Centrum Informatyki Statystycznej

Znak: CIS-WAZ.271.8.2024

Warszawa, dnia 26.08.2024 r.

Do zainteresowanych wykonawców

Dotyczy: Postępowania prowadzonego w trybie przetargu nieograniczonego **CIS-WAZ.271.8.2024** na **Zakup internetowego, brzegowego systemu bezpieczeństwa**

Centrum Informatyki Statystycznej działając na podstawie art. 135 ust. 2 ustawy Prawo zamówień publicznych (tj. Dz. U. 2023 poz. 1605 ze zm) dalej „ustawa Pzp", informuje , iż wpłynęły pytania do treści Specyfikacji Warunku Zamówienia (dalej SWZ) i udziela następujących wyjaśnień opisu przedmiotu zamówień (załącznik nr 1 do SWZ) dalej OPZ:

Pytanie 1.
Załącznik nr 1 do SWZ
Zadanie 2.
A Zakup i dostawa urządzeń zapory brzegowej (HA) w konfiguracji minimum.
I.2 szt. urządzeń typu NG Firewall – system HA

3. W komplecie muszą znajdować się szyny umożliwiające montaż urządzenia w szafie rack oraz kable zasilające, zaślepki na miejsca dla nieużywanych modułów itp.
Czy Zamawiający dopuszcza urządzenia montowane za pomocą uchwytów, nie posiadające szyn?

Odpowiedź:
Zamawiający dopuszcza stosowanie innych, zgodnych ze specyfikacją Producenta dostarczonych urządzeń, systemów montażu urządzeń do szaf typu rack.

Pytanie 2.
Załącznik nr 1 do SWIZ
Zadanie 2.
A Zakup i dostawa urządzeń zapory brzegowej (HA) w konfiguracji minimum.
I.2 szt. urządzeń typu NG Firewall – system HA

Każde z urządzeń w klastrze HA musi być wyposażone w co najmniej następujące interfejsy sieciowe:
a) 8 portów 1/10GBASE-F obsadzone wkładkami SFP+,
b) 4 porty 10/25GBASE-F obsadzone wkładkami min. 10 Gbps,
c) 2 porty 40/100GBASE-F obsadzone wkładkami min. 40 Gbps.
Proszę o potwierdzenie czy wkładki o których mowa to
a) 8 wkładek 10G SR SFP+
b) 4 wkładki 10G SR SFP+
10 2 wkładki 40G SR4 SFP+

Odpowiedź:
Zamawiający podtrzymuje zapisy zawarte w OPZ. Wyszczególnione w podpunktach b) i c) interfejsy określają tylko oczekiwaną przepustowość transmisji, natomiast nie definiują typu wkładek optycznych. Ich rodzaj zależy od zastosowanej przez producenta technologii.

Pytanie 3.
Załącznik nr 1 do SWIZ
Zadanie 2.
A Zakup i dostawa urządzeń zapory brzegowej (HA) w konfiguracji minimum.
I.2 szt. urządzeń typu NG Firewall – system HA

Centrum Informatyki Statystycznej
Aleja Niepodległości 208, 00-925 Warszawa
tel. 22 608 31 44
cissek@stat.gov.pl
cis.stat.gov.pl

14. Każde z urządzeń w klastrze HA musi obsługiwać nie mniej niż 20 000 000 jednoczesnych połączeń i umożliwiać zestawianie nie mniej niż 900 000 połączeń na sekundę.
Czy Zamawiający zmieni zapis i dopuści rozwiązanie posiadające 870 000 połączeń na sekundę? Obecny wymóg powoduje konieczność zaproponowania przez jednego z największych i najwyżej ocenianych przez Gartnera (firmę Fortinet) produktu dużo droższego oraz takiego, który jest kilka razy bardziej wydajny. Obecnie sformułowane wymaganie nie pozwoli firmie fortinet zaproponować konkurencyjnego rozwiązania do opisanego urządzenia Checkpoint 29100.

Odpowiedź:
Zamawiający dopuszcza rozwiązanie posiadające 870 000 połączeń na sekundę. Wielkość tego parametru zawiera się w przewidywanym przez Zamawiającego zakresie błędu przepustowości +/- 5%.

