IEEE 802.1Q), z jednoczesnym uwzględnieniem przydziału dynamicznego na podstawie informacji przesyłanej w atrybutach Access-Accept protokołu RADIUS,
- zarządzając punktami dostępowymi pracującymi w standardach WPA-Enterprise/TKIP oraz WPA2-Enterprise/AES propagującymi sieć, gwarantować przełączanie użytkownika między punktami dostępowymi; przełączenie użytkownika musi się odbywać bez ponownego uwierzytelnienia zarówno w WPA-Enterprise/TKIP jak i WPA2-Enterprise/AES,
- kontroler musi posiadać wewnętrzną bazę danych użytkowników na potrzeby uwierzytelniania klientów 802.1x oraz captive portal,
- kontroler musi mieć zapewnioną min. 24 miesięczną gwarancję producenta. Kontroler powinien być objęty dodatkowym wsparciem technicznym uprawniającym do aktualizacji oprogramowania i kontaktów z linią wsparcia technicznego producenta, w trybie 8/5/365,
- kontroler powinien być wyposażony przynajmniej w cztery porty 10/100/1000 Base-T Ethernet oraz port konsoli (RJ45 lub USB),

- kontroler musi umożliwiać kontrolę aplikacji (deep packet inspection) opartą o bazę minimum 2000 aplikacji,
- kontroler musi umożliwiać diagnostykę stacji końcowych oraz punktów dostępowych w czasie rzeczywistym, oraz udostępniać podgląd logów z aktywności stacji końcowych,
- kontroler musi zapewniać mechanizmy wysokiej dostępności dla minimum dwóch kontrolerów,
- kontroler lub punkt dostępowy musi zapewniać możliwość zapisywania pakietów do dalszej analizy tzw. packet-capture (zarówno dla ruchu wired jak i wireless),
- kontroler musi umożliwiać funkcje skanera pasma, analizatora widma w oparciu o zarządzane punkty dostępowe,
- kontroler musi zapewniać funkcje koncentratora vpn dla zdalnie podłączonych punktów dostępowych.

Kontroler może być zintegrowany z UTM lub stanowić oddzielne urządzenie.

VI. Przełącznik sieciowy typ 1 – 4 szt.

Lokalizacja – miejsce dostawy/ montażu/uruchomienia:

Szkoła Podstawowa w Radoryżu Kościelnym. - 1szt.
Szkoła Podstawowa w Radoryżu Smolanym - 1szt
Szkoła Podstawowa w Fiukówce - 1szt.
Szkoła Podstawowa w Woli Okrzejskiej - 1szt.

Opis:

1. Parametry fizyczne platformy:
   - wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U
   - Zasilanie 230V

2. Interfejsy sieciowe – wymagania minimalne:
   - 24 porty GE, RJ-45; wymaga się aby co najmniej 12 portów było zgodnych ze standardami 802.3af i 802.3at
   - 2 porty GE SFP
   - 1 dedykowany interfejs do zarządzania GE – RJ-45

3. Parametry wydajnościowe:
   - przepustowość urządzenia - min. 52 Gbps
   - możliwość zapamiętania co najmniej 16 000 adresów MAC
   - Opóźnienie - poniżej 2 mikrosekund

4. Wymagane funkcje:
   - możliwość automatycznej negocjacji prędkości i duplexu dla połączeń
   - obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree)
   - możliwość agregacji portów zgodna z 802.3ad
   - obsługa co najmniej 4000 VLANów, zgodna z 802.1Q
   - możliwość wykonywania routingu statycznego
   - port-mirroring
   - Kontrola dostępu na poziomie portu w oparciu o standard 802.1x, możliwość uwierzytelniania w oparciu o bazę Radius

- zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS, SNMP w wersjach 1-3, SNTP, LLDP (w trybie odbioru)
- możliwość zarządzania przez interfejs graficzny i tekstowy
- możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI
- integracja z systemem bezpieczeństwa (NGFW, UTM) pochodzącym od tego samego producenta, w zakresie co najmniej:
    - możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników
    - obsługa białych i czarnych list MAC
    - stateful firewall, umożliwiający kontrolę dostępu pomiędzy segmentami sieci
    - routing statyczny i dynamiczny, co najmniej OSPF

VII. Przełącznik sieciowy typ 2 – 2 szt.

Lokalizacja – miejsce dostawy/ montażu/uruchomienia:

Zespół Szkół w Okrzei - 1szt.

