Załącznik nr 1

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**Rozbudowa i odnowienie wsparcia serwisowego dla posiadanego przez Zamawiającego systemu bezpieczeństwa opartego na rozwiązaniach firmy Cisco i systemów wspomagających.**

# **Odnowienie usługi serwisowej dla urządzeń Bezpieczeństwa typ I - Cisco ASA 5506-X**

**Oferowany model \* …………………….. Producent \* …………………..**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **L.p.** | **Nazwa urządzenia** | **Numer seryjny** | **Data rozpoczęcia serwisu [dzień-miesiąc-rok]** | **Typ serwisu** |
| **1** | **Cisco ASA 5506** |  Zał do OPZ nr.2 | Z dniem podpisania umowy(na 3 lata) | Zgodnie z ofertą Wykonawcy  |
| **2** | **Inne wymagania** | 1. Wykonawca zapewni serwis gwarancyjny realizowany przez producenta rozwiązania lub Autoryzowanego Dystrybutora producenta wraz z przedłużeniem wymaganych licencji.
2. Wykonawca wyrówna terminy związane z serwisem wszystkich urządzeń do jednej daty zgodnie z ofertą Wykonawcy
3. Wykonawca zapewni dostęp wskazanego personelu Zamawiającego do dedykowanego portalu www producenta urządzenia, na którym będzie możliwe co najmniej pobieranie nowych wersji dedykowanego dla danego urządzenia oprogramowania, pobieranie aktualizacji, patch-y, a także dostęp do bazy wiedzy, przewodników konfiguracyjnych, narzędzi diagnostycznych, oprogramowania wspomagającego itp..
4. Wykonawca zapewni możliwość zgłaszania na stronach www producenta sprzętu problemów eksploatacyjnych związanych z obsługą sprzętu będącego przedmiotem zamówienia.
5. Pakiet serwisowy musi zapewniać bezpośrednie zgłoszenie awarii sprzętu do producenta sprzętu (nie tylko do serwisu Wykonawcy) przez cały okres świadczenia usług serwisowych.
6. Wykonawca w oferowanych pakietach serwisowych producenta zapewni dostęp do pomocy technicznej producenta (drogą telefoniczną, poprzez email lub stronę WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego.
7. Wykonawca zaktualizuje urządzanie do wersji najnowszej rekomendowanej przez producenta rozwiązania.
8. Wykonawca dostarczy w terminie 60 dni od dnia podpisania umowy dokument potwierdzający zarejestrowanie kontraktu serwisowego oraz dokument potwierdzający bezpośredni dostęp Zamawiającego do pomocy technicznej producenta oraz do zasobów pobierania oprogramowania do urządzeń objętych serwisem, wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela.
9. Wykonawca przekształci obecnie posiadane licencje na licencje Cisco Smart Account i dołączy do posiadanego przez Zamawiającego systemu Cisco Smart Software Manager (CSSM)
 |
| **3** | **Szkolenia** | Wykonawca dostarczy kredyty szkoleniowe w wysokości 500 tokenów szkoleniowych z programu „Cisco Learning Credits Program” ważne przez okres co najmniej 18 miesięcy do wykorzystania w autoryzowanym ośrodku szkoleniowym na terenie Warszawy. |

Na podstawie art. 25 ust. 1 pkt 2 ustawy i zgodnie z art. 30 ust. 5 ustawy w celu potwierdzenia, że oferowany przedmiot zamówienia odpowiada wymaganiom określonym przez Zamawiającego, Zamawiający żąda złożenia wraz z ofertą **wypełnionej i podpisanej przez Wykonawcę** specyfikacji technicznej dla oferowanych produktów**.**

Zamawiający dopuszcza dostarczenie produktów równoważnych o poniższych parametrach technicznych (wraz z przeniesieniem konfiguracji obecnie eksploatowanych urządzeń Cisco 5506-X)

| **Lp.** | **Opis wymagań minimalnych** |
| --- | --- |
| 1 | Architektura urządzenia | * 1. Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.
	2. Urządzenie wyposażone w:
1. co najmniej sześć interfejsów Gigabit Ethernet 10/100/1000 (RJ45)
2. dedykowany interfejs Gigabit Ethernet 10/100/1000 (RJ45) do zarządzania
	1. Urządzenie posiada dedykowany dla zarządzania port konsoli
	2. Urządzenie posiada zasilacz umożliwiający zasilanie prądem zmiennym 230V
	3. Wydajność na poziomie 300 Mbps w dla testów w warunkach produkcyjnych dla ruchu poddawanego inspekcji przez mechanizmy zapory sieciowej (statefull firewall, ruch TCP)
	4. Przepustowość dla systemu wykrywania ataków IPS musi zapewniać wydajność co najmniej 80Mbps
	5. Urządzenie posiada wydajność co najmniej 50 Mbps dla ruchu szyfrowanego (VPN) w przypadku testów w warunkach laboratoryjnych
	6. Urządzenie umożliwia terminowanie co najmniej 50 jednoczesnych sesji VPN (site-to-site i IPsec client VPN)
	7. Urządzenie obsługuje co najmniej 50.000 jednoczesnych sesji/połączeń z prędkością zestawiania 5.000 połączeń na sekundę.
 |
| 2 | Funkcjonalność urządzenia | * 1. Urządzenie musi działać pod kontrolą dedykowanego systemu operacyjnego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia
	2. Urządzenie musi pełnić funkcję ściany ogniowej śledzącej stan połączeń (tzw. stateful inspection) z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji
	3. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity), integrując się ściśle z usługą katalogową Microsoft Active Directory
	4. Urządzenie musi posiadać możliwość uwierzytelnienia z wykorzystaniem LDAP, NTLM oraz Kerberos
	5. Urządzenie nie może wprowadzać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
	6. Urządzenie pełni funkcję koncentratora VPN umożliwiającego zestawianie połączeń IPSec VPN (zarówno site-to-site, jak i remote access)
	7. Urządzenie musi obsługiwać protokoły IKEv1 i IKEv2.
	8. Urządzenie musi obsługiwać funkcję skrótu SHA-2 o długości co najmniej 256 i 384 bitów.
	9. Urządzenie musi obsługiwać szyfrowanie protokołem AES z kluczem 128, 192 i 256 bitów w trybie pracy Galois/Counter Mode(GCM)
	10. Urządzenie musi obsługiwać protokół Diffiego-Hellmana w przestrzeni krzywych eliptycznych (ECDH) dla grup 19 i 20.
	11. Urządzenie musi posiadać klienta, zapewnianego przez producenta urządzenia i objętego jednolitym wsparciem technicznym dla technologii SSL VPN
	12. Oprogramowanie klienta VPN ma możliwość instalacji na stacjach roboczych pracujących pod kontrolą systemów operacyjnych Windows 7 – wersje 32 i 64-bitowe i umożliwia zestawienie do urządzenia połączeń VPN z komputerów osobistych PC.
	13. Urządzenie musi zapewniać możliwość pracy jako transparentna ściana ogniowa warstwy drugiej ISO/OSI
	14. Urządzenie musi wspierać protokół NTP
	15. Urządzenie musi zapewniać współpracę z zewnętrznymi serwerami CA
	16. Urządzenie musi obsługiwać funkcjonalność Network Address Translation (NAT oraz PAT) – zarówno dla ruchu wchodzącego, jak i wychodzącego
	17. Urządzenie musi wspierać mechanizm translowania adresów sieciowych NAT i translowania adresów i portów PAT w następujących wariantach: z IPv4 na IPv4, NAT64.
	18. Urządzenie musi zapewniać mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby.
	19. Urządzenie musi zapewniać możliwość konfiguracji redundancji na poziomie interfejsów fizycznych urządzenia
	20. Urządzenie musi zapewniać funkcjonalność stateful failover dla ruchu VPN
	21. Urządzenie musi umożliwiać ograniczenie maksymalnej liczby równoczesnych otwartych połączeń TCP i UDP zestawionych do hosta lub do grupy hostów.
	22. Urządzenie musi zapewniać wsparcie stosu protokołów IPv6 w tym:
		1. wspierać inspekcję protokołu IPv6, pracując w trybie transparentnym
		2. wspierać adresację IPv6 interfejsów w scenariuszach wdrożeniowych z wysoką dostępnością (failover)
		3. wspierać realizację połączeń VPN typu site-to-site opartych o minimum IKEv1 z użyciem protokołu IPv6
	23. Urządzenie musi zapewniać obsługę routingu statycznego i dynamicznego (co najmniej dla protokołów RIP, OSPFv2, OSPFv3 i BGP).
	24. Urządzenie musi obsługiwać ruch multicastowy w zakresie wsparcia protokołu PIM, IGMP i definiowania reguł dostępu dla ruchu multicastowego.
	25. Urządzenie musi umożliwiać konfigurację w roli serwera DHCP.
	26. Urządzenie musi umożliwiać funkcję przekazywania zapytań DHCP do zewnętrznego serwera DHCP (DHCP relay).
	27. Urządzenie musi zapewniać konfigurację globalnych reguł filtrowania ruchu, które przykładane są na wszystkie interfejsy urządzenia jednocześnie
	28. Reguły dostępu muszą umożliwiać definiowanie reguł w oparciu o następujące podstawowe parametry:
		1. źródłowy i docelowy adres IPv4
		2. źródłowy i docelowy adres IPv6
		3. źródłowy i docelowy numer portu UDP
		4. źródłowy i docelowy numer portu TCP
		5. nazwy domenowej hosta źródłowego lub docelowego
		6. nazwa użytkownika w usłudze katalogowej Microsoft Active Directory
		7. nazwa grupy w usłudze katalogowej Microsoft Active Directory
		8. czas
		9. protokół i port
		10. aplikacji z uwzględnieniem sygnatury a nie numeru portu
	29. Urządzenie musi mieć możliwość tworzenia reguł firewall, w których warunkiem jest nazwa aplikacji definiowana za pomocą sygnatury.
	30. Urządzenie musi umożliwiać przypisywanie różnych profili ochrony przed złośliwym oprogramowaniem dla różnych aplikacji nawet jeśli pracują na tym samym porcie.
	31. Urządzenie musi umożliwiać tworzenie reguł wykorzystując poziom ryzyka aplikacji
	32. Urządzenie musi umożliwiać tworzenie reguł translacji adresów (NAT) niezależnie od konfiguracji polityki bezpieczeństwa
	33. Urządzenie musi umożliwiać tworzenie reguł QoS niezależnie od konfiguracji polityki bezpieczeństwa
	34. Urządzenie musi zapewniać funkcjonalności tzw, Next-Generation firewall w zakresie nie mniejszym niż:
		1. System automatycznego wykrywania i klasyfikacji aplikacji
		2. System IPS
	35. System wykrywania aplikacji musi:
		1. posiadać możliwość klasyfikacji ruchu i wykrywania co najmniej 3000 aplikacji sieciowych
		2. pozwalać na wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji
		3. umożliwiać administratorowi skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tej aplikacji przez system oraz wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia i w raportach
	36. Urządzenie musi posiadać możliwość rozszyfrowania ruchu SSL w celu przeprowadzenia analizy ruchu pod kątem zagrożeń.
	37. System IPS musi:
		1. posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system)
		2. posiadać możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu)
		3. posiadać możliwość wykrywania i uniemożliwiać rozprzestrzenianie zagrożeń w tym co najmniej:
			1. złośliwe oprogramowanie,
			2. skanowanie sieci,
			3. ataki na usługę VoIP,
			4. próby przepełnienia bufora,
			5. zagrożenia dnia zerowego
			6. posiadać możliwość wykrywania znanych ataków (sygnatury)
			7. zapewniać co najmniej poniższe sposoby wykrywania zagrożeń:
			8. sygnatury ataków opartych na exploitach
			9. reguły oparte na zagrożeniach
			10. mechanizm wykrywania anomalii w protokołach
			11. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego
		4. mieć możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu
		5. posiadać mechanizm minimalizujący liczbę fałszywych alarmów jak i niewykrytych ataków (ang. false positives i false negatives).
		6. mieć możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu zdarzeń
		7. posiadać co najmniej możliwości reakcji na zdarzenia:
			1. tylko monitorowanie,
			2. blokowanie ruchu zawierającego zagrożenia,
			3. zapisywanie pakietów
		8. mieć możliwość detekcji ataków i zagrożeń opartych na protokole IPv6
		9. posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji
		10. zapewniać możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS.
		11. zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne
		12. zapewniać możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP
		13. zapewniać mechanizmy automatyzacji co najmniej w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise)
	38. Urządzenie musi być w stanie utworzyć regułę filtrowania z wieloma kategoriami
	39. Polityka kontroli aplikacji musi być możliwa do zdefiniowania według tożsamości użytkowników
	40. Urządzenie musi posiadać możliwość zaplanowania automatycznego pobierania aktualizacji bazy sygnatur ataków bez ich instalowania. Możliwość zaplanowania o określonej godzinie lub cyklicznie minimum co godzinę, dzień lub tydzień
	41. Urządzenie musi mieć możliwość zaplanowania automatycznego generowania raportów.
	42. Urządzenie musi mieć możliwość tworzenia szablonów raportów.
 |
| 3 | Zarządzanie i konfiguracja | * 1. Urządzenie musi umożliwiać zarządzanie:
1. przez linię poleceń (ang. Command Line Interface) dostępną poprzez bezpośrednie połączenie do portu konsoli urządzenia i dostępną zdalnie przy pomocy protokołów telnet i SSH v2.
2. przez graficzny interfejs użytkownika
3. przez protokół SNMPv3 ze wsparciem dla integralności i poufności komunikacji
	1. Urządzenie musi posiadać dedykowany interfejs do zarządzania,
	2. Urządzenie musi posiadać możliwość definiowania grup administratorów z określeniem uprawnień co do poszczególnych poleceń.
	3. Zdalnie dostępne interfejsy zarządzania muszą być dostępne co najmniej w sieci IPv4.
	4. Urządzenie dla protokołu SSH musi umożliwiać uwierzytelnienie w oparciu nazwę użytkownika i hasło oraz w oparciu o klucz publiczny.
	5. Urządzenie musi umożliwiać ograniczenie dostępu do zdalnie dostępnych interfejsów zarządzania tylko z wybranych adresów IPv4.
	6. Urządzenie musi posiadać możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołu co najmniej RADIUS.
 |