Pytanie 4.
Załącznik nr 1 do SWIZ
Zadanie 2.
A Zakup i dostawa urządzeń zapory brzegowej (HA) w konfiguracji minimum.
I.2 szt. urządzeń typu NG Firewall – system HA
34. System musi zapewniać możliwość rozbudowy o funkcjonalności:
c) Możliwość filtrowania URL, musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. Wymagane jest posiadanie oddzielnych kategorii dla zagrożeń typu malware, phishing, command-and-control oraz ostatnio zarejestrowane domeny (NRD). Równolegle z oceną URL musi być dokonywany i określany poziom ryzyka związany z danym URL na poziomie małe ryzyko, średnie ryzyko, wysokie ryzyko.
Czy Zamawiający dopuści rozwiązanie, które zamiast nazwy malware posiada kategorię malicious websites. To jest nazwa określająca ten sam rodzaj stron url.
Czy Zamawiający dopuści rozwiązanie, które zamiast kategorii „command-and-control" w url filtering posiada inny mechanizm ochrony przez atakami typu botnet np. przez blokowanie komunikacji do serwerów command-and-control za pomocą filtrów DNS. Różni producenci różnie podchodzą do zagadnienia ochrony przed atakami bot. Uważamy że blokowanie za pomocą filtrów DNS jest dużo bardziej skuteczne niż blokowanie za pomocą filtrów url, ponieważ większość komunikacji do serwerów command-and-control jest realizowana za pomocą innych protokołów niż http/https i dlatego filtry url nie są skuteczne. Dużo bardziej skuteczna jest ochrona za pomocą filtrów DNS, ponieważ praktycznie każda komunikacja z serwerami command-and-control odbywa się przez nazwy rozwiązywane za pomocą serwera DNS.
Czy Zamawiający dopuści rozwiązanie, które nie określa ryzyka na poziomie małe ryzyko, średnie ryzyko, wysokie ryzyko? Kategoryzowanie URL samo w sobie definiuje jakie jest ryzyko. Są kategorie takie jak Malicious Websites, Phishing, Newly Registered Domain, które samo w sobie świadczą o dużym ryzyku. Są kategorie, które są klasyfikowane jako średnie ryzyko oraz takie które mają małe ryzyko. Prosimy o usunięcie tego wymagania.

Odpowiedź:
Zamawiający dopuszcza rozwiązania, które zamiast kategorię „malware" posiadają kategorię „malicious websites".
Zamawiający dopuszcza rozwiązanie, które zamiast kategorii „command-and-control" w url filtering posiada inny mechanizm ochrony przez atakami typu botnet.
Zamawiający akceptuje uwagi Wykonawcy i dokonuje zmiany poprzez wykreślenie zdania „Równolegle z oceną URL musi być dokonywany i określany poziom ryzyka związany z danym URL na poziomie małe ryzyko, średnie ryzyko, wysokie ryzyko". Punkt 34 otrzymuje brzmienie:
System musi zapewniać możliwość rozbudowy o funkcjonalności:
a) DNS sinkholing. Funkcjonalność zabezpieczania DNS dostępna na urządzeniu musi umożliwiać procesowanie zapytań DNS w celu wykrywania i blokowania: zagrożeń, wycieku danych (exfiltracja), tunelowania DNS.
b) Przechwytywanie i przesyłanie do zewnętrznych systemów typu „SandBox" plików różnych typów przechodzących przez firewall w celu ochrony przed zagrożeniami typu zero-day.

Centrum Informatyki Statystycznej
Aleja Niepodległości 208, 00-925 Warszawa
tel. 22 608 31 44
cissek@stat.gov.pl
cis.stat.gov.pl

c) Możliwość filtrowania URL, musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. Wymagane jest posiadanie oddzielnych kategorii dla zagrożeń typu malware, phishing, command-and-control oraz ostatnio zarejestrowane domeny (NRD).
Zamawiający nie wymaga powyższych funkcjonalności w momencie dostarczenia systemu przez Wykonawcę.

Pytanie 5.
Załącznik nr 1 do SWIZ
Zadanie 2.
A Zakup i dostawa urządzeń zapory brzegowej (HA) w konfiguracji minimum.
I.2 szt. urządzeń typu NG Firewall – system HA
36. Urządzenie musi posiadać możliwość wykonania kopii migawkowych oraz jej odtworzenie, zawierających konfigurację wraz z systemem operacyjnym w formie pliku binarnego.
Pojęcie kopii migawkowych jest charakterystyczne dla producenta firmy Checkpoint i nie jest realizowane przez żadnego innego producenta firewalli. Forma kopii zapasowej w pliku binarnym nie daje żadnej wartości, producenci różnych systemów realizują kopię zapasowe w plikach tekstowych lub xml oraz dają możliwość szyfrowania danego pliku. Czy w związku z tym Zamawiający zmieni wymaganie w sposób następujący?:
Urządzenie musi posiadać możliwość wykonania kopii zapasowej oraz jej odtworzenie.

Odpowiedź:
Zamawiający akceptuje uwagi Wykonawcy i dokonuje zmiany przedmiotowego zapisu. Punkt 36 otrzymuje brzmienie:
„Urządzenie musi posiadać możliwość wykonania kopii zapasowej oraz jej odtworzenie".

