Załącznik nr 1 do Umowy ZI/39/2023/U

OPIS PRZEDMIOTU ZAMÓWIENIA

WYMAGANIA OGÓLNE	
W ramach postępowania wymaganym jest dostarczenie oprogramowania na stacje końcowe, zapewniającego bezpieczne połączenie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN z zaporą UTM Zamawiającego. Zamawiający jest w posiadaniu rozwiązania „FortiGate-600E HA". Oferowane rozwiązanie musi również podnosić bezpieczeństwo przed cyberatakami, posiadając funkcje zgodne z poniższymi wymaganiami.	
ADMINISTRACJA ZDALNA	
Oferowane rozwiązanie musi być dostarczone wraz z konsolą, pozwalającą na centralne zarządzanie ustawieniami oferowanego oprogramowania, zainstalowanego na stacjach końcowych. Konsola musi również wspierać tworzenie i zdalną dystrybucję przez administratora pakietów instalacyjnych, a także pozwalać na wybór funkcji, które gotowy pakiet instalacyjny ma zawierać i które docelowo mają znaleźć się na stacji końcowej. Konsola musi wspierać instalację na systemie Microsoft Windows Server 2012R2 lub nowszych wersji.	
MINIMALNE WYMAGANIA	
LICENCJE TYP1	
Liczba sztuk	50
Ochrona i funkcje dla stacji roboczych	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7 (32-bit i 64-bit), Windows 8 (32-bit i 64-bit), Windows 8.1 (32-bit i 64-bit), Windows 10 (32-bit i 64-bit), Windows 11 (64-bit), Windows Server 2012 i nowsze), macOS (11+, 10.15, 10.14), iOS (wersja 9 i nowsze), Android (wersja 5 i nowsze) oraz Linux (Ubuntu 16.04 i nowszy, RedHat 7.4 i nowszy, CentOS 7.4 i nowszy). 2. Połączenie VPN miedzy stacją końcową, a zaporą Zamawiającego musi być nawiązane automatycznie, przed logowaniem do systemu Windows. 3. W przypadku błędu lub niepowodzenia połączenia VPN IPsec, oferowane rozwiązanie musi automatycznie podjąć próbę nawiązania połączenia tunelem VPN SSL. 4. Strony internetowe na komputerach muszą być filtrowane przed niebezpiecznymi i nieodpowiednimi treściami. Administrator musi mieć możliwość ustawienia filtru tak, by działał on w jednym z czterech zakresów: a. Blokowania witryn uznanych za nieodpowiednie b. Dopuszczenia wybranych stron c. Monitorowania odwiedzanych przez użytkowników stron d. Ostrzegania administratora o wejściu przez użytkownika na witrynę, znajdujących się na filtrowanej liście 5. Filtr stron internetowych musi mieć minimum 85 predefiniowanych filtrów i kategorii (w tym kategorii stron zabronionych prawem – Hazard), a także opcję przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 6. Oferowane oprogramowanie musi stale monitorować wersje zainstalowanych aplikacji oraz systemu operacyjnego na stacji końcowej, a w przypadku pojawienia się nowszej wersji (aktualizacji), musi