(\*) Należy podać nazwę oferowanego Sprzętu, model i producenta.

# **Odnowienie usługi serwisowej dla urządzenia Urządzenie Bezpieczeństwa Typ II - Cisco ASA 5516-X**

**Oferowany model \* …………………….. Producent \* …………………..**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Nazwa urządzenia** | **Numer seryjny** | **Data rozpoczęcia serwisu [dzień-miesiąc-rok]** | **Typ serwisu** |
| **1** | **Cisco ASA 5516-X** |  Zał do OPZ nr.2 | Z dniem podpisania umowy(na 3 lata) | Zgodnie z ofertą Wykonawcy  |
| **2** | **Inne wymagania** | 1. Wykonawca zapewni serwis pogwarancyjny realizowany przez producenta rozwiązania lub Autoryzowanego Dystrybutora producenta wraz z przedłużeniem wymaganych licencji.
2. Wykonawca wyrówna terminy związane z serwisem wszystkich urządzeń do jednej daty zgodnie z ofertą Wykonawcy
3. Wykonawca zapewni dostęp wskazanego personelu Zamawiającego do dedykowanego portalu www producenta urządzenia, na którym będzie możliwe co najmniej pobieranie nowych wersji dedykowanego dla danego urządzenia oprogramowania, pobieranie aktualizacji, patch-y, a także dostęp do bazy wiedzy, przewodników konfiguracyjnych, narzędzi diagnostycznych, oprogramowania wspomagającego itp..
4. Wykonawca zapewni możliwość zgłaszania na stronach www producenta sprzętu problemów eksploatacyjnych związanych z obsługą sprzętu będącego przedmiotem zamówienia.
5. Zaproponowany pakiet serwisowy musi zapewniać bezpośrednie zgłoszenie awarii sprzętu do producenta sprzętu (nie tylko do serwisu Wykonawcy) przez cały okres świadczenia usług serwisowych.
6. Wykonawca w oferowanych pakietach serwisowych producenta zapewni dostęp do pomocy technicznej producenta (drogą telefoniczną, poprzez email lub stronę WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego.
7. Wykonawca zaktualizuje urządzanie do wersji najnowszej rekomendowanej przez producenta rozwiązania.
8. Wykonawca dostarczy w terminie 60 dni od dnia podpisania umowy dokument potwierdzający zarejestrowanie kontraktu serwisowego oraz dokument potwierdzający bezpośredni dostęp Zamawiającego do pomocy technicznej producenta oraz do zasobów pobierania oprogramowania do urządzeń objętych serwisem, wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela.
9. Wykonawca przekształci obecnie posiadane licencje na licencje Cisco Smart Account i dołączy do posiadanego przez Zamawiającego systemu Cisco Smart Software Manager (CSSM)
 |

Na podstawie art. 25 ust. 1 pkt 2 ustawy i zgodnie z art. 30 ust. 5 ustawy w celu potwierdzenia, że oferowany przedmiot zamówienia odpowiada wymaganiom określonym przez Zamawiającego, Zamawiający żąda złożenia wraz z ofertą **wypełnionej i podpisanej przez Wykonawcę** specyfikacji technicznej dla oferowanych produktów**.**

Zamawiający dopuszcza dostarczenie urządzenia równoważnego spełniającego co najmniej poniższe wymagania techniczne (wraz z przeniesieniem konfiguracji obecnie eksploatowanych urządzeń Cisco ASA 5516-X):