Pytanie 6.
A Zakup i dostawa urządzeń zapory brzegowej (HA) w konfiguracji minimum.
II. 1 szt. Centralny System Zarządzania i Raportowania (CSZiR)
8. Komunikacja pomiędzy modułem zapory sieciowej (funkcjonujących na zewnętrznych urządzeniach) i modułem zarządzania i raportowania (CSZiR) powinna być szyfrowana i uwierzytelniona z użyciem certyfikatów cyfrowych generowanych przez moduł zarządzania i raportowania(CSZiR).
Czy Zamawiający dopuści rozwiązanie, w którym certyfikat cyfrowy do komunikacji z systemem zarządzania jest generowany na zaporze sieciowej lub zewnętrznym serwerze CA? Generowanie certyfikatów dla zapory bezpieczeństwa przez moduł zarządzania i raportowania jest wymaganiem, które nie wnosi nic w zakresie bezpieczeństwa lub łatwości konfiguracji a jednocześnie wyklucza urządzenia innych producentów niż Checkpoint.

Odpowiedź:
Zamawiający dopuszcza rozwiązania, w których certyfikaty cyfrowe dla komunikacji z CSZiR są generowane w inny sposób (np. na zaporze sieciowej, zewnętrznym CA). Zapisy pkt. 8 miały określić oczekiwane standardy bezpiecznej komunikacji.

Pytanie 7.
Załącznik nr 1 do SWIZ
Zadanie 2.
A Zakup i dostawa urządzeń zapory brzegowej (HA) w konfiguracji minimum.
II. 1 szt. Centralny System Zarządzania i Raportowania (CSZiR)
10. Uwierzytelnianie administratorów powinno umożliwiać wykorzystanie następujących metod:
c)uwierzytelnienie wieloskładnikowe przynajmniej na podstawie loginu i hasła oraz przynajmniej certyfikatu dla przeglądarki/urządzenia lub kodu OTP lub tokenu sprzętowego.
Czy w ramach postępowania należy dostarczyć licencję lub token, czy urządzenie ma mieć tylko taką możliwość? Jeżeli należy dostarczyć tokeny to prosimy o podanie informacji ile sztuk.
Odpowiedź:

Zamawiający wymaga funkcjonalności uwierzytelniania wieloskładnikowego przynajmniej na podstawie: login/password i certyfikatu przeglądarki/urządzenia. Pozostałe zapisy określają tylko możliwości dalszej funkcjonalności. Zamawiający nie wymaga dostarczenia tokenów w momencie dostarczenia systemu przez Wykonawcę.

Pytanie 8.

Załącznik nr 1 do SWIZ
Zadanie 2.
A Zakup i dostawa urządzeń zapory brzegowej (HA) w konfiguracji minimum.
II. 1 szt. Centralny System Zarządzania i Raportowania (CSZiR)
11. Musi istnieć możliwość definiowania szczegółowych uprawnień administratorów, minimalnie:
d) do administracji kontami użytkowników poszczególnych elementów systemu.
Czy Zamawiający dopuści rozwiązanie, które ma możliwość definiowania uprawnień administratorów do konfiguracji systemu (w tym kont użytkowników) nie posiadając bezpośredniej możliwości definiowania szczegółowych uprawnień do administracji kontami użytkowników. Wymaganie opisane nie jest spełniane przez większość producentów firewalli.

Odpowiedź:
Zamawiający dopuszcza rozwiązania definiowania uprawnień administratorów do konfiguracji systemu (w tym kont użytkowników) i nie wymaga możliwości definiowania szczegółowych uprawnień do administracji kontami użytkowników.

Pytanie 9.

A Zakup i dostawa urządzeń zapory brzegowej (HA) w konfiguracji minimum.
II. 1 szt. Centralny System Zarządzania i Raportowania (CSZiR)
12. System zarządzania i raportowania (CSZiR) musi być w stanie wyświetlić z graficznej konsoli listę aktywnych połączeń obsługiwanych przez moduły zapór sieciowych. Informacja o połączeniu powinna zawierać minimum adres źródła, adres przeznaczenia, port źródła, port przeznaczenia oraz identyfikator usługi sieciowej.
Czy Zamawiający jest w stanie zrezygnować z tego wymagania, ogranicza one możliwość zaproponowania konkurencyjnego rozwiązania.
Odpowiedź:
Zamawiający wymaga aby system zarządzania i raportowania posiadał możliwość wyświetlania informacji o zakończonych połączeniach w formie graficznej (chociażby poprzez https) a nie tylko przez CLI. Zamawiający wymaga aby aktywne sesje były widoczne na urządzeniu zapory brzegowej.

Pytanie 10.

