Wieprz, dnia 28.07.2022r.

OR.271.11.2022

Wykonawcy biorący udział w postępowaniu

Dotyczy:

Postepowania prowadzonego w trybie podstawowym bez negocjacji na:

Dostawa sprzętu informatycznego

realizowana w ramach projektu

„Cyfrowa Gmina"

Zamawiający działając na podstawie art. 284 ust. 2, 6 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U.2021.1129 t.j. z dnia 2021.06.24) informuje o wypłynięciu zapytań od Wykonawców do SWZ oraz zamieszcza odpowiedzi:

Pytania z dnia 21.07.2022r.

Informujemy Zamawiającego, że po zapoznaniu się z treścią opublikowanego w dniu 15.07.2022 przetargu, „**CGRW - IT_załącznik 2_OPZ.docx (425,48 kB)"** Specyfikacji Warunków Zamówienia dotyczącej przetargu: **OR.271.11.2022** na „Dostawa sprzętu informatycznego realizowanym w ramach projektu „Cyfrowa Gmina" stwierdzamy, że część jej postanowień odnoszących się do opisu przedmiotu zamówienia została sporządzona w sposób naruszający przepisy ustawy Prawo Zamówień Publicznych art. 7 ust. l i art. 29 ust. 1-2. oraz, art. 30 ust. 4.
Na Zamawiającym, zgodnie z przepisami ustawy Prawo Zamówień Publicznych, spoczywa obowiązek przygotowania i przeprowadzenia postępowania o udzielenia zamówienia w sposób zapewniający zachowanie uczciwej konkurencji oraz równe traktowanie wykonawców.

Po analizie „**CGRW - IT_załącznik 2_OPZ.docx (425,48 kB)**" pkt „V.Zakup systemu ochrony danych UTM" i kontakcie z producentami rozwiązań z obszaru bezpieczeństwa sieci działającymi w Polsce lub posiadającymi swoje centrum serwisowe w Polsce, nie udało się nam znaleźć innego rozwiązania, które spełnia **łącznie punkt V podpunkty od 1 do 22** poza urządzeniem **FORTIGATE 60F firmy Fortinet**

A dla punkt VI podpunkty 1 do 22 poza urządzeniem **FORTIGATE 40F firmy Fortinet**

Wybrane wymogi opisane w **„„CGRW - IT_załącznik 2_OPZ.docx (425,48 kB" punkty V oraz VI** wskazują na jednego konkretnego dostawcę, w tym przypadku firmę FORTINET z rozwiązaniami Fortigate.

Dodatkowo, informujemy Zamawiającego, że zapisy o których mowa powyżej są wprost przepisane ze specyfikacji rozwiązań Fortigate https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf

również użyta nomenklatura, słownictwo oraz wydajność dla pakietów 512 UDP wykorzystywana jest tylko przez producenta Fortigate.
Również słowo AHB wskazuje na usługę ofertowaną tylko dla rozwiązań Fortigate.

Przykład nadużyć ze strony Zamawiającego:
(po lewej tabelka producenta Fortigate, a po prawej wymogi Zamawiającego – na żółto zaznaczone te spisane 1:1)
Punkt V OPZ – Fortigate 60F

	FG/FWF-60F
Firewall Throughput (1518/512/64 byte UDP)	10/10/6 Gbps
IPsec VPN Throughput (512 byte) [1]	6.5 Gbps
IPS Throughput (Enterprise Mix) [2]	1.4 Gbps
NGFW Throughput (Enterprise Mix) [2, 4]	1 Gbps
Threat Protection Throughput (Ent. Mix) [2, 5]	700 Mbps
Firewall Latency	3.3 µs
Concurrent Sessions	700,000
New Sessions/Sec	35,000
Firewall Policies	5,000
Max G/W to G/W IPSEC Tunnels	200
Max Client to G/W IPSEC Tunnels	500
SSL VPN Throughput	900 Mbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	200
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	630 Mbps
Application Control Throughput (HTTP 64K) [2]	1.8 Gbps

4	PARAMETRY WYDAJNOŚCIOWE:
1)	W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2)	Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3)	Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4)	Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.
5)	Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
6)	Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7)	Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps

Punkt VI OPZ – Fortigate 40F

	FG/FWF-40F
Firewall Throughput (1518/512/64 byte UDP)	5 / 5 / 5 Gbps
IPsec VPN Throughput (512 byte) [1]	4.4 Gbps
IPS Throughput (Enterprise Mix) [2]	1 Gbps
NGFW Throughput (Enterprise Mix) [2, 4]	800 Mbps
Threat Protection Throughput (Ent. Mix) [2, 5]	600 Mbps
Firewall Latency	2.97 µs
Concurrent Sessions	700,000
New Sessions/Sec	35,000
Firewall Policies	5,000
Max G/W to G/W IPSEC Tunnels	200
Max Client to G/W IPSEC Tunnels	250
SSL VPN Throughput	490 Mbps

4	PARAMETRY WYDAJNOŚCIOWE
1)	W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2)	Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3)	Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4)	Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.
5)	Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.
6)	Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.
7)	Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

W związku z powyższym wnioskujemy do Zamawiającego o dopuszczenie rozwiązań równoważnych dla punktów
Punkt V:

ARCHITEKTURA SYSTEMU
1. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, umożliwiającej rozbudowę do dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności conajmniej Active-Passive, o specyfikacji opisanej poniżej 2. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. 3. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
1. Metalowa obudowa typu desktop. 2. Obsługa nielimitowanej ilości hostów w sieci chronionej.

3. Minimalna liczba i typ interfejsów fizycznych:
   •System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000
   •Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
4. Minimalna liczba nowych połączeń na sekundę: 18 000
5. Minimalna liczba jednoczesnych połączeń: 300 000
6. Minimalna przepustowość Firewall: 4 Gbps
7. Minimalna przepustowość IPS: 2,4 Gbps
8. Minimalna przepustowość Threat Protection: 495 Mbps
9. Minimalna przepustowość IPSec VPN: 600 Mbps
10. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 200 GB SSD do celów logowania i raportowania lub musi istnieć możliwość wykorzystania karty SD do celów logowania i raportowania.

PODSTAWOWE FUNKCJE SYSTEMU OCHRONY	
Zarządzanie i utrzymanie	1. Rozwiązanie musi być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH. 2. Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej ping 3. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 4. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 5. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. 6. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego 7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników. 8. Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora. 9. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP 10. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3 11. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do

	tworzenia kopii zapasowych konfiguracji z zapisem do chmury producenta lub własnego serwera. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, tygodniowo oraz miesięcznie. 12. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware)
Zapora sieciowa, konfiguracja sieciowa oraz routing	1. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection. 2. Rozwiązanie musi umożliwiać budowanie reguł zapory sieciowych w oparciu o takie obiekty jak elementy jak host, sieć, interfejs, harmonogram, port, protokół, użytkownik, grupa użytkowników, metoda uwierzytelnienia 3. System musi umożliwiać budowanie reguł bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. 4. Rozwiązanie musi pozwolić na definiowanie własnych polityk NAT wraz z IP masquerading. 5. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection). 6. System musi zapewniać ochronę przed skanowaniem portów (portscan blocking). 7. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). 8. Rozwiązanie musi zapewniać obsługę routingu statycznego. 9. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, OSPF, BGP). 10. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z obsługą RSTP oraz MSTP. 11. System musi oferować funkcjonalność serwera DHCP lub DHCP Relay. 12. System musi oferować wsparcie dla IEEE 802.1Q VLAN z niezależnymi pulami DHCP. 13. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. 14. Rozwiązanie musi umożliwiać rozkładanie ruchu do Internetu w oparciu o wagi poszczególnych bram ISP. 15. Wymagane jest by rozwiązanie zapewniało obsługę modemu USB LTE np. jako łącze zapasowe . 16. Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). 17. Rozwiązanie musi dawać możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza. 18. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA

	(monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 19. Rozwiązanie musi dawać możliwość optymalizacji ruchu wychodzącego w dostępie do określonych usług. 20. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. 21. System musi dawać możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.
Podstawowe kształtowanie pasma oraz limity ilości danych	1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla użytkownika, hosta lub połączenia. 2. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
Autoryzacja użytkowników	1. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 100 kont. 2. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP 3. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory 4. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP. 5. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal. 6. Rozwiązanie musi posiadać wbudowany moduł zapewniający uwierzytelnianie na poziomie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 7. Metoda 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
Samoobsługowy portal dla użytkowników	1. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). 2. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta OpenVPN dla Windows, Mac OS X, Linux, iOS, Android 3. Rozwiązanie musi umożliwiać zmianę hasła.
Podstawowe opcje VPN	System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń: 1. Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK) 2. Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
OCHRONA SIECI	
IPS	1. Dodatkowy moduł ochrony klasy IPS z bazą minimum 1000 sygnatur. 2. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS. 3. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.