| **Lp.** | **Opis wymagań minimalnych** |
| --- | --- |
| 1 | Architektura urządzenia | * 1. Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.
	2. Urządzenie wyposażone w:
1. co najmniej osiem interfejsów Gigabit Ethernet 10/100/1000 (RJ45)
2. dedykowany interfejs Gigabit Ethernet 10/100/1000 (RJ45) do zarządzania
	1. Urządzenie posiada dedykowany dla zarządzania port konsoli
	2. Urządzenie posiada zasilacz umożliwiający zasilanie prądem zmiennym 230V
	3. Wydajność na poziomie 600 Mbps dla testów w warunkach produkcyjnych dla ruchu poddawanego inspekcji przez mechanizmy zapory sieciowej (statefull firewall, ruch TCP)
	4. Przepustowość dla systemu wykrywania ataków IPS musi zapewniać wydajność co najmniej 200Mbps
	5. Urządzenie posiada wydajność 175 Mbps dla ruchu szyfrowanego (VPN)
	6. Urządzenie umożliwia terminowanie 100 jednoczesnych sesji VPN (site-to-site i IPsec client VPN)
	7. Urządzenie obsługuje co najmniej 100.000 jednoczesnych sesji/połączeń z prędkością zestawiania 10.000 połączeń na sekundę.
 |
| 2 | Funkcjonalność urządzenia | * 1. Urządzenie musi działać pod kontrolą dedykowanego systemu operacyjnego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia
	2. Urządzenie musi pełnić funkcję ściany ogniowej śledzącej stan połączeń (tzw. stateful inspection) z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji
	3. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity), integrując się ściśle z usługą katalogową Microsoft Active Directory
	4. Urządzenie musi posiadać możliwość uwierzytelnienia z wykorzystaniem LDAP, NTLM oraz Kerberos
	5. Urządzenie nie może wprowadzać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
	6. Urządzenie pełni funkcję koncentratora VPN umożliwiającego zestawianie połączeń IPSec VPN (zarówno site-to-site, jak i remote access)
	7. Urządzenie musi obsługiwać protokoły IKEv1 i IKEv2.
	8. Urządzenie musi obsługiwać funkcję skrótu SHA-2 o długości co najmniej 256 i 384 bitów.
	9. Urządzenie musi obsługiwać szyfrowanie protokołem AES z kluczem 128, 192 i 256 bitów w trybie pracy Galois/Counter Mode(GCM)
	10. Urządzenie musi obsługiwać protokół Diffiego-Hellmana w przestrzeni krzywych eliptycznych (ECDH) dla grup 19 i 20.
	11. Urządzenie musi posiadać klienta, zapewnianego przez producenta urządzenia i objętego jednolitym wsparciem technicznym dla technologii SSL VPN
	12. Oprogramowanie klienta VPN ma możliwość instalacji na stacjach roboczych pracujących pod kontrolą systemów operacyjnych Windows 7 – wersje 32 i 64-bitowe i umożliwia zestawienie do urządzenia połączeń VPN z komputerów osobistych PC.
	13. Urządzenie musi zapewniać możliwość pracy jako transparentna ściana ogniowa warstwy drugiej ISO/OSI
	14. Urządzenie musi wspierać protokół NTP
	15. Urządzenie musi zapewniać współpracę z zewnętrznymi serwerami CA
	16. Urządzenie musi obsługiwać funkcjonalność Network Address Translation (NAT oraz PAT) – zarówno dla ruchu wchodzącego, jak i wychodzącego
	17. Urządzenie musi wspierać mechanizm translowania adresów sieciowych NAT i translowania adresów i portów PAT w następujących wariantach: z IPv4 na IPv4, NAT64.
	18. Urządzenie musi zapewniać mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby.
	19. Urządzenie musi zapewniać możliwość konfiguracji redundancji na poziomie interfejsów fizycznych urządzenia
	20. Urządzenie musi zapewniać funkcjonalność stateful failover dla ruchu VPN
	21. Urządzenie musi umożliwiać ograniczenie maksymalnej liczby równoczesnych otwartych połączeń TCP i UDP zestawionych do hosta lub do grupy hostów.
	22. Urządzenie musi zapewniać wsparcie stosu protokołów IPv6 w tym:
		1. wspierać inspekcję protokołu IPv6, pracując w trybie transparentnym
		2. wspierać adresację IPv6 interfejsów w scenariuszach wdrożeniowych z wysoką dostępnością (failover)
		3. wspierać realizację połączeń VPN typu site-to-site opartych o minimum IKEv1 z użyciem protokołu IPv6
	23. Urządzenie musi zapewniać obsługę routingu statycznego i dynamicznego (co najmniej dla protokołów RIP, OSPFv2, OSPFv3 i BGP).
	24. Urządzenie musi obsługiwać ruch multicastowy w zakresie wsparcia protokołu PIM, IGMP i definiowania reguł dostępu dla ruchu multicastowego.
	25. Urządzenie musi umożliwiać konfigurację w roli serwera DHCP.
	26. Urządzenie musi umożliwiać funkcję przekazywania zapytań DHCP do zewnętrznego serwera DHCP (DHCP relay).
	27. Urządzenie musi zapewniać konfigurację globalnych reguł filtrowania ruchu, które przykładane są na wszystkie interfejsy urządzenia jednocześnie
	28. Reguły dostępu muszą umożliwiać definiowanie reguł w oparciu o następujące podstawowe parametry:
		1. źródłowy i docelowy adres IPv4
		2. źródłowy i docelowy adres IPv6
		3. źródłowy i docelowy numer portu UDP
		4. źródłowy i docelowy numer portu TCP
		5. nazwy domenowej hosta źródłowego lub docelowego
		6. nazwa użytkownika w usłudze katalogowej Microsoft Active Directory
		7. nazwa grupy w usłudze katalogowej Microsoft Active Directory
		8. czas
		9. protokół i port
		10. aplikacji z uwzględnieniem sygnatury a nie numeru portu
	29. Urządzenie musi mieć możliwość tworzenia reguł firewall, w których warunkiem jest nazwa aplikacji definiowana za pomocą sygnatury.
	30. Urządzenie musi umożliwiać przypisywanie różnych profili ochrony przed złośliwym oprogramowaniem dla różnych aplikacji nawet jeśli pracują na tym samym porcie.
	31. Urządzenie musi umożliwiać tworzenie reguł wykorzystując poziom ryzyka aplikacji
	32. Urządzenie musi umożliwiać tworzenie reguł translacji adresów (NAT) niezależnie od konfiguracji polityki bezpieczeństwa
	33. Urządzenie musi umożliwiać tworzenie reguł QoS niezależnie od konfiguracji polityki bezpieczeństwa
	34. Urządzenie musi zapewniać funkcjonalności tzw, Next-Generation firewall w zakresie nie mniejszym niż:
		1. System automatycznego wykrywania i klasyfikacji aplikacji
		2. System IPS
	35. System wykrywania aplikacji musi:
		1. posiadać możliwość klasyfikacji ruchu i wykrywania co najmniej 3000 aplikacji sieciowych
		2. pozwalać na wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji
		3. umożliwiać administratorowi skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tej aplikacji przez system oraz wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia i w raportach
	36. Urządzenie musi posiadać możliwość rozszyfrowania ruchu SSL w celu przeprowadzenia analizy ruchu pod kątem zagrożeń.
	37. System IPS musi:
		1. posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system)
		2. posiadać możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu)
		3. posiadać możliwość wykrywania i uniemożliwiać rozprzestrzenianie zagrożeń w tym co najmniej:
			1. złośliwe oprogramowanie,
			2. skanowanie sieci,
			3. ataki na usługę VoIP,
			4. próby przepełnienia bufora,
			5. zagrożenia dnia zerowego
			6. posiadać możliwość wykrywania znanych ataków (sygnatury)
			7. zapewniać co najmniej poniższe sposoby wykrywania zagrożeń:
			8. sygnatury ataków opartych na exploitach
			9. reguły oparte na zagrożeniach
			10. mechanizm wykrywania anomalii w protokołach
			11. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego
		4. mieć możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu
		5. posiadać mechanizm minimalizujący liczbę fałszywych alarmów jak i niewykrytych ataków (ang. false positives i false negatives).
		6. mieć możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu zdarzeń
		7. posiadać co najmniej możliwości reakcji na zdarzenia:
			1. tylko monitorowanie,
			2. blokowanie ruchu zawierającego zagrożenia,
			3. zapisywanie pakietów
		8. mieć możliwość detekcji ataków i zagrożeń opartych na protokole IPv6
		9. posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji
		10. zapewniać możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS.
		11. zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne
		12. zapewniać możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP
		13. zapewniać mechanizmy automatyzacji co najmniej w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise)
	38. Urządzenie musi być w stanie utworzyć regułę filtrowania z wieloma kategoriami
	39. Polityka kontroli aplikacji musi być możliwa do zdefiniowania według tożsamości użytkowników
	40. Urządzenie musi posiadać możliwość zaplanowania automatycznego pobierania aktualizacji bazy sygnatur ataków bez ich instalowania. Możliwość zaplanowania o określonej godzinie lub cyklicznie minimum co godzinę, dzień lub tydzień
	41. Urządzenie musi mieć możliwość zaplanowania automatycznego generowania raportów.
	42. Urządzenie musi mieć możliwość tworzenia szablonów raportów.
 |
| 3 | Zarządzanie i konfiguracja | * 1. Urządzenie musi umożliwiać zarządzanie:
1. przez linię poleceń (ang. Command Line Interface) dostępną poprzez bezpośrednie połączenie do portu konsoli urządzenia i dostępną zdalnie przy pomocy protokołów telnet i SSH v2.
2. przez graficzny interfejs użytkownika
3. przez protokół SNMPv3 ze wsparciem dla integralności i poufności komunikacji
	1. Urządzenie musi posiadać dedykowany interfejs do zarządzania,
	2. Urządzenie musi posiadać możliwość definiowania grup administratorów z określeniem uprawnień co do poszczególnych poleceń.
	3. Zdalnie dostępne interfejsy zarządzania muszą być dostępne co najmniej w sieci IPv4.
	4. Urządzenie dla protokołu SSH musi umożliwiać uwierzytelnienie w oparciu nazwę użytkownika i hasło oraz w oparciu o klucz publiczny.
	5. Urządzenie musi umożliwiać ograniczenie dostępu do zdalnie dostępnych interfejsów zarządzania tylko z wybranych adresów IPv4.
	6. Urządzenie musi posiadać możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołu co najmniej RADIUS.
 |

 (\*) Należy podać nazwę oferowanego Sprzętu, model i producenta.

# **Odnowienie usługi serwisowej dla urządzeń bezpieczeństwa Typ III - Cisco ASA 5545 -X**

**Oferowany model \* …………………….. Producent \* …………………..**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Nazwa urządzenia posiadanego przez Zamawiającego** | **Numer seryjny** | **Data rozpoczęcia serwisu [dzień-miesiąc-rok]** | **Typ serwisu** |
| **1** | **Cisco ASA 5545 -X** |  Zał do OPZ nr.2 | Z dniem podpisania umowy(na 3 lata) | Zgodnie z ofertą Wykonawcy  |
| **2** | **Inne wymagania** | 1. Wykonawca zapewni serwis pogwarancyjny realizowany przez producenta rozwiązania lub Autoryzowanego Dystrybutora producenta wraz z przedłużeniem wymaganych licencji
2. Wykonawca wyrówna terminy związane z serwisem wszystkich urządzeń do jednej daty zgodnie z ofertą Wykonawcy
3. Wykonawca zapewni dostęp wskazanego personelu Zamawiającego do dedykowanego portalu www producenta urządzenia, na którym będzie możliwe co najmniej pobieranie nowych wersji dedykowanego dla danego urządzenia oprogramowania, pobieranie aktualizacji, patch-y, a także dostęp do bazy wiedzy, przewodników konfiguracyjnych, narzędzi diagnostycznych, oprogramowania wspomagającego itp..
4. Wykonawca zapewni możliwość zgłaszania na stronach www producenta sprzętu problemów eksploatacyjnych związanych z obsługą sprzętu będącego przedmiotem zamówienia.
5. Zaproponowany pakiet serwisowy musi zapewniać bezpośrednie zgłoszenie awarii sprzętu do producenta sprzętu (nie tylko do serwisu Wykonawcy) przez cały okres świadczenia usług serwisowych.
6. Wykonawca w oferowanych pakietach serwisowych producenta zapewni dostęp do pomocy technicznej producenta (drogą telefoniczną, poprzez email lub stronę WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego.
7. Wykonawca zaktualizuje urządzanie do wersji najnowszej rekomendowanej przez producenta rozwiązania.
8. Wykonawca dostarczy w terminie 60 dni od dnia podpisania umowy dokument potwierdzający zarejestrowanie kontraktu serwisowego oraz dokument potwierdzający bezpośredni dostęp Zamawiającego do pomocy technicznej producenta oraz do zasobów pobierania oprogramowania do urządzeń objętych serwisem, wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela.
9. Wykonawca przekształci obecnie posiadane licencje na licencje Cisco Smart Account i dołączy do posiadanego przez Zamawiającego systemu Cisco Smart Software Manager (CSSM)
 |