Szkoła Podstawowa w Krzywdzie - 1szt.

Opis:

1. Parametry fizyczne platformy:
    - wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U
    - Zasilanie 230V

2. Interfejsy sieciowe – wymagania minimalne:
    - 20 portów GE RJ-45; wymaga się aby co najmniej 12 portów było zgodnych ze standardami 802.3af
    - 4 porty typu combo GE RJ-45/SFP

3. Parametry wydajnościowe:
    - przepustowość urządzenia - min. 48 Gbps
    - możliwość zapamiętania co najmniej 16 000 adresów MAC
    - Opóźnienie - poniżej 2 mikrosekund

4. Wymagane funkcje:
    - możliwość automatycznej negocjacji prędkości i duplexu dla połączeń
    - obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree)
    - możliwość agregacji portów zgodna z 802.3ad
    - obsługa co najmniej 4000 VLANów, zgodna z 802.1Q
    - możliwość wykonywania routingu statycznego
    - port-mirroring
    - Kontrola dostępu na poziomie portu w oparciu o standard 802.1x, możliwość uwierzytelniania w oparciu o bazę Radius
    - zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS, SNMP w wersjach 1-3, SNTP, LLDP (w trybie odbioru)
    - możliwość zarządzania przez interfejs graficzny i tekstowy
    - możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI

- integracja z systemem bezpieczeństwa (NGFW, UTM) pochodzącym od tego samego producenta, w zakresie co najmniej:
    - możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników
    - obsługa białych i czarnych list MAC
    - stateful firewall, umożliwiający kontrolę dostępu pomiędzy segmentami sieci
    - routing statyczny i dynamiczny, co najmniej OSPF

VIII. Przełącznik sieciowy typ 3 – 1 szt.

Lokalizacja – miejsce dostawy/ montażu/uruchomienia:

Zespół Szkół w Hucie Dąbrowie - 1szt.

Opis:

1. Parametry fizyczne platformy:
    - wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U
    - Zasilanie 230V

2. Interfejsy sieciowe – wymagania minimalne:
    - 24 porty GE, RJ-45 zgodnych ze standardami 802.3af i 802.3at
    - 4 porty GE SFP
    - 1 dedykowany interfejs do zarządzania FE – RJ-45

3. Parametry wydajnościowe:
    - przepustowość urządzenia - min. 56 Gbps
    - możliwość zapamiętania co najmniej 16 000 adresów MAC
    - Opóźnienie - poniżej 2 mikrosekund

4. Wymagane funkcje:
    - możliwość automatycznej negocjacji prędkości i duplexu dla połączeń
    - obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree)
    - możliwość agregacji portów zgodna z 802.3ad
    - obsługa co najmniej 4000 VLANów, zgodna z 802.1Q
    - możliwość wykonywania routingu statycznego
    - port-mirroring
    - Kontrola dostępu na poziomie portu w oparciu o standard 802.1x, możliwość uwierzytelniania w oparciu o bazę Radius
    - zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS, SNMP w wersjach 1-3, SNTP, LLDP (w trybie odbioru)
    - możliwość zarządzania przez interfejs graficzny i tekstowy
    - możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI
    - integracja z systemem bezpieczeństwa (NGFW, UTM) pochodzącym od tego samego producenta, w zakresie co najmniej:
        - możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników

- obsługa białych i czarnych list MAC
- stateful firewall, umożliwiający kontrolę dostępu pomiędzy segmentami sieci
- routing statyczny i dynamiczny, co najmniej OSPF

IX. Punk dostępowy AP – 44 szt.

Lokalizacja – miejsce dostawy/ montażu/uruchomienia:

Zespół Szkół w Hucie Dąbrowie -8szt
Zespół Szkół w Okrzei - 8szt.
Szkoła Podstawowa w Krzywdzie - 8szt.
Szkoła Podstawowa w Radoryżu Kościelnym - 6szt.
Szkoła Podstawowa w Radoryżu Smolanym - 6szt
Szkoła Podstawowa w Fiukówce - 4szt.
Szkoła Podstawowa w Woli Okrzejskiej - 4szt.