	4. Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur 5. System musi generować alerty w przypadku wykrycia ataku.
OCHRONA I KONTORLA WEB ORAZ APLIKACJI	
Ochrona i kontrola Web	1. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS. 2. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP. 3. Rozwiązanie musi zapewniać skanowanie AV plików w czasie rzeczywistym 4. Rozwiązanie musi oferować funkcję inspekcji z obsługą protokołu TLS 1.3 oraz z tzw. walidacją certyfikatów. 5. System musi filtrować pliki na podstawie MIME. 6. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch. 7. Rozwiązanie musi zawierać przynajmniej 50 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www. 8. Rozwiązanie musi zapewniać możliwość blokowanie i wysyłania treści poprzez HTTP i HTTPS. 9. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego.
Ochrona i kontrola aplikacji	1. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji. 2. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook) 3. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
Kształtowanie pasma dla Web i Aplikacji	1. Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download. 2. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu. 3. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym.
OCHRONA ANTYWIRUSOWA	
Ochrona i kontrola Email	1. Rozwiązanie musi oferować możliwość trybu pracy Transparent Email Proxy 2. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S. 3. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.

	4. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń. 5. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników. 6. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL. 7. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów email. 8. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka.
OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY	
On-cloud Sandboxing	Rozwiązaniem musi dawać możliwość rozbudowy o dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności: 1. Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych np., .exe 2. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf. 3. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf. 4. Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym zip, arj, lha, rar, cab 5. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows .
LOGOWANIE I RAPORTOWANIE	
	1. System musi umożliwiać składowanie oraz archiwizację logów. 2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. 3. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących. 4. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych). 5. Rozwiązanie musi generować raporty w HTML i CSV. 6. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog. 7. System musi zapewniać podgląd wykorzystania łącza internetowego. 8. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP 9. Rozwiązanie musi oferować możliwość zanonimizowania danych.

Punkt VI:

ARCHITEKTURA SYSTEMU
4. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, umożliwiającej rozbudowę do dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności conajmniej Active-Passive, o specyfikacji opisanej poniżej 5. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. 6. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
11. Metalowa obudowa typu desktop. 12. Obsługa nielimitowanej ilości hostów w sieci chronionej. 13. Minimalna liczba i typ interfejsów fizycznych: •System realizujący funkcję Firewall musi dysponować minimum 12 interfejsami miedzianymi Ethernet 10/100/1000 •Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q. 14. Minimalna liczba nowych połączeń na sekundę: 25 000 15. Minimalna liczba jednoczesnych połączeń: 500 000 16. Minimalna przepustowość Firewall: 7,9 Gbps 17. Minimalna przepustowość IPS: 3,2 Gbps 18. Minimalna przepustowość Threat Protection: 1 Gbps 19. Minimalna przepustowość IPSec VPN: 1,3 Gbps 20. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 200 GB SSD do celów logowania i raportowania

PODSTAWOWE FUNKCJE SYSTEMU OCHRONY	
Zarządzanie i utrzymanie	13. Rozwiązanie musi być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH. 14. Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej ping 15. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 16. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 17. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.

	18. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego 19. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników. 20. Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora. 21. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP 22. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3 23. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do chmury producenta lub własnego serwera. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, tygodniowo oraz miesięcznie. 24. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware)
Zapora sieciowa, konfiguracja sieciowa oraz routing	22. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection. 23. Rozwiązanie musi umożliwiać budowanie reguł zapory sieciowych w oparciu o takie obiekty jak elementy jak host, sieć, interfejs, harmonogram, port, protokół, użytkownik, grupa użytkowników, metoda uwierzytelnienia 24. System musi umożliwiać budowanie reguł bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. 25. Rozwiązanie musi pozwolić na definiowanie własnych polityk NAT wraz z IP masquerading. 26. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection). 27. System musi zapewniać ochronę przed skanowaniem portów (portscan blocking). 28. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). 29. Rozwiązanie musi zapewniać obsługę routingu statycznego. 30. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, OSPF, BGP). 31. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z obsługą RSTP oraz MSTP. 32. System musi oferować funkcjonalność serwera DHCP lub DHCP Relay. 33. System musi oferować wsparcie dla IEEE 802.1Q VLAN z niezależnymi pulami DHCP. 34. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym

	przełączaniem ruchu w przypadku awarii łącza. 35. Rozwiązanie musi umożliwiać rozkładanie ruchu do Internetu w oparciu o wagi poszczególnych bram ISP. 36. Wymagane jest by rozwiązanie zapewniało obsługę modemu USB LTE np. jako łącze zapasowe . 37. Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). 38. Rozwiązanie musi dawać możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza. 39. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 40. Rozwiązanie musi dawać możliwość optymalizacji ruchu wychodzącego w dostępie do określonych usług. 41. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. 42. System musi dawać możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.
Podstawowe kształtowanie pasma oraz limity ilości danych	3. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla użytkownika, hosta lub połączenia. 4. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
Autoryzacja użytkowników	8. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 100 kont. 9. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP 10. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory 11. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP. 12. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal. 13. Rozwiązanie musi posiadać wbudowany moduł zapewniający uwierzytelnianie na poziomie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 14. Metoda 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
Samoobsługowy portal dla użytkowników	4. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). 5. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta OpenVPN dla Windows, Mac OS X, Linux, iOS, Android 6. Rozwiązanie musi umożliwiać zmianę hasła.

Podstawowe opcje VPN	System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń: 3. Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK) 4. Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
OCHRONA SIECI	
IPS	6. Dodatkowy moduł ochrony klasy IPS z bazą minimum 1000 sygnatur. 7. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS. 8. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń. 9. Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur 10. System musi generować alerty w przypadku wykrycia ataku.
OCHRONA I KONTORLA WEB ORAZ APLIKACJI	
Ochrona i kontrola Web	10. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS. 11. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP. 12. Rozwiązanie musi zapewniać skanowanie AV plików w czasie rzeczywistym 13. Rozwiązanie musi oferować funkcję inspekcji z obsługą protokołu TLS 1.3 oraz z tzw. walidacją certyfikatów. 14. System musi filtrować pliki na podstawie MIME. 15. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch. 16. Rozwiązanie musi zawierać przynajmniej 50 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www. 17. Rozwiązanie musi zapewniać możliwość blokowanie i wysyłania treści poprzez HTTP i HTTPS. 18. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego.
Ochrona i kontrola aplikacji	4. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji. 5. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook) 6. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
Kształtowanie pasma dla Web i Aplikacji	4. Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download. 5. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.

	6. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym.
OCHRONA ANTYWIRUSOWA	
Ochrona i kontrola Email	9. Rozwiązanie musi oferować możliwość trybu pracy Transparent Email Proxy 10. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S. 11. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP. 12. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń. 13. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników. 14. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL. 15. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów email. 16. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka.
OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY	
On-cloud Sandboxing	Rozwiązaniem musi dawać możliwość rozbudowy o dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności: 6. Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych np., .exe 7. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf. 8. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf. 9. Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym zip, arj, lha, rar, cab 10. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows .
LOGOWANIE I RAPORTOWANIE	
	10. System musi umożliwiać składowanie oraz archiwizację logów. 11. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. 12. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.

	13. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych). 14. Rozwiązanie musi generować raporty w HTML i CSV. 15. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog. 16. System musi zapewniać podgląd wykorzystania łącza internetowego. 17. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP 18. Rozwiązanie musi oferować możliwość zanonimizowania danych.

W przypadku braku dopuszczenia rozwiązania równoważnego, zgłosimy sprawę do instytucji finansującej projekt „Cyfrowa Gmina”.

<u>Odpowiedź Zamawiającego:</u> Według wiedzy Zamawiającego, wymagania opisane w opisie przedmiotu zamówienia dla systemu ochronnych danych UTM mogą być spełnione przez kilku producentów. Zamawiający nie może więc w całości uwzględnić wniosku Wykonawcy aby całkowicie zmienić minimalne wymagania dla systemu UTM, gdyż przesłana specyfikacja jest ukierunkowana na konkretny produkt jednej marki. Wykonawca nie podaje we wniosku które z opisanych funkcjonalności dla systemu UTM ograniczają możliwość złożenia oferty, tylko przesyła gotową specyfikację konkretnego produktu z prośbą o zmianę minimalnych wymagań. W związku z powyższym aby dodatkowo rozszerzyć krąg potencjalnych Wykonawców Zamawiający zmienia zapisy OPZ.

Signature Not Verified
Dokument podpisany przez Grzegorz Biela;
GMINA RADZIECHOWY-WIEPRZ
Data: 2022.07.28 15:46:37 CEST