Na podstawie art. 25 ust. 1 pkt 2 ustawy i zgodnie z art. 30 ust. 5 ustawy w celu potwierdzenia, że oferowany przedmiot zamówienia odpowiada wymaganiom określonym przez Zamawiającego, Zamawiający żąda złożenia wraz z ofertą **wypełnionej i podpisanej przez Wykonawcę** specyfikacji technicznej dla oferowanych produktów**.**

Zamawiający dopuszcza dostarczenie urządzenia równoważnego spełniającego co najmniej poniższe wymagania techniczne (wraz z przeniesieniem konfiguracji obecnie eksploatowanych urządzeń Cisco ASA 5545 -X):

lub rozwiązanie równoważne o poniższych parametrach:

| **Lp.** | **Opis wymagań minimalnych** |
| --- | --- |
| 1 | Architektura urządzenia | * 1. Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.
	2. Urządzenie wyposażone w:
1. co najmniej sześć interfejsów Gigabit Ethernet 10/100/1000 (RJ45)
2. dedykowany interfejs Gigabit Ethernet 10/100/1000 (RJ45) do zarządzania
	1. Urządzenie posiada dedykowany dla zarządzania port konsoli
	2. Urządzenie posiada zasilacz umożliwiający zasilanie prądem zmiennym 230V
	3. Wydajność na poziomie 1,5 Gbps dla testów w warunkach produkcyjnych dla ruchu poddawanego inspekcji przez mechanizmy zapory sieciowej (statefull firewall, ruch TCP)
	4. Przepustowość dla systemu wykrywania ataków IPS musi zapewniać wydajność co najmniej 450Mbps dla testów w warunkach laboratoryjnych
	5. Urządzenie posiada wydajność 250 Mbps dla ruchu szyfrowanego (VPN) dla testów w warunkach laboratoryjnych
	6. Urządzenie umożliwia terminowanie 300 jednoczesnych sesji VPN (site-to-site i IPsec client VPN)
	7. Urządzenie obsługuje co najmniej 250.000 jednoczesnych sesji/połączeń z prędkością zestawiania 20.000 połączeń na sekundę.
 |
| 2 | Funkcjonalność urządzenia | * 1. Urządzenie musi działać pod kontrolą dedykowanego systemu operacyjnego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia
	2. Urządzenie musi pełnić funkcję ściany ogniowej śledzącej stan połączeń (tzw. stateful inspection) z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji
	3. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity), integrując się ściśle z usługą katalogową Microsoft Active Directory
	4. Urządzenie musi posiadać możliwość uwierzytelnienia z wykorzystaniem LDAP, NTLM oraz Kerberos
	5. Urządzenie nie może wprowadzać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
	6. Urządzenie pełni funkcję koncentratora VPN umożliwiającego zestawianie połączeń IPSec VPN (zarówno site-to-site, jak i remote access)
	7. Urządzenie musi obsługiwać protokoły IKEv1 i IKEv2.
	8. Urządzenie musi obsługiwać funkcję skrótu SHA-2 o długości co najmniej 256 i 384 bitów.
	9. Urządzenie musi obsługiwać szyfrowanie protokołem AES z kluczem 128, 192 i 256 bitów w trybie pracy Galois/Counter Mode(GCM)
	10. Urządzenie musi obsługiwać protokół Diffiego-Hellmana w przestrzeni krzywych eliptycznych (ECDH) dla grup 19 i 20.
	11. Urządzenie musi posiadać klienta, zapewnianego przez producenta urządzenia i objętego jednolitym wsparciem technicznym dla technologii SSL VPN
	12. Oprogramowanie klienta VPN ma możliwość instalacji na stacjach roboczych pracujących pod kontrolą systemów operacyjnych Windows 7 – wersje 32 i 64-bitowe i umożliwia zestawienie do urządzenia połączeń VPN z komputerów osobistych PC.
	13. Urządzenie musi zapewniać możliwość pracy jako transparentna ściana ogniowa warstwy drugiej ISO/OSI
	14. Urządzenie musi wspierać protokół NTP
	15. Urządzenie musi zapewniać współpracę z zewnętrznymi serwerami CA
	16. Urządzenie musi obsługiwać funkcjonalność Network Address Translation (NAT oraz PAT) – zarówno dla ruchu wchodzącego, jak i wychodzącego
	17. Urządzenie musi wspierać mechanizm translowania adresów sieciowych NAT i translowania adresów i portów PAT w następujących wariantach: z IPv4 na IPv4, NAT64.
	18. Urządzenie musi zapewniać mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby.
	19. Urządzenie musi zapewniać możliwość konfiguracji redundancji na poziomie interfejsów fizycznych urządzenia
	20. Urządzenie musi zapewniać funkcjonalność stateful failover dla ruchu VPN
	21. Urządzenie musi umożliwiać ograniczenie maksymalnej liczby równoczesnych otwartych połączeń TCP i UDP zestawionych do hosta lub do grupy hostów.
	22. Urządzenie musi zapewniać wsparcie stosu protokołów IPv6 w tym:
		1. wspierać inspekcję protokołu IPv6, pracując w trybie transparentnym
		2. wspierać adresację IPv6 interfejsów w scenariuszach wdrożeniowych z wysoką dostępnością (failover)
		3. wspierać realizację połączeń VPN typu site-to-site opartych o minimum IKEv1 z użyciem protokołu IPv6
	23. Urządzenie musi zapewniać obsługę routingu statycznego i dynamicznego (co najmniej dla protokołów RIP, OSPFv2, OSPFv3 i BGP).
	24. Urządzenie musi obsługiwać ruch multicastowy w zakresie wsparcia protokołu PIM, IGMP i definiowania reguł dostępu dla ruchu multicastowego.
	25. Urządzenie musi umożliwiać konfigurację w roli serwera DHCP.
	26. Urządzenie musi umożliwiać funkcję przekazywania zapytań DHCP do zewnętrznego serwera DHCP (DHCP relay).
	27. Urządzenie musi zapewniać konfigurację globalnych reguł filtrowania ruchu, które przykładane są na wszystkie interfejsy urządzenia jednocześnie
	28. Reguły dostępu muszą umożliwiać definiowanie reguł w oparciu o następujące podstawowe parametry:
		1. źródłowy i docelowy adres IPv4
		2. źródłowy i docelowy adres IPv6
		3. źródłowy i docelowy numer portu UDP
		4. źródłowy i docelowy numer portu TCP
		5. nazwy domenowej hosta źródłowego lub docelowego
		6. nazwa użytkownika w usłudze katalogowej Microsoft Active Directory
		7. nazwa grupy w usłudze katalogowej Microsoft Active Directory
		8. czas
		9. protokół i port
		10. aplikacji z uwzględnieniem sygnatury a nie numeru portu
	29. Urządzenie musi mieć możliwość tworzenia reguł firewall, w których warunkiem jest nazwa aplikacji definiowana za pomocą sygnatury.
	30. Urządzenie musi umożliwiać przypisywanie różnych profili ochrony przed złośliwym oprogramowaniem dla różnych aplikacji nawet jeśli pracują na tym samym porcie.
	31. Urządzenie musi umożliwiać tworzenie reguł wykorzystując poziom ryzyka aplikacji
	32. Urządzenie musi umożliwiać tworzenie reguł translacji adresów (NAT) niezależnie od konfiguracji polityki bezpieczeństwa
	33. Urządzenie musi umożliwiać tworzenie reguł QoS niezależnie od konfiguracji polityki bezpieczeństwa
	34. Urządzenie musi zapewniać funkcjonalności tzw, Next-Generation firewall w zakresie nie mniejszym niż:
		1. System automatycznego wykrywania i klasyfikacji aplikacji
		2. System IPS
	35. System wykrywania aplikacji musi:
		1. posiadać możliwość klasyfikacji ruchu i wykrywania co najmniej 3000 aplikacji sieciowych
		2. pozwalać na wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji
		3. umożliwiać administratorowi skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tej aplikacji przez system oraz wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia i w raportach
	36. Urządzenie musi posiadać możliwość rozszyfrowania ruchu SSL w celu przeprowadzenia analizy ruchu pod kątem zagrożeń.
	37. System IPS musi:
		1. posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system)
		2. posiadać możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu)
		3. posiadać możliwość wykrywania i uniemożliwiać rozprzestrzenianie zagrożeń w tym co najmniej:
			1. złośliwe oprogramowanie,
			2. skanowanie sieci,
			3. ataki na usługę VoIP,
			4. próby przepełnienia bufora,
			5. zagrożenia dnia zerowego
			6. posiadać możliwość wykrywania znanych ataków (sygnatury)
			7. zapewniać co najmniej poniższe sposoby wykrywania zagrożeń:
			8. sygnatury ataków opartych na exploitach
			9. reguły oparte na zagrożeniach
			10. mechanizm wykrywania anomalii w protokołach
			11. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego
		4. mieć możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu
		5. posiadać mechanizm minimalizujący liczbę fałszywych alarmów jak i niewykrytych ataków (ang. false positives i false negatives).
		6. mieć możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu zdarzeń
		7. posiadać co najmniej możliwości reakcji na zdarzenia:
			1. tylko monitorowanie,
			2. blokowanie ruchu zawierającego zagrożenia,
			3. zapisywanie pakietów
		8. mieć możliwość detekcji ataków i zagrożeń opartych na protokole IPv6
		9. posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji
		10. zapewniać możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS.
		11. zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne
		12. zapewniać możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP
		13. zapewniać mechanizmy automatyzacji co najmniej w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise)
	38. Urządzenie musi być w stanie utworzyć regułę filtrowania z wieloma kategoriami
	39. Polityka kontroli aplikacji musi być możliwa do zdefiniowania według tożsamości użytkowników
	40. Urządzenie musi posiadać możliwość zaplanowania automatycznego pobierania aktualizacji bazy sygnatur ataków bez ich instalowania. Możliwość zaplanowania o określonej godzinie lub cyklicznie minimum co godzinę, dzień lub tydzień
	41. Urządzenie musi mieć możliwość zaplanowania automatycznego generowania raportów.
	42. Urządzenie musi mieć możliwość tworzenia szablonów raportów.
 |
| 3 | Zarządzanie i konfiguracja | * 1. Urządzenie musi umożliwiać zarządzanie:
1. przez linię poleceń (ang. Command Line Interface) dostępną poprzez bezpośrednie połączenie do portu konsoli urządzenia i dostępną zdalnie przy pomocy protokołów telnet i SSH v2.
2. przez graficzny interfejs użytkownika
3. przez protokół SNMPv3 ze wsparciem dla integralności i poufności komunikacji
	1. Urządzenie musi posiadać dedykowany interfejs do zarządzania,
	2. Urządzenie musi posiadać możliwość definiowania grup administratorów z określeniem uprawnień co do poszczególnych poleceń.
	3. Zdalnie dostępne interfejsy zarządzania muszą być dostępne co najmniej w sieci IPv4.
	4. Urządzenie dla protokołu SSH musi umożliwiać uwierzytelnienie w oparciu nazwę użytkownika i hasło oraz w oparciu o klucz publiczny.
	5. Urządzenie musi umożliwiać ograniczenie dostępu do zdalnie dostępnych interfejsów zarządzania tylko z wybranych adresów IPv4.
	6. Urządzenie musi posiadać możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołu co najmniej RADIUS.
 |

