Zakład Emerytalno-Rentowy
Ministerstwa Spraw Wewnętrznych i Administracji

Warszawa, dnia 26 WRZ. 2022 r.

Nr sprawy: ZER-ZP-13/2022

Wykonawcy

W związku z pytaniami zgłoszonymi w trybie w trybie art. 284 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710), zwanej dalej „ustawą Pzp", w sprawie postępowania nr ZER-ZP-13/2022, prowadzonego w trybie podstawowym bez negocjacji, zgodnie z art. 275 pkt 1 ustawy Pzp na: ***Zakup firewall-i ze wsparciem technicznym***, Zamawiający, na podstawie art. 284 ust. 2 i 6 ustawy Pzp, udziela wyjaśnień treści specyfikacji warunków zamówienia, zwanej dalej „SWZ" oraz zmienia treść Opisu przedmiotu zamówienia.

Jednocześnie Zamawiający informuje, że zgodnie z art. 286 ust. 1 i ust. 7 ustawy Pzp dokonał zmiany treści specyfikacji warunków zamówienia, zwanej dalej „SWZ", zgodnie z treścią niniejszego pisma.

I. Wyjaśnienia treści oraz zmiana SWZ

Pytanie nr 1:

„Czy Zamawiający dopuści rozwiązanie rozpoznawania aplikacji równoważne do AVC, jako że AVC to nazwa własna producenta Cisco.
Wymaganie dotyczące rozwiązania rozpoznawania aplikacji AVC ogranicza możliwość złożenia oferty na systemy innych producentów, którzy używają innych nazw odpowiadających temu rozwiązaniu, co zgodnie z Pzp może utrudniać uczciwą konkurencję wykonawców."

Odpowiedź na pytanie nr 1:

Zamawiający modyfikuje treść Opisu przedmiotu zamówienia stanowiącego Załącznik nr 1 do SWZ – Tabela nr 1, zgodnie z poniższym:
Obecna treść:

Nazwa	Parametry minimalne
Opis urządzenia	1. Urządzenie musi pełnić rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej firewall-a Next-Generation (NGFW). 2. Urządzenie musi być wyposażone w: a) min. 12 portów 1 Gigabit Ethernet (każdy obsługujący prędkość 10/100/1000BaseT Gigabit Ethernet), b) min. 4 porty 1 GE SFP oraz c) min. 2 porty 10 GE SFP. d) zamiast pozycji lit. b i c Zamawiający dopuszcza 4 porty pracujące z prędkością 1/10 GE SFP/SFP+ e) lub równoważną konfigurację dla punktów lit. a, b, c, d 3. Urządzenie musi być wyposażone w dedykowany port konsoli oraz dedykowany port 1 Gigabit Ethernet do zarządzania MGMT. 4. Urządzanie musi posiadać redundantne wbudowane zasilacze zasilane

	prądem przemiennym 230V. 5. Urządzenie musi posiadać możliwość montażu w szafie RACK 19". Urządzenie będzie dostarczone wraz z elementami montażowymi do szafy RACK 19". 6. Urządzenie musi mieć wysokość nie większą niż 1U. 7. Urządzenie musi posiadać dysk twardy SSD min. 200 GB do zapisu logów.
UTM Firewall	1. Wydajność urządzenia dla uruchomionych modułów firewall-a oraz kontroli aplikacji (AVC) – min. 1,5 Gb/s. 2. Wydajność urządzenia dla uruchomionych modułów systemu IPS – min. 1,2 Gb/s. 3. Min. liczba obsługiwanych sesji równoległych (TCP): 250 000, z możliwością zestawiania min. 12 000 nowych połączeń na sekundę (TCP). 4. Urządzenie musi mieć możliwość pracy jako brama VPN z wydajnością min. 600 Mb/s dla IPSec VPN AES256-SHA256. 5. Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej. 6. Urządzenie musi obsługiwać routing statyczny i dynamiczny (RIP, OSPF, BGP). 7. Urządzenie musi zapewniać poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 8. Urządzenie musi posiadać ochronę przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 9. Urządzenie musi posiadać kontrolę zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 10. Urządzenie musi posiadać kontrolę stron WWW oraz SSL Inspection 11. Urządzenie musi posiadać możliwość stworzenia/uruchomienia usługi Web-Proxy. 12. Urządzenie musi posiadać możliwość zarządzania pasmem (QoS, Traffic shaping). 13. Polityka firewall-a musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 14. Firewall musi zapewniać translację adresów NAT: źródłowego i docelowego. 15. Urządzenie musi posiadać możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory. 16. Urządzenie musi zapewniać mechanizmy redundancji w tym możliwość konfiguracji urządzenia w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active-active, active-passive, clustering. 17. Urządzenie musi zapewniać funkcjonalność tzw. Firewall-a Next-Generation w zakresie: • systemu automatycznego wykrywania i klasyfikacji aplikacji