	automatycznie ją zainstalować. Administrator musi mieć także możliwość wykluczenia wybranych aplikacji lub systemów z automatycznej instalacji aktualizacji. 7. Rozwiązanie musi przekazywać informacje o uruchomionych na stacji końcowej procesach/aplikacjach, rodzaju i wersji systemu operacyjnego, zalogowanej domeny, certyfikatach i kluczach w rejestrze do posiadanej przez Zamawiającego zapory UTM, by na podstawie przesłanych informacji dynamicznie przypisywać polityki na zaporze UTM Zamawiającego. 8. Oferowane rozwiązanie musi posiadać funkcje chroniące stacje końcowe przed szkodliwym oprogramowaniem (w tym przed ransomware) 9. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 10. W ramach logowania oferowane oprogramowanie musi zapewniać przekazywanie danych o ruchu sieciowym i wykrytych podatnościach na stacjach końcowych. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 11. Oferowane rozwiązanie musi wspierać następujące formy autentykacji: a. RADIUS b. LDAP c. Lokalna baza danych d. xAuth e. TACACS+ f. Certyfikat (format X509) g. Tokeny mobilne i sprzętowe
Certyfikaty	Oferowany producent musi być rekomendowany przez laboratoria NSS Labs, a także posiadać certyfikat AV Comapratives oraz VB100 (Virus Bulletin).
Serwisy i licencje	Wykonawca musi dostarczyć licencje na oprogramowanie klienckie VPN dla 50 urządzeń na okres 12 miesięcy, zgodnych funkcjonalnie z powyższym opisem.
Gwarancje i wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, ramach którego producent musi zapewniać dostęp do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
LICENCJE TYP2	
Liczba sztuk	100
Ochrona i funkcje dla stacji roboczych	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7 (32-bit i 64-bit), Windows 8 (32-bit i 64-bit), Windows 8.1 (32-bit i 64-bit), Windows 10 (32-bit i 64-bit), Windows 11 (64-bit), Windows Server 2012 i nowsze), macOS (11+, 10.15, 10.14), iOS (wersja 9 i nowsze), Android (wersja 5 i nowsze) oraz Linux (Ubuntu 16.04 i nowszy, RedHat 7.4 i nowszy, CentOS 7.4 i nowszy). 2. Połączenie VPN miedzy stacją końcową, a zaporą Zamawiającego musi być nawiązane automatycznie, przed logowaniem do systemu Windows. 3. W przypadku błędu lub niepowodzenia połączenia VPN IPsec, oferowane rozwiązanie musi automatycznie podjąć próbę nawiązania połączenia tunelem VPN SSL. 4. Strony internetowe na komputerach muszą być filtrowane przed niebezpiecznymi i nieodpowiednimi treściami. Administrator musi mieć

	możliwość ustawienia filtru tak, by działał on w jednym z czterech zakresów: a. Blokowania witryn uznanych za nieodpowiednie b. Dopuszczenia wybranych stron c. Monitorowania odwiedzanych przez użytkowników stron d. Ostrzegania administratora o wejściu przez użytkownika na witrynę, znajdujących się na filtrowanej liście 5. Filtr stron internetowych musi mieć minimum 85 predefiniowanych filtrów i kategorii (w tym kategorii stron zabronionych prawem – Hazard) , a także opcję przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 6. Oferowane oprogramowanie musi stale monitorować wersje zainstalowanych aplikacji oraz systemu operacyjnego na stacji końcowej, a w przypadku pojawienia się nowszej wersji (aktualizacji), musi automatycznie ją zainstalować. Administrator musi mieć także możliwość wykluczenia wybranych aplikacji lub systemów z automatycznej instalacji aktualizacji. 7. Rozwiązanie musi przekazywać informacje o uruchomionych na stacji końcowej procesach/aplikacjach, rodzaju i wersji systemu operacyjnego, zalogowanej domeny, certyfikatach i kluczach w rejestrze do posiadanej przez Zamawiającego zapory UTM, by na podstawie przesłanych informacji dynamicznie przypisywać polityki na zaporze UTM Zamawiającego. 8. W ramach logowania oferowane oprogramowanie musi zapewniać przekazywanie danych o ruchu sieciowym i wykrytych podatnościach na stacjach końcowych. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 9. Oferowane rozwiązanie musi wspierać następujące formy autentykacji: a. RADIUS b. LDAP c. Lokalna baza danych d. xAuth e. TACACS+ f. Certyfikat (format X509) g. Tokeny mobilne i sprzętowe
Certyfikaty	Oferowany producent musi być rekomendowany przez laboratoria NSS Labs, a także posiadać certyfikat AV Comapratives oraz VB100 (Virus Bulletin).
Serwis i licencje	Wykonawca musi dostarczyć licencje na oprogramowanie klienckie VPN dla 100 urządzeń na okres 12 miesięcy, zgodnych funkcjonalnie z powyższym opisem.
Gwarancje i wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, ramach którego producent musi zapewniać dostęp do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.