(\*) Należy podać nazwę oferowanego Sprzętu, model i producenta.

# **Rozbudowa posiadanego rozwiązania Cisco Firepower Management Center 4000 Chassis**

**Oferowany model \* …………………….. Producent \* …………………..**

Obecnie wykorzystywane przez Zamawiającego rozwiązanie Cisco Firepower Management Center 4000 służące do zarządzania siecią, składające się z urządzeń Cisco należy rozbudować o drugie takie samo urządzenie tak aby zbudować klaster niezawodnościowy. Obecna konfiguracja musi zostać przeniesiona na nowopowstały klaster urządzeń. W przypadku wycofania obecnie wykorzystywanego modelu urządzenia ze sprzedaży, należy dostarczyć rozwiązanie równoważne o poniższych parametrach.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Nazwa urządzenia posiadanego przez Zamawiającego** | **Numer seryjny** | **Data rozpoczęcia serwisu [dzień-miesiąc-rok]** | **Typ serwisu** |
| **1** | **Cisco Firepower Management Center 4000** | **FCH2112V3QA** | Z dniem podpisania umowy(na 3 lata) | Zgodnie z ofertą Wykonawcy  |
| **2** | **Inne wymagania** | 1. Wykonawca zapewni serwis pogwarancyjny realizowany przez producenta rozwiązania lub Autoryzowanego Dystrybutora producenta wraz z przedłużeniem wymaganych licencji
2. Wykonawca wyrówna terminy związane z serwisem wszystkich urządzeń do jednej daty zgodnie z ofertą Wykonawcy
3. Wykonawca zapewni dostęp wskazanego personelu Zamawiającego do dedykowanego portalu www producenta urządzenia, na którym będzie możliwe co najmniej pobieranie nowych wersji dedykowanego dla danego urządzenia oprogramowania, pobieranie aktualizacji, patch-y, a także dostęp do bazy wiedzy, przewodników konfiguracyjnych, narzędzi diagnostycznych, oprogramowania wspomagającego itp..
4. Wykonawca zapewni możliwość zgłaszania na stronach www producenta sprzętu problemów eksploatacyjnych związanych z obsługą sprzętu będącego przedmiotem zamówienia.
5. Zaproponowany pakiet serwisowy musi zapewniać bezpośrednie zgłoszenie awarii sprzętu do producenta sprzętu (nie tylko do serwisu Wykonawcy) przez cały okres świadczenia usług serwisowych.
6. Wykonawca w oferowanych pakietach serwisowych producenta zapewni dostęp do pomocy technicznej producenta (drogą telefoniczną, poprzez email lub stronę WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego.
7. Wykonawca zaktualizuje urządzanie do wersji najnowszej rekomendowanej przez producenta rozwiązania.
8. Wykonawca dostarczy w terminie 60 dni od dnia podpisania umowy dokument potwierdzający zarejestrowanie kontraktu serwisowego oraz dokument potwierdzający bezpośredni dostęp Zamawiającego do pomocy technicznej producenta oraz do zasobów pobierania oprogramowania do urządzeń objętych serwisem, wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela.
9. Wykonawca przekształci obecnie posiadane licencje na licencje Cisco Smart Account i dołączy do posiadanego przez Zamawiającego systemu Cisco Smart Software Manager (CSSM)
 |

Zamawiający dopuszcza dostarczenie urządzenia równoważnego spełniającego co najmniej poniższe wymagania techniczne (wraz z przeniesieniem konfiguracji obecnie eksploatowanych urządzeń Cisco Firepower Management Center 4000):

|  |  |
| --- | --- |
| **Platforma zarządzania** | 1. Platforma zarządzania musi składać się z dwóch identycznych urządzeń tworzący klaster HA.
2. Platforma zarządzania musi umożliwiać zarządzanie obecnymi w sieci Zamawiającego modułami Cisco FirePower uruchomionymi na urządzenia Cisco ASA typ I,II,III
3. Dedykowana platforma zarządzająca oparta na dedykowanym, uodpornionym (ang. hardened) systemie operacyjnym.
4. Platforma zarządzająca musi mieć formę maszyny fizycznej 1RU wyposażonej w:

- Dwa interfejsy RJ45 1Gbps- Dwa interfejsy SFP+ 10Gbps- 128GB RAM- dwa interfejsy USB 3.0 Typu A- 3,2 TB przestrzeni dyskowej |
| **Platforma zarządzania spełnia następujące wymagania** | 1. Każde z urządzeń musi być wyposażone w dwa redundantne zasilacze w technologii Hot-swappable
2. Możliwość obsługi 300 milionów zdarzeń systemu IPS
3. Zarządzanie do 750 sensorami bezpieczeństwa producenta platformy zarządzania.
4. Umożliwia integracje z systemem ochrony stacji końcowej producenta platformy zarządzania w celu agregowania zdarzeń bezpieczeństwa z obu systemów.
5. Umożliwia agregację wszystkich zdarzeń IDS/IPS oraz centralne monitorowanie i analizę działającą w czasie rzeczywistym
6. Jest dostępna przez interfejs WEB, bez potrzeby instalacji dodatkowego oprogramowania klienckiego
7. Zapewnia interfejs, który może zostać dostosowany do wymagań użytkownika, w szczególności administrator posiada możliwość definiowania widoków (dashboard), które spełniają jego indywidualne kryteria
8. Ma możliwość konfigurowania limitu powtórzeń danego zdarzenia w określonym czasie zanim zostanie wygenerowany alarm
9. Ma możliwość automatycznej konfiguracji pobierania zestawów sygnatur na najnowsze zagrożenia i podatności. Ma możliwość informowania o zmianach w pakietach z nowymi sygnaturami/regułami
10. Zapewnia zarządzanie oparte o role, gdzie każdy z użytkowników systemu może mieć różne widoki interfejsu oraz różne możliwości konfiguracyjne w zależności od roli, do której został przypisany
11. Zapewnia funkcjonalność typu harmonogram zadań umożliwiającą automatyczne uruchamianie rutynowych czynności administracyjnych takich jak kopie zapasowe, uaktualnienia, tworzenie raportów, stosowanie polityk bezpieczeństwa oraz automatyczne dostrajanie polityki IPS
12. Zapewnia grupowanie urządzeń i polityk w celu ułatwienia zarządzania konfiguracją
13. Ma możliwość przechowywania atrybutów hostów definiowanych przez użytkownika takich jak jego krytyczność tak, aby ułatwić czynności monitorowania sieci
14. Daje możliwość znaczącej redukcji nakładów operacyjnych oraz przyśpieszenie reakcji na zagrożenia poprzez automatyczną priorytetyzację alarmów w oparciu o korelację zagrożeń ze skutecznością ataku na docelowego hosta
15. Ma możliwość dynamicznego dostrajania systemu IDS/IPS przy zachowaniu minimalnej interwencji administratora
16. Zapewnia możliwość automatycznego uaktualniania reguł publikowanych przez producenta, automatyczną dystrybucję i stosowanie reguł na urządzeniach IPS
17. Ma możliwość wykonywania i odtwarzania kopi zapasowych zarówno urządzeń bezpieczeństwa, jak i platformy zarządzającej
18. Zapewnia funkcjonalność pozwalającą na zarządzanie cyklem życia incydentu, od początkowego powiadomienia, poprzez odpowiedzi, aż do rozwiązania
19. Zapewnia możliwość wglądu w reguły, które wygenerowały dany incydent oraz powiązanego z nim pakietu
20. Zapewnia możliwość synchronizowania czasu pomiędzy wszystkimi komponentami przez protokół NTP
21. Zapewnia możliwość logowania wszystkich czynności wykonywanych przez administratora zarówno lokalnie jak i na zdalnym serwerze
22. Zapewnia szerokie możliwości generowania raportów włączając w to raporty predefiniowane oraz możliwość kompletnego dostosowania raportów do wymagań użytkownika
23. Zapewnia informowanie o zagrożeniach poprzez:
24. Wysłanie e-maila,
25. Wysłanie trap SNMP,
26. Przesłanie informacji do serwera Syslog,
27. Uruchomienie skryptu użytkownika
28. Wysłanie informacji do jednego lub kilku rozwiązań typu SIEM poprzez zaszyfrowane łącze
29. Posiada zaawansowany system przeszukiwania logów pozwalający na przeprowadzanie analizy:
30. Aktualnego stanu danego urządzenia,
31. Podglądu historii dostępnych zasobów,
32. Możliwość eliminacji powtarzających się alarmów (tzw. Black Listing)
33. Ma możliwość ustanawiania i wymuszania polityki zgodności jak i alarmowania w przypadku jej naruszeń w czasie rzeczywistym
34. Ma możliwość przypisywania następujących parametrów w polityce kontroli dostępu dla danych interfejsów, podsieci, vlanów i użytkowników:
35. Dozwolone porty i protokoły
36. Dozwolone aplikacje według różnych kategorii
37. Dozwolone kategorie stron internetowych (URL filtering)
38. Dedykowaną politykę wykrywania zagrożeń IPS dla każdej z reguł zapory ogniowej
39. Sposób traktowania wyspecyfikowanego ruchu w danej regule: przepuszczanie bez analizy, analiza, blokowanie ciche, blokowanie z resetowaniem sesji, blokowanie interaktywne
40. W ramach funkcji kategoryzacji zapytań HTTP (URL filtering) rozwiązanie ma możliwość interaktywnego blokowania z resetowaniem zapytań. W ramach tej funkcji jest zapewniona możliwość zdefiniowania własnej strony internetowej ostrzegającej o naruszeniu polityki kontroli dostępu i zrzuceniu zablokowanej próby połączenia
 |

(\*) Należy podać nazwę oferowanego oprogramowania, numer wersji i producenta.