Załącznik nr 1 do SWIZ
Zadanie 2
A Zakup i dostawa urządzeń zapory brzegowej (HA) w konfiguracji minimum.
II. 1 szt. Centralny System Zarządzania i Raportowania (CSZiR)
14. CSZiR musi umożliwiać monitorowanie i prezentowanie za pomocą graficznej konsoli takich parametrów zarządzanych zapór sieciowych takich jak: średnie obciążenie procesora, zajętość pamięci operacyjnej, zajętość przestrzeni dyskowej, wersję oprogramowania zapory sieciowej, nazwę i wersję zainstalowanej polityki bezpieczeństwa.
Czy Zamawiający zaakceptuje rozwiązanie, które nie jest w stanie monitorować zajętości przestrzeni dyskowej?
Odpowiedź:
Zamawiający akceptuje uwagi Wykonawcy i dopuszcza rozwiązanie które nie monitoruje zajętości dysku.

Pytanie 11.

Załącznik nr 1 do SWIZ
Zadanie 2.
A Zakup i dostawa urządzeń zapory brzegowej (HA) w konfiguracji minimum.

Centrum Informatyki Statystycznej

Aleja Niepodległości 208, 00-925 Warszawa
tel. 22 608 31 44
cissek@stat.gov.pl
cis.stat.gov.pl

II. 1 szt. Centralny System Zarządzania i Raportowania (CSZiR)
18. CSZiR musi umożliwiać graficzną prezentację zdarzeń pogrupowanych w zależności od kraju pochodzenia źródła transmisji.
Czy Zamawiający jest w stanie zrezygnować z tego wymagania, ogranicza one możliwość zaproponowania konkurencyjnego rozwiązania.

Odpowiedź:
Zamawiający akceptuje uwagi Wykonawcy. dokonuje usunięcia pkt 18. „CSZiR musi umożliwiać graficzną prezentację zdarzeń pogrupowanych w zależności od kraju pochodzenia źródła transmisji".

Pytanie 12.
I. 2 szt. urządzeń typu NG Firewall – system HA
13. Każde z urządzeń w klastrze HA musi posiadać przepustowość ruchu co najmniej 30 Gbit/s dla kontroli zawartości tj.: firewall, kontrola aplikacji na wszystkich portach, IPS, antywirus, antymalware i antyspyware. Wydajność IPSec VPN urządzenie musi wynosić co najmniej 75 Gbit/s.
- Czy Zamawiający dopuszcza aby wydajność IPSec VPN każdego z urządzeń wynosiła co najmniej 20 Gbit/s?

Odpowiedź:
Zamawiający podtrzymuje zapisy zawarte w OPZ.

Pytanie 13
14. Każde z urządzeń w klastrze HA musi obsługiwać nie mniej niż 20 000 000 jednoczesnych połączeń i umożliwiać zestawianie nie mniej niż 900 000 połączeń na sekundę.
- Czy Zamawiający dopuszcza aby każde z urządzeń w klastrze HA obsługiwało nie mniej niż 4 500 000 jednoczesnych połączeń i umożliwiało zestawianie nie mniej niż 250 000 połączeń na sekundę?

Odpowiedź:
Zamawiający podtrzymuje zapisy zawarte w OPZ.

Pytanie 14
II. 1 szt. Centralny System Zarządzania i Raportowania (CSZiR)
2. W przypadku jeżeli Wykonawca nie wykorzysta udostępnionych w pkt. 1 urządzeń jest zobowiązany dostarczyć wraz z urządzeniami NGFW:
b) odpowiednią, komercyjną platformę sprzętową (appliance) z systemem operacyjnym wraz z licencjami (o ile będzie wymagana) i gwarancją na okres trwania umowy,
- Czy Zamawiający dopuszcza aby Centralny System Zarządzania i Raportowania (CSZiR) dostarczony został w formie Maszyny Wirtualnej (VM)?

Odpowiedź:
Zamawiający podtrzymuje zapisy zawarte w OPZ.

Pytanie 15
Jeszcze odnośnie serwisu:
W punkcie IV.18. OPZ Zamawiający określił następujące wymagania odnośnie czasu naprawy oferowanych rozwiązań:
"Wymagany czas na wykonanie naprawy wynosi 24 godziny od momentu potwierdzenia zgłoszenia telefonicznego lub pisemnie do siedziby serwisu, natomiast działania serwisowe należy podjąć w ciągu 4 godzin od momentu zgłoszenia telefonicznego lub pisemnie do siedziby serwisu."
Czy Zamawiający dopuszcza aby w przypadku awarii wymiana lub naprawa urządzenia odbywała się w trybie NBD (Next Business Day)? Dla urządzeń wdrożonych w kastrze wysokiej dostępności taki tryb jest powszechnie stosowany i uznawany za wystarczający.

Odpowiedź:
Zamawiający podtrzymuje zapisy zawarte w OPZ.

DYREKTOR
Centrum Informatyki Statystycznej
Marcin Piekarek

Centrum Informatyki Statystycznej
Aleja Niepodległości 208, 00-925 Warszawa
tel. 22 608 31 44
cissek@stat.gov.pl
cis.stat.gov.pl