Wymagania Ogólne

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

Obudowa urządzenia musi być wykonana z tworzywa sztucznego i umożliwiać montaż na suficie wewnątrz budynku.

Musi być wyposażone w dwa niezależne moduły radiowe pracujące w pasmach i obsługiwać następujące standardy:

1. 2.4 GHz b/g/n
2. 5 GHz a/n/ac

Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 14 SSID

Minimalna liczba interfejsów Ethernet – 2 w standardzie 10/100/1000 Base-TX

Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz

Interfejs radiowy urządzenia powinien wspierać minimum następujące funkcje:

1. MIMO – 4x4
2. Maksymalna przepustowość interfejsu dla poszczególnych pasm:
   a) 2.4GHz – 600 Mbps
   b) 5 GHz – 1733 Mbps
3. Wymagana moc nadawania min. 19 dBm
4. Wsparcie dla 802.11n 20/40Mhz HT
5. Wsparcie dla kanału 80 MHz dla 802.11ac
6. Anteny – 8 wbudowanych o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz

X. Wdrożenie sieci – 6 szt.

Lokalizacja – miejsce dostawy/ montażu/uruchomienia:

Zespół Szkół w Okrzei - 1szt.
Szkoła Podstawowa w Krzywdzie - 1szt.

Szkoła Podstawowa w Radoryżu Kościelnym - 1szt.
Szkoła Podstawowa w Radoryżu Smolanym - 1szt.
Szkoła Podstawowa w Fiukówce - 1szt.
Szkoła Podstawowa w Woli Okrzejskiej - 1szt.

1. Dostawca zobowiązuje się do montażu wszystkich elementów sieci. Adaptacja do istniejącego okablowania strukturalnego obejmuje uzupełnienie wszystkich niezbędnych akcesoriów.
2. Dostawca zobowiązuje się do wdrożenia sieci zgodnie z wytycznymi zamawiającego w zakresie konfiguracji urządzenia UTM oraz sieci bezprzewodowej w celu zapewnienia odpowiedniego poziomu bezpieczeństwa.
3. Dostawca zobowiązuje się do przeszkolenia w zakresie konfiguracji urządzeń do 7 osób w zakresie konfiguracji poszczególnych modułów, monitoringu i diagnozowania występujących w sieci zdarzeń w obrębie kontrolera sieci bezprzewodowej oraz urządzenia UTM.

Pozostałe minimalne wymagania, jakie muszą spełniać elementy dla tej części zamówienia:

- w cenie należy uwzględnić dostawę i montaż w/w elementów na miejscu wskazanym przez Zamawiającego,
- w cenie należy uwzględnić również koszty gdy producent sprzętu wymaga jego uruchomienia w obecności przedstawiciela serwisu w celu zachowania warunków gwarancji.

W ramach dostawy powyżej opisanych urządzeń Wykonawca w ramach ceny za dostawę urządzeń zobowiązany jest do rozpakowania, instalacji, integracji i uruchomienia- stosownie do potrzeb danego elementu przedmiotu zamówienia .
Wykonawca wraz ze sprzętem dostarczy odpowiednie gwarancje oraz dokumenty potwierdzające, że oferowany sprzęt posiada niezbędne normy, atesty i certyfikaty. Powyższe dokumenty wraz z kartami gwarancyjnymi winny być dostarczone w miejscu i terminie dostawy danego elementu zamówienia, przed podpisaniem protokołu odbioru końcowego.
W przypadku gdy producent danego elementu zamówienia (sprzętu) w celu zachowania warunków gwarancji wymaga uruchomienia przez przedstawiciela serwisu– organizację i koszt takiego uruchomienia ponosi Wykonawca – zawarty jest w cenie oferty.