# **Odnowienie usługi serwisowej i licencji dla Cisco Security Manager**

Wykonawca przedłuży licencję i support na rozwiązanie Cisco Security Manager na okres 3 lat . Zamawiający posiada obecnie zainstalowane rozwiązanie w wersji **4.2.2**

# **Oferowane oprogramowanie \* …………………….. Producent \* …………………..**

|  |  |
| --- | --- |
| **Oprogramowanie** | 1. Wykonawca zapewni odnowienie licencji i supportu przez producenta rozwiązania lub Autoryzowanego Dystrybutora producenta wraz z przedłużeniem wymaganych licencji
2. Wykonawca wyrówna terminy związane z serwisem i licencjami
3. Wykonawca zapewni dostęp wskazanego personelu Zamawiającego do dedykowanego portalu www producenta oprogramowania, na którym będzie możliwe co najmniej pobieranie nowych wersji dedykowanego dla danego urządzenia oprogramowania, pobieranie aktualizacji, patch-y, a także dostęp do bazy wiedzy, przewodników konfiguracyjnych, narzędzi diagnostycznych, oprogramowania wspomagającego itp..
4. Wykonawca zapewni możliwość zgłaszania na stronach www producenta oprogramowania problemów eksploatacyjnych związanych z obsługą sprzętu będącego przedmiotem zamówienia.
5. Zaproponowany pakiet serwisowy musi zapewniać bezpośrednie zgłoszenie awarii oprogramowania do producenta oprogramowania (nie tylko do serwisu Wykonawcy) przez cały okres świadczenia usług serwisowych.
6. Wykonawca w oferowanych pakietach serwisowych producenta zapewni dostęp do pomocy technicznej producenta (drogą telefoniczną, poprzez email lub stronę WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego.
7. Wykonawca zaktualizuje oprogramowanie do wersji najnowszej rekomendowanej przez producenta rozwiązania.
8. Wykonawca dostarczy w terminie 60 dni od dnia podpisania umowy dokument potwierdzający zarejestrowanie kontraktu serwisowego oraz dokument potwierdzający bezpośredni dostęp Zamawiającego do pomocy technicznej producenta oraz do zasobów pobierania oprogramowania do urządzeń objętych serwisem, wystawiony przez producenta oprogramowania lub jego oficjalnego przedstawiciela.
9. Wykonawca przekształci obecnie posiadane licencje na licencje Cisco Smart Account i dołączy do posiadanego przez Zamawiającego systemu Cisco Smart Software Manager (CSSM)
 |

(\*) Należy podać nazwę oferowanego oprogramowania, numer wersji i producenta

Zamawiający dopuszcza dostarczenie oprogramowania równoważnego spełniającego co najmniej poniższe wymagania techniczne (wraz z przeniesieniem konfiguracji obecnie eksploatowanych oprogramowania Cisco Security Manager ):

|  |  |
| --- | --- |
| Architektura  | 1. Dostarczone rozwiązanie musi być w postaci dedykowanego urządzenia (applaiance) lub w postaci oprogramowania.
2. W przypadku dostarczenia systemu zarządzania w postaci oprogramowania, Wykonawca dostarczy kompleksowo niezbędne środowisko do jego uruchomienia (licencje na system operacyjny, licencje na oprogramowanie bazy danych, licencje na oprogramowanie wirtualizacyjne itp. ) w tym fizyczny serwer w obudowie Rack z redundantnymi zasilaczami i wentylatorami o parametrach nie gorszych niż:
	1. 2 procesory 8-rdzeniowe o taktowaniu co najmniej 2,5 GHz
	2. co najmniej 8 TB HDD skonfigurowane w RAID 5 dostępne dla Zamawiającego po uruchomieniu systemu centralnego zarządzania pod przyszłe potrzeby związane z działaniem systemu centralnego zarządzania
	3. 256 GB pamięci RAM
3. Serwer musi się znajdować na liście kompatybilności sprzętu producenta centralnego systemu zarządzania
4. Rozwiązanie dostarczone w postaci dedykowanego applaiance powinno mieć parametry fizyczne nie gorsze niż wyspecyfikowane w pkt 2.
 |
| Funkcjonalności | 1. Rozwiązanie bezagentowe (brak dodatkowego oprogramowania agenta na urządzeniach),
2. Rozwiązanie dostarczone z licencją na obsługę minimum 500 urządzeń,
3. Rozwiązanie musi umożliwiać grupowanie urządzeń, automatyczne wykonywanie zaplanowanych zadań, informowanie o zmianach w konfiguracji, możliwość wersjonowania konfiguracji danego urządzenia wraz z wyróżnionymi zmianami, możliwość przywracania wcześniejszej konfiguracji,
4. Rozwiązanie musi umożliwiać tworzenie obiektów konfiguracyjnych tj. musi umożliwiać grupowanie szeregu komend konfiguracyjnych w jeden obiekt, którego przypisanie do urządzenia spowoduje wprowadzenie predefiniowanej konfiguracji,
5. Rozwiązanie musi zapewniać mechanizmy porównywania dwóch różnych konfiguracji tego samego urządzenia,
6. Rozwiązanie musi zapewniać mechanizmy analizy reguł bezpieczeństwa,
7. Rozwiązanie musi posiadać mechanizm weryfikacji polityki bezpieczeństwa przed instalacją polityki.
8. Rozwiązanie musi posiadać mechanizm kontroli zmian polityki bezpieczeństwa.
9. Rozwiązanie musi zawierać możliwość wykorzystania zewnętrznych jednostek certyfikacyjnych, obsługującą standard co najmniej PKCS#12,
10. Rozwiązanie musi zapewniać mechanizmy współdzielenia polityki bezpieczeństwa tzn. raz zdefiniowana polityka bezpieczeństwa musi mieć możliwość przypisania do wielu urządzeń. Nie dopuszcza się systemów gdzie konieczna będzie powtórna konfiguracja polityki per każde z urządzeń
11. Rozwiązanie musi zapewniać narzędzia workflow w zakresie:
12. tworzenia, edycji i zatwierdzania polityki bezpieczeństwa,
13. generowania, zatwierdzania oraz wdrażania działań związanych z zatwierdzoną polityką bezpieczeństwa,
14. Rozwiązanie musi zapewniać dostęp administracyjny w trybie Role-based Access Control,
15. Rozwiązanie musi umożliwiać tworzenie archiwów konfiguracji dla poszczególnych urządzeń,
16. Rozwiązanie musi umożliwiać zarządzanie i monitoring Urządzeń w zakresie nie mniejszym niż:
17. jedna wspólna tablica reguł dla wszystkich zarządzanych urządzeń,
18. możliwość tworzenia zapytań dotyczących reguł - tzn. możliwość przeszukania tablicy zdefiniowanych reguł pod kątem sprawdzenia czy znajdują się w niej wpisy dotyczące wskazanego ruchu (źródło, cel, port usługi itp.),
19. możliwość wykrywania konfliktów w regułach skonfigurowanych na różnych urządzeniach,
20. możliwość wykrywania powtarzających się reguł i nakładających się reguł w tablicach celem optymalizacji tablic reguł,
21. możliwość współdzielenia i dziedziczenia polityk bezpieczeństwa,
22. możliwość wymuszenia obligatoryjnego i automatycznego dziedziczenia podstawowych ustawień konfiguracyjnych dla nowych urządzeń w sieci,
23. możliwość sprawdzania liczników dla poszczególnych reguł celem sprawdzenia czy reguła funkcjonuje poprawnie,
24. możliwość definiowania reguł AAA,
25. możliwość konfiguracji mechanizmów QoS na zarządzanych urządzeniach,
26. możliwość konfiguracji list kontroli dostępu (ACL) z restrykcjami czasowymi,
27. możliwość konfiguracji NAT na urządzeniach,
28. możliwość konfiguracji routingu na zarządzanych urządzeniach,
29. możliwość definiowania usług zarządzania np. SNMP dla zarządzanych platform,
30. możliwość definiowania i konfiguracji usług sieciowych np. DHCP, sieci VLAN itp.,
31. możliwość uruchamiania i blokowania reguł na wskazanych urządzeniach,
32. możliwość tworzenia sieci VPN z wykorzystaniem kreatorów dla sieci:
33. Site-to-site VPN
34. Remote Acess VPN
35. możliwość dostosowywania poszczególnych parametrów sieci VPN dla pojedynczego urządzenia i grupy urządzeń,
36. możliwość wizualizacji sieci VPN na mapie topologicznej,
37. informowanie o zasobach systemów takich jak obciążenie procesora, aktywnych tunelach i sesjach VPN,
38. możliwość zarządzania i wprowadzania zmian konfiguracyjnych i update'ów image oprogramowania do wielu Urządzeń,
39. Rozwiązanie musi umożliwiać zarządzanie i monitoring urządzeń IDS/IPS w zakresie nie mniejszym niż:
40. możliwość zarządzania różnymi typami sond,
41. możliwość zarządzania wieloma sondami z jednej konsoli,
42. możliwość tworzenia hierarchii sond z opcją dziedziczenia polityki,
43. możliwość automatycznego uaktualniania oprogramowania sond w tym oprogramowania systemowego oraz bazy danych sygnatur,
44. możliwość monitoringu stanu sondy,
45. możliwość wprowadzania zmian rozłożonych w czasie,
46. możliwość zarządzania pojedynczą sondą co najmniej w zakresie:
47. dodania/usunięcia z systemu,
48. restartu,
49. przypisania do grupy,
50. przypisania konfiguracji dziedziczonej,
51. obserwacji statystyk.
52. zarządzania certyfikatami (jeżeli są dostępne)
53. możliwość globalnej konfiguracji dla całości zarządzanego systemu co najmniej następujących parametrów:
54. sygnatury,
55. sygnatury własne - konfigurowane przez administratora,
56. reakcje na zdarzenia,
57. SNMP,
58. NTP,
59. możliwość zarządzania sygnaturami dla urządzeń podległych w zakresie co najmniej:
60. edytowania,
61. strojenia (Tunning),
62. aktywacji/deaktywacji reakcji na zdarzenia,
63. kopiowania,
64. zbieranie informacji o zaistniałych atakach sieciowych oraz ich grupowanie,
65. System zarządzania umożliwia integrację z usługą katalogową LDAP, w szczególności z Microsoft Active Directory. Integracja ma co najmniej polegać na możliwości zaimportowania grup użytkowników z LDAP oraz wykorzystywanie tych grup w regułach polityki bezpieczeństwa.
 |
| Zarządzanie i konfiguracja | 1. Rozwiązanie umożliwiające zalogowanie się do panelu zarządzania z wykorzystaniem protokołu https poprzez przeglądarkę internetową,
2. Rozwiązanie posiadające graficzny interfejs do zarządzania wdrażanymi urządzeniami umożliwiający realizację wszystkich wymaganych funkcjonalności,
3. Rozwiązanie obsługujące adresy zarówno IPv4 i IPv6,
4. Rozwiązanie musi posiadać wbudowane, predefiniowane raporty. Administrator jest w stanie zdefiniować własne szablony wyszukiwania i wyświetlania zdarzeń.
5. Rozwiązanie musi zapewnić możliwość tworzenia kont administratorów oraz przydzielanie im uprawnień do czynności jakie dane użytkownik może wykonać w tym minimum przypisywania im uprawnień do zarządzania i konfigurowania wskazanych urządzeń zainstalowanych w lokalizacjach prokuratury.
6. Uwierzytelnianie administratorów odbywa się za pomocą haseł statycznych, haseł dynamicznych lub certyfikatów cyfrowych.
7. Rozwiązanie musi posiadać możliwość konfiguracji kont operatorów o uprawnieniach niższych niż administratorzy oraz przydzielanie im uprawnień do czynności jakie dane użytkownik może wykonać. Rozwiązanie musi zapewniać możliwość sprawdzania i rozliczania użytkowników z ich aktywności,
8. Jeżeli do osiągnięcia którejkolwiek z wymienionych funkcjonalności wymagane jest dostarczenie licencji, Wykonawca musi uwzględnić ten fakt w swojej ofercie i dostarczyć urządzenie wraz ze wszystkimi wymaganymi licencjami.
 |

