

SECYFIKACJA TECHNICZNA ZAOFEROWANEGO SPRZĘTU

Przedmiot zamówienia: **Dostawa klastra UTM wraz z zestawem licencji dla Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach**

Urządzenie klasy UTM z zestawem licencji – 2 sztuki

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Oferowane
1.	Producent:	Proszę podać:	
2.	Nazwa i typ produktu:	Proszę podać:	
3.	Informacje ogólne	<p>Rozwiązanie musi być dostępne jako platforma sprzętowa. Urządzenie jest nielimitowane na użytkowników.</p> <p>Urządzenie musi być fabrycznie nowe.</p> <p>Dostarczone urządzenie musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład urządzenia 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.</p> <p>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 rozwiązania 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 co najmniej 8 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: Firewall, Ochrony w warstwie aplikacji. Protokołów routingu dynamicznego.</p>	TAK/NIE
4.	Redundancja, monitoring i wykrywanie awarii	<p>W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klastr Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.</p> <p>W ramach postępowania system musi zostać dostarczony w postaci redundantnej.</p> <p>Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</p> <p>Monitoring stanu realizowanych połączeń VPN.</p> <p>System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.</p>	TAK/NIE
5.	Parametry sprzętowe	<p>System realizujący funkcję Firewall musi dysponować minimum:</p> <ul style="list-style-type: none"> - 10 portami Gigabit Ethernet RJ-45 - 8 gniazdami SFP 1 Gbps. - 2 gniazdami SFP+ 10 Gbps. <p>System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</p> <p>W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard</p>	TAK/NIE

		802.1Q. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB. System musi być wyposażony w zasilanie AC.	
6.	Parametry wydajnościowe:	W zakresie Firewall'a obsługa nie mniej niż 8 mln jednoczesnych połączeń oraz 300.000 nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 36 Gbps dla pakietów 512 B. Przepustowość Stateful Firewall: nie mniej niż 32 Gbps dla pakietów 64 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 14 Gbps. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 20 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu HTTP - minimum 11 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 4.7 Gbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 6.8 Gbps.	TAK/NIE
7.	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 - zaporą ogniową klasy StatefulInspection. 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 - IntrusionPrevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Trafficshaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. Analiza ruchu szyfrowanego protokołem SSH.	TAK/NIE
8.	Polityki, Firewall	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 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. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.	TAK/NIE
9.	Połączenia VPN	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/CounterMode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and	TAK/NIE

		<p>SPOKE.</p> <ul style="list-style-type: none"> • 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. <p>2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:</p> <ul style="list-style-type: none"> • 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. 	
10.	Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie powinno zapewniać obsługę:</p> <ul style="list-style-type: none"> • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. <p>System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.</p>	TAK/NIE
11.	Zarządzanie pasmem	<p>System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.</p> <p>System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.</p>	TAK/NIE
12.	Kontrola Antywirusowa	<p>Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.</p> <p>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.</p>	TAK/NIE
13.	Ochrona przed atakami	<p>Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>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.</p> <p>Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p>	TAK/NIE
14.	Kontrola aplikacji	<p>Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie,</p>	TAK/NIE

		<p>wysyłanie plików.</p> <p>Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.</p>	
15.	Kontrola WWW	<p>Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p> <p>W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxyavoidance.</p> <p>Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.</p> <p>Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>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.</p> <p>Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.</p>	TAK/NIE
16.	Uwierzytelnianie użytkowników w ramach sesji	<p>System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:</p> <ul style="list-style-type: none"> • Hasła statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Hasła statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Hasła dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. <p>Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</p> <p>Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.</p>	TAK/NIE
17.	Zarządzanie	<p>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.</p> <p>Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.</p> <p>System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.</p> <p>System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p>	TAK/NIE
18.	Logowanie	<p>System musi mieć możliwość logowania do posiadanej aplikacji FortiAnalyzer VM.</p> <p>W ramach logowania system musi zapewniać przekazywanie danych</p>	TAK/NIE

		<p>o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <p>Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.</p> <p>Musi istnieć możliwość logowania do serwera SYSLOG.</p>	
19.	Certyfikaty	<p>Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:</p> <ul style="list-style-type: none"> • ICSA lub EAL4 dla funkcji Firewall. • ICSA lub NSS Labs dla funkcji IPS. • ICSA dla funkcji IPSec VPN. • ICSA dla funkcji SSL VPN. 	TAK/NIE
20.	Serwisy, licencje i gwarancje	<p>W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 36 miesięcy.</p> <p>Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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.</p> <p>W przypadku wymiany urządzenia zamawiający musi mieć możliwość usunięcia i zachowania dysku twardego przed jego odesłaniem do dostawcy bez utraty gwarancji.</p>	TAK/NIE

_____dnia _____2018 roku
(miejscowość)

(podpis Wykonawcy)