	(Application Visibility and Control), • systemu IPS, • systemu antymalware, • filtracja treści URL.
IPS	1. System IPS musi zapewniać: • możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system), • możliwość pracy w trybie pasywnym (IDS). 2. System IPS musi zapewniać możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym: • złośliwego oprogramowania, • ataków na usługę VoIP, • prób przepełnienia bufora, • ataków na aplikacje P2P, • zagrożeń dnia zerowego, itp. 3. System IPS musi zapewniać możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna). 4. System IPS musi zapewniać wiele sposobów wykrywania zagrożeń w tym: • sygnatur ataków opartych na exploitach, • reguł opartych o wzorce znanych zagrożeń, • mechanizmy wykrywania anomalii w protokołach. 5. System IPS musi zapewniać możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, jak również sprawdzania zawartości pakietów. 6. System IPS musi zapewniać mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives). lub inny mechanizm realizując podobną funkcjonalność. 7. System IPS musi zapewniać możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń lub możliwość wyeksportowania tego typu zdarzeń do zewnętrznego urządzenia typu SIEM. 8. System IPS musi zapewniać możliwość reakcji na zdarzenia min. takie, jak: • tylko monitorowanie, • blokowanie ruchu zawierającego zagrożenia, • zapisywanie pakietów. 9. System IPS musi zapewniać możliwość detekcji ataków i zagrożeń opartych na protokole IPv6. 10. System IPS musi zapewniać możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, SSH itp. 11. System IPS musi zapewniać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji. 12. System IPS musi zapewniać możliwość obrony przed atakami

	skonstruowanymi tak, aby uniknąć wykrycia przez IPS. W tym celu musi zapewnić możliwość blokowania każdego połączenia, które nosi znamiona manipulacji nr sekwencyjnymi segmentów TCP, be względu do jakiego hosta docelowego kierowane jest to połączenie. 13. System IPS musi zapewniać mechanizm bezpiecznej aktualizacji sygnatur/reguł. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne. 14. System IPS musi umożliwiać definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie. 15. System IPS musi zapewniać możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS.
Antymalware	1. Urządzenie musi zapewniać możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym: • pliki systemowe, • pliki graficzne, • pliki PDF, • pliki wykonywalne, • pliki multimedialne, • pliki pakietu Office, • pliki skompresowane. 2. Urządzenie musi posiadać możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download. 3. Urządzenie musi posiadać podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez: • sprawdzenie reputacji plików w systemie globalnym, • statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu.
URL filtering	System filtracji URL musi zapewniać: • kategoryzację stron – w co najmniej 50 kategoriach.

Zostaje zmieniona na:

Nazwa	Parametry minimalne
Opis urządzenia	1. Urządzenie musi pełnić rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej firewall-a Next-Generation (NGFW). 2. Urządzenie musi być wyposażone w: a) min. 12 portów 1 Gigabit Ethernet (każdy obsługujący prędkość 10/100/1000BaseT Gigabit Ethernet), b) min. 4 porty 1 GE SFP oraz c) min. 2 porty 10 GE SFP. d) zamiast pozycji lit. b i c Zamawiający dopuszcza 4 porty pracujące z prędkością 1/10 GE SFP/SFP+ e) lub równoważną konfigurację dla punktów lit. a, b, c, d 3. Urządzenie musi być wyposażone w dedykowany port konsoli oraz