# **Odnowienie usługi serwisowej i licencji dla System Monitorowania Sieci oraz Korelacji Logów**

* + - 1. **Solarwinds License Log and Event Manager - LEM 500**
			2. **Solarwinds Lincese Orion Network Performance Monitor –SLX – 500 device**

**Oferowane oprogramowanie nr 1 \* …………………….. Producent \* …………………..**

**Oferowane oprogramowanie nr 2 \* …………………….. Producent \* …………………..**

|  |  |
| --- | --- |
| **Oprogramowanie** | 1. Wykonawca zapewni odnowienie licencji i suportu na okres 3 lat przez producenta rozwiązania lub Autoryzowanego Dystrybutora producenta wraz z przedłużeniem wymaganych licencji
2. Wykonawca wyrówna terminy związane z serwisem i licencjami
3. Wykonawca zapewni dostęp wskazanego personelu Zamawiającego do dedykowanego portalu www producenta oprogramowania, na którym będzie możliwe co najmniej pobieranie nowych wersji dedykowanego dla danego urządzenia oprogramowania, pobieranie aktualizacji, patch-y, a także dostęp do bazy wiedzy, przewodników konfiguracyjnych, narzędzi diagnostycznych, oprogramowania wspomagającego itp..
4. Wykonawca zapewni możliwość zgłaszania na stronach www producenta oprogramowania problemów eksploatacyjnych związanych z obsługą sprzętu będącego przedmiotem zamówienia.
5. Zaproponowany pakiet serwisowy musi zapewniać bezpośrednie zgłoszenie awarii oprogramowania do producenta oprogramowania (nie tylko do serwisu Wykonawcy) przez cały okres świadczenia usług serwisowych.
6. Wykonawca w oferowanych pakietach serwisowych producenta zapewni dostęp do pomocy technicznej producenta (drogą telefoniczną, poprzez email lub stronę WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego.
7. Wykonawca zaktualizuje oprogramowanie do wersji najnowszej rekomendowanej przez producenta rozwiązania.
8. Wykonawca dostarczy w terminie 60 dni od dnia podpisania umowy dokument potwierdzający zarejestrowanie kontraktu serwisowego oraz dokument potwierdzający bezpośredni dostęp Zamawiającego do pomocy technicznej producenta oraz do zasobów pobierania oprogramowania do urządzeń objętych serwisem, wystawiony przez producenta oprogramowania lub jego oficjalnego przedstawiciela.
9. Wykonawca dokona migracji kont administracyjnych z kontrolera domeny obecnie wykorzystywanego (60 użytkowników ) do centralnej domeny oraz wykona rekonfiguracje systemów monitorowania i korelacji logów.
 |

(\*) Należy podać nazwę oferowanego oprogramowania, numer wersji i producenta.

Zamawiający dopuszcza dostarczenie oprogramowania równoważnego spełniającego co najmniej poniższe wymagania techniczne (wraz z przeniesieniem konfiguracji obecnie eksploatowanych oprogramowania służącego do monitorowania i korelacji logów ):

|  |  |
| --- | --- |
| Architektura  | 1. Dostarczone rozwiązanie musi być w postaci dedykowanego urządzenia (applaiance) lub w postaci oprogramowania.
2. W przypadku dostarczenia systemu monitorowania sieci i korelacji logów w postaci oprogramowania, Wykonawca dostarczy kompleksowo niezbędne środowisko do jego uruchomienia (licencje na system operacyjny, licencje na oprogramowanie bazy danych, licencje na oprogramowanie wirtualizacyjne itp. ) w tym fizyczny serwer w obudowie Rack z redundantnymi zasilaczami i wentylatorami o parametrach nie gorszych niż:
3. 2 procesory 8-rdzeniowe o taktowaniu co najmniej 2,5 GHz
4. co najmniej 20 TB HDD skonfigurowane w RAID 5 dostępne dla Zamawiającego po uruchomieniu systemu monitorowania sieci i korelacji logów pod przyszłe potrzeby związane z działaniem systemu centralnego zarządzania
5. 256 GB pamięci RAM
6. Serwer musi się znajdować na liście kompatybilności sprzętu producenta systemu monitorowania sieci i korelacji logów.
7. Rozwiązanie dostarczone w postaci dedykowanego applaiance powinno mieć parametry fizyczne nie gorsze niż wyspecyfikowane w pkt 2
8. Wydajność i pojemność systemu musi pozwalać na równoczesną obsługę co najmniej 500 urządzeń.
 |
| Funkcjonalności | 1. Rozwiązanie bezagentowe (brak dodatkowego oprogramowania agenta na urządzeniach),
2. Rozwiązanie dostarczone z licencją bez ograniczenia ilości monitorowanych urządzeń oraz interfejsów,
3. Interfejs zarządzania dostępny z wykorzystaniem protokołu https
4. Rozwiązanie posiadające funkcje zaawansowanego alarmowania polegające na:
5. wywoływaniu alarmu przy określonych zdarzeniach
6. wywoływaniu alarmu przy długotrwałym stanie
7. wywoływaniu alarmu przy konfigurowalnej kombinacji stanów urządzeń
8. wysłanie informacji o alarmie do operatorów.
9. Możliwość monitorowania przynajmniej następujących parametrów: wykorzystanie pasma, straty pakietów, opóźnień, błędów
10. Możliwość opracowania konfigurowalnych list urządzeń informujących co najmniej o: największym obciążeniu procesora, największym użyciu pamięci, największym natężeniu ruchu
11. Możliwość odpytywania urządzeń poprzez co najmniej: protokoły ICMP, SNMP (v1, v2c, v3), obsługę trapów SNMP
12. Obsługa zarówno IPv4 jak i IPv6
13. Możliwość konfiguracji kont użytkowników oraz przypisywanie im uprawnień tylko do odpowiednich raportów
14. Możliwość identyfikacji użytkowników, aplikacji i protokołów wykorzystujących sieć
15. Prezentacja danych historycznych oraz wykrywania trendów wykorzystania przepustowości
16. Monitorowanie aplikacji działających na serwerach poprzez weryfikacje aktywności określonego portu
17. Wizualizacja sieci LAN oraz sieci WAN poprzez konfigurację map, na których:
18. będą umieszczane urządzenia oraz połączenia
19. kolory będą wyświetlane w zależności od dostępności lub przepustowości połączeń
20. możliwość stosowania własnych grafik/ikon
21. prezentowania statusu urządzeń (min. dostępne, niedostępne, problem)
22. Możliwość analizowania trendów pojawiających się w infrastrukturze LAN i wykrywania anomalii w ruchu sieciowym oraz zbierania danych chwilowych jak i historycznych (co najmniej w 3 lub 6 miesięcznym okresie)
23. Możliwość informowania o awariach (warunkowe awarie) oraz zapewnienia reakcji na awarie (np. wysłanie wiadomości e-mail, SMS, wykonanie skryptu, itp.)
24. Graficzna prezentacja zarządzanych urządzeń wraz ze stanami portów, możliwością dostępu i narzędziami do monitorowania
25. Możliwość monitorowania dostępności i opóźnień na łączach WAN
26. Rozwiązanie musi umożliwiać zbieranie konsolidowanie i analizowanie logów oraz zdarzeń z:
27. zapór sieciowych (minimum dostarczane urządzenia),
28. urządzeń IDS/IPS (minimum dostarczane urządzenia),

c) przełączników sieciowych (minimum Cisco Systems, Juniper).1. Rozwiązanie musi umożliwiać korelacje w celu identyfikacji ataków,
2. Rozwiązanie musi blokować podejrzane aktywności w tym nieuprawnione użycie USB minimum poprzez kwarantannę zainfekowanych maszyn, blokowanie adresów IP, zabijanie procesów oraz poprzez zastosowanie ustawień Active Directory,
3. Rozwiązanie musi zapewniać monitorowanie integralności plików gromadzonych logów,
4. Rozwiązanie musi zapewniać możliwość generowania zgodności ze standardami bezpieczeństwa,
5. Rozwiązanie musi zapewniać przyjazny interfejs użytkownika umożliwiający łatwe wyszukiwanie informacji,
6. Rozwiązanie musi umożliwiać kompresowanie logowanych danych
 |
| Zarządzanie i konfiguracja | 1. Wymagane jest dostarczenie wraz z rozwiązaniem bazy MIB różnych producentów, a w szczególności posiadanych i eksploatowanych przez Zamawiającego (Cisco Systems, Juniper Networks) oraz możliwość późniejszej aktualizacji bazy MIB.
2. Możliwość konfiguracji bazy administratorów wraz z ich uprawnieniami tzn.:
3. konfigurację kont głównych administratorów posiadających możliwość monitorowania wszystkich urządzeń
4. konfigurację kont administratorów lokalnych posiadających możliwość monitorowania wszystkich przypisanych urządzeń
5. konfigurację kont bez możliwości/uprawnień do zmiany konfiguracji
6. Oprogramowanie musi umożliwiać obsługę co najmniej dostarczanych urządzeń w zakresie korelacji zdarzeń z urządzeń sieciowych.
7. Uwierzytelnianie administratorów odbywa się za pomocą haseł statycznych, haseł dynamicznych lub certyfikatów cyfrowych.
8. Rozwiązanie musi posiadać możliwość konfiguracji kont operatorów o uprawnieniach niższych niż administratorzy oraz przydzielanie im uprawnień do czynności jakie dane użytkownik może wykonać. Rozwiązanie musi zapewniać możliwość sprawdzania i rozliczania użytkowników z ich aktywności,
9. Rozwiązanie musi mieć możliwość integracji z pozostałymi oferowanymi modułami systemu zabezpieczeń, w szczególności z centralnym systemem zarządzania
10. System raportowania musi zapewniać skonsolidowane informacje na temat:
11. Liczby połączeń zablokowanych przez regułę bezpieczeństwa.
12. Głównych źródeł zablokowanych połączeń, ich miejsc docelowych i usług
13. Głównych reguł wykorzystywanych przez politykę bezpieczeństwa
14. Głównych ataków na bezpieczeństwo wykrytych przez punkt egzekwowania polityki, z określeniem ich głównych źródeł i celów
15. Liczby zainstalowanych i odinstalowanych polityk w punkcie egzekwowania
16. Głównych usług sieciowych
17. Aktywności użytkownika z wyszczególnieniem głównych odwiedzanych witryn/adresów
18. Głównych usług, które utworzyły większość obciążenia dla ruchu szyfrowanego
19. Głównych użytkowników VPN, wykonujących połączenia o najdłuższym czasie trwania
20. Jeżeli do osiągnięcia którejkolwiek z wymienionych funkcjonalności wymagane jest dostarczenie licencji, Wykonawca musi uwzględnić ten fakt w swojej ofercie i dostarczyć urządzenie wraz ze wszystkimi wymaganymi licencjami.
 |

# **Rozbudowa posiadanego rozwiązania Cisco UCS C240 o karty FiberChannel oraz przedłużenie usługi serwisowej wraz z wymaganymi licencjami.**

Wykonawca dostarczy do każdego serwera kartę rozszerzeń FC HBA Dual-Port zgodną ze „Spec Sheet” Cisco UCS C240 oraz przedłuży usługę serwisową na posiadany przez zamawiającego sprzęt uwzględniając modyfikacje oraz niezbędne licencje na okres 3 lat.

**Oferowany model \* …………………….. Producent \* …………………..**

|  |  |
| --- | --- |
| **Serwery UCS posiadane przez Zamawiającego** | UCS C240 M4L FCH2039V0N0UCS C240 M4L FCH2116V2H9UCS C240 M4L FCH2116V0JA |
| **Karta rozszerzeń** | UCSC-PCIE-E16002 **Emulex LPe16002-M6, 16Gb Fibre Channel HBA with SR Optics** lub inna spełniająca poniższe wymagania oraz zgodna ze „Spec Sheet” Cisco UCS C240Interfejs: PCIe 3.0 x8Standard: Fibre Channel class 2 oraz 3Ilość portów wraz z wkładkami: 2 (ang. 16 Gb/s short wave lasers with LC type)Szybkość transmisji: min. 16 Gbit/s negocjowana automatycznieDługość okablowania:dla 16Gb: - OM4 (Multi-Mode 50/125μm, 4700 MHz\*km) 125m - OM3 (Multi-Mode 50/125μm, 2000 MHz\*km) 100m - OM2 (Multi-Mode 50/125μm, 500 MHz\*km) 35m dla 8Gb:- OM4 (Multi-Mode 50/125μm, 4700 MHz\*km) 190m - OM3 (Multi-Mode 50/125μm, 2000 MHz\*km) 150m - OM2 (Multi-Mode 50/125μm, 500 MHz\*km) 50m Wsparcie systemów operacyjnych:Microsoft WindowsRed Hat Enterprise LinuxSUSE Linux Enterprise ServerOracle SolarisVMware vSphereBudowa:niski profil PCIe |
| **Zakres prac** | Instalacja kart FC HBA w serwerach, aktualizacja sterowników i kompatybilności sprzętu |

Zamawiający dopuszcza dostarczenie sprzętu równoważnego spełniającego co najmniej poniższe wymagania techniczne (wraz z przeniesieniem konfiguracji obecnie eksploatowanych serwerów. Serwery muszą się znajdować na liście kompatybilności sprzętu producenta systemu monitorowania sieci i korelacji logów.

| Parametr | Serwer 1 | Serwer 2 | Serwer 3 |
| --- | --- | --- | --- |
| Procesory CPU | 16 x 3.20 GHz | 16 x 3.20 GHz | 16 x 3.20 GHz |
| Pamięć RAM | 256GB | 256GB | 256GB |
| Dyski twarde | 8x 600GB4x 10TB | 4x 400GB4x 600GB | 4x 600GB4x 1,2TB4x 4TB |
| Karta rozszerzeń | Emulex LPe16002-M6, 16Gb Fibre Channel HBA with SR Optics lub równoważna | Emulex LPe16002-M6, 16Gb Fibre Channel HBA with SR Optics lub równoważna | Emulex LPe16002-M6, 16Gb Fibre Channel HBA with SR Optics lub równoważna |

(\*) Należy podać nazwę oferowanego sprzętu, oprogramowania, numer wersji i producenta.

# **Rekonfiguracja posiadanego przez zamawiającego środowiska opartego na Vmware.**

Zamawiający posiada następujące kończące się licencje:

Production Support/Subscription VMware vSphere 6 Essentials Plus Kit for 3 years VMware vSphere 6 Essentials Plus Kit for 3 hosts (Max 2 processors per host) 1

Production Support/Subscription VMware vSphere 6 Essentials Plus Kit for 3 years VMware vCenter Server 6 Essentials for vSphere 1

Production Support/Subscription VMware vSphere 6 Essentials Plus Kit for 3 years VMware vSphere 6 Essentials Plus for 1 processor 6

W związku z kończącym się suportem na produkty Vmware Zamawiający dostarczy nowe licencje (vSphere Enterprise Plus) i obejmie produkty Vmware własnym suportem (nie leży to w gestii Wykonawcy)

|  |  |
| --- | --- |
| **Zakres prac** | **Niezbędne prace do wykonania podłączania ESX do vCenter Zamawiającego:**1. Instalacja najnowszej rekomendowanej wersji VMware na serwerach kompatybilne z vCenter Zamawiającego
2. Konfiguracja klastra zgodnie z najlepszymi praktykami w istniejącym vCenter i dodanie 3 serwerów z dokonaniem niezbędnych konfiguracji.
3. Wykonawca zapewni podłączenie niezbędnego okablowania dla sieci LAN/SAN
4. Rekonfiguracja sieci LAN/SAN na potrzeby podłączenia zasobów macierzowych do nowo utworzonego klastra Vmware m.in. zony.
5. Wystawienie niezbędnych zasobów dyskowych z macierzy pod stworzony klaster Vmware
6. Przeniesienie maszyn wirtualnych z obecnego środowiska do nowo utworzonego, testy dostępności, migracji itd.
7. Rekonfiguracja systemu backup na potrzeby nowo utworzonego klastra wspólnie z Zamawiającym, testy odtworzeniowe.
8. Przeszkolenie administratorów z zakresu tzn. przeprowadzenie warsztatów dla 3 administratorów Zamawiającego z Vmware, SAN w zakresie podstawowym w ilości 24 godzin)
9. Przygotowanie dokumentacji powdrożeniowej, administratora i procedur utrzymaniowych.
 |

(\*) Należy podać nazwę oferowanego oprogramowania, numer wersji i producenta.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Czytelny podpis/podpisy osoby/osób uprawnionego/ych do reprezentowania Wykonawcy**

**Miejscowość\_\_\_\_\_\_\_\_\_\_\_\_\_, dnia \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**