	dedykowany port 1 Gigabit Ethernet do zarządzania MGMT. 4. Urządzanie musi posiadać redundantne wbudowane zasilacze zasilane prądem przemiennym 230V. 5. Urządzenie musi posiadać możliwość montażu w szafie RACK 19". Urządzenie będzie dostarczone wraz z elementami montażowymi do szafy RACK 19". 6. Urządzenie musi mieć wysokość nie większą niż 1U. 7. Urządzenie musi posiadać dysk twardy SSD min. 200 GB do zapisu logów.
UTM Firewall	1. Wydajność urządzenia dla uruchomionych modułów firewall-a oraz kontroli aplikacji na poziomie min. 1,5 Gb/s. 2. Wydajność urządzenia dla uruchomionych modułów systemu IPS – min. 1,2 Gb/s. 3. Min. liczba obsługiwanych sesji równoległych (TCP): 250 000, z możliwością zestawiania min. 12 000 nowych połączeń na sekundę (TCP). 4. Urządzenie musi mieć możliwość pracy jako brama VPN z wydajnością min. 600 Mb/s dla IPSec VPN AES256-SHA256. 5. Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej. 6. Urządzenie musi obsługiwać routing statyczny i dynamiczny (RIP, OSPF, BGP). 7. Urządzenie musi zapewniać poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 8. Urządzenie musi posiadać ochronę przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 9. Urządzenie musi posiadać kontrolę zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 10. Urządzenie musi posiadać kontrolę stron WWW oraz SSL Inspection 11. Urządzenie musi posiadać możliwość stworzenia/uruchomienia usługi Web-Proxy. 12. Urządzenie musi posiadać możliwość zarządzania pasmem (QoS, Traffic shaping). 13. Polityka firewall-a musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 14. Firewall musi zapewniać translację adresów NAT: źródłowego i docelowego. 15. Urządzenie musi posiadać możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory. 16. Urządzenie musi zapewniać mechanizmy redundancji w tym możliwość konfiguracji urządzenia w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active-active, active-passive, clustering. 17. Urządzenie musi zapewniać funkcjonalność tzw. Firewall-a Next-Generation w zakresie: • systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control), • systemu IPS, • systemu antymalware, • filtracja treści URL.

IPS	16. System IPS musi zapewniać: • możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system), • możliwość pracy w trybie pasywnym (IDS). 17. System IPS musi zapewniać możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym: • złośliwego oprogramowania, • ataków na usługę VoIP, • prób przepełnienia bufora, • ataków na aplikacje P2P, • zagrożeń dnia zerowego, itp. 18. System IPS musi zapewniać możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna). 19. System IPS musi zapewniać wiele sposobów wykrywania zagrożeń w tym: • sygnatur ataków opartych na exploitach, • reguł opartych o wzorce znanych zagrożeń, • mechanizmy wykrywania anomalii w protokołach. 20. System IPS musi zapewniać możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, jak również sprawdzania zawartości pakietów. 21. System IPS musi zapewniać mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives). lub inny mechanizm realizując podobną funkcjonalność. 22. System IPS musi zapewniać możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń lub możliwość wyeksportowania tego typu zdarzeń do zewnętrznego urządzenia typu SIEM. 23. System IPS musi zapewniać możliwość reakcji na zdarzenia min. takie, jak: • tylko monitorowanie, • blokowanie ruchu zawierającego zagrożenia, • zapisywanie pakietów. 24. System IPS musi zapewniać możliwość detekcji ataków i zagrożeń opartych na protokole IPv6. 25. System IPS musi zapewniać możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, SSH itp. 26. System IPS musi zapewniać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji. 27. System IPS musi zapewniać możliwość obrony przed atakami skonstruowanymi tak, aby uniknąć wykrycia przez IPS. W tym celu musi zapewnić możliwość blokowania każdego połączenia, które nosi znamiona manipulacji nr sekwencyjnymi segmentów TCP, be względu do jakiego hosta docelowego kierowane jest to połączenie. 28. System IPS musi zapewniać mechanizm bezpiecznej aktualizacji sygnatur/reguł. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne. 29. System IPS musi umożliwiać definiowania wyjątków dla sygnatur

	z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie. 30. System IPS musi zapewniać możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS.
Antymalware	1. Urządzenie musi zapewniać możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym: • pliki systemowe, • pliki graficzne, • pliki PDF, • pliki wykonywalne, • pliki multimedialne, • pliki pakietu Office, • pliki skompresowane. 2. Urządzenie musi posiadać możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download. 3. Urządzenie musi posiadać podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez: • sprawdzenie reputacji plików w systemie globalnym, • statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu.
URL filtering	System filtracji URL musi zapewniać: • kategoryzację stron – w co najmniej 50 kategoriach.

Pytanie nr 2:
„Czy Zamawiający dopuści rozwiązanie mające dysk SSD o wielkości 100GB?"

Odpowiedź na pytanie nr 2:
Zamawiający podtrzymuje zapisy Opisu przedmiotu zamówienia.

Proszę o uwzględnienie zmian przy sporządzaniu oferty.

ZASTĘPCA DYREKTORA
Zakładu Emerytalno-Rentowego
Ministerstwa Spraw Wewnętrznych i Administracji
6.09.2022
Jarosław SOCHA

(data i podpis Kierownika Zamawiającego lub osoby przez niego upoważnionej)