Załącznik nr 4 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiot zamówienia obejmuje zakup i dostawę urządzeń typu UTM na wyposażenie jednostek organizacyjnych Gminy Mikołów – Centrum Usług Wspólnych w Mikołowie oraz jednostek obsługiwanych w ramach Programu „Cyberbezpieczny Samorząd" współfinansowanego przez Unię Europejską w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.
2. Dostawa obejmuje fabrycznie nowe, oryginalnie zapakowane, nieużywane, wolne od wad fizycznych i prawnych urządzenia wraz z wszelkimi akcesoriami niezbędnymi do prawidłowego działania (okablowanie, zasilacze itp.), bez wcześniejszej eksploatacji. Przedmiot zamówienia musi spełniać warunki opisane w niniejszej specyfikacji oraz w prawie powszechnie obowiązującym. Zamawiający wymaga, aby przedmiot zamówienia nie był przedmiotem praw osób trzecich. Zamawiający wyklucza dostawę sprzętu powystawowego. Zamawiający wymaga aby dostarczone urządzenia wyprodukowane były nie wcześniej niż w 2023 r.
3. Wykonawca zobowiązuje się dostarczyć sprzęt bezpośrednio na adres użytkownika końcowego - jednostki organizacyjnej Gminy Mikołów, której zostanie on przekazany przez Gminę: Centrum Usług Wspólnych w Mikołowie, ul. K. Miarki 9, 43 – 190 Mikołów, w dniach urzędowania i godzinach ustalonych na etapie realizacji umowy z Zamawiającym, ale nie później niż do godz. 13:00.
4. Kompatybilność - urządzenie UTM Centralny zapewni bezproblemową współpracę z urządzeniami typu UTM Klient w zakresie zestawiania i utrzymywania połączeń VPN oraz VLAN (zalecane rozwiązanie jednego producenta).
5. Konfiguracja dostarczonych urządzeń po stronie Zamawiającego.
6. Zamawiający wymaga przeszkolenia z obsługi i zarządzania dostarczonymi urządzeniami. Dopuszcza się przeprowadzenie szkolenia online. Termin szkolenia zostanie ustalony pomiędzy Zamawiającym, a Wykonawcą po dostarczeniu urządzeń, przy czym szkolenie należy przeprowadzić w terminie miesiąca licząc od dnia dostawy urządzeń do Zamawiającego.
7. Zamawiający wymaga gwarancji nie krótszej niż 24 miesiące licząc od daty protokolarnego odbioru przedmiotu umowy, z możliwością jej przedłużenia.

PARAMETRY SPRZĘTOWE UTM – Centralny – sztuk: 1

1. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB.
2. Urządzenie wyposażone jest w redundantne zasilanie.
3. Liczba portów Ethernet (RJ-45, Standard 10/100/1000 lub szybszych) – min. 6.
4. Port umożliwiający podłączenie światłowodu o przepustowości min. 10 Gbps – min. 2.
5. Firewall musi dysponować minimum 2 portami WAN o przepustowości minimum 1Gbps.
6. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.

7. Urządzenie musi być wyposażone w co najmniej jeden port konsolowy typu RJ45, z opcjonalnymi dodatkowymi portami konsolowymi.
8. Przepustowość Firewall – minimum 18Gbps.
9. Przepustowość Firewall wraz z włączonym systemem IPS – minimum 5Gbps.
10. Przepustowość filtrowania Antywirusowego – minimum 2,5Gbps.
11. Liczba tuneli VPN IPSec – minimum 1 000.
12. Obsługa interfejsów 802.1q (VLAN) – TAK.
13. Liczba równoczesnych sesji – minimum 1 000 000 i nie mniej niż 50 000 nowych sesji/sekundę.
14. Urządzenie musi być wyposażone w moduł TPM.
15. Liczba tras statycznego routingu – minimum 500.
16. Urządzenie UTM musi realizować wszystkie wymienione poniżej funkcje bezpieczeństwa.
17. Urządzenie w obudowie umożliwiającej montaż w szafie RACK 19''. Wraz z urządzeniem Wykonawca dostarczy elementy potrzebne do montażu urządzenia w szafie RACK 19 ''(max 2U).

PARAMETRY SPRZĘTOWE UTM – Klient – sztuk: 21

1. Urządzenie ma być wyposażone w dysk SSD lub w wypadku zastosowania dysku zewnętrznego, pendrive lub karty pamięci SD, wykonawca wraz z urządzeniem dostarczy kartę SD, pendrive lub zewnętrzny dysk o pojemności minimum 64 GB do urządzenia.
2. Liczba portów Ethernet (RJ-45, 10/100/1000 lub szybszych) – min. 8.
3. Port umożliwiający podłączenie światłowodu o przepustowości min. 1 Gbps – min. 1.
4. Przepustowość Firewall – minimum 4 Gbps.
5. Przepustowość Firewall wraz z włączonym systemem IPS – minimum 1 Gbps.
6. Liczba tuneli VPN IPSec – minimum 100.
7. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.
8. Urządzenie UTM musi realizować wszystkie wymienione poniżej funkcje bezpieczeństwa. Urządzenie w obudowie umożliwiającej montaż w szafie RACK 19''. Wraz z urządzeniem Wykonawca dostarczy elementy potrzebne do montażu urządzenia w szafie RACK 19 ''(max 2U). Dopuszczalna jest obudowa inna niż do montażu RACK 19", jednakże Zamawiający wymaga dostarczenia elementów (półki) umożliwiającej montaż w szafie RACK.

Wymagania wspólne dla wszystkich zamawianych urządzeń UTM:

OBSŁUGA SIECI

Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection, ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT, urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge), Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP.
Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos, ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

INTRUSION PREVENTION SYSTEM (IPS)

System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe, ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia, ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.

OCHRONA ANTYWIRUSOWA

Skaner antywirusowy ma być dostarczany w ramach podstawowej licencji.
Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.

OCHRONA ANTYSPAM

Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
Ochrona antyspam ma działać w oparciu o:
a) białe/czarne listy,
b) Skaner heurystyczny.

WIRTUALNE SIECI PRYWATNE (VPN)

Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
a) PPTP VPN lub nowszy,
b) IPSec VPN,
c) SSL VPN.
SSL VPN ma działać co najmniej w trybach tunelu i portalu.
Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal).
Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).

FILTR DOSTĘPU DO STRON WWW

Urządzenie ma posiadać wbudowany filtr URL.
Administrator ma mieć możliwość dodawania własnych kategorii URL, zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii.
Do wyboru ma być przynajmniej:
a) blokowanie dostępu do adresu URL,
b) zezwolenie na dostęp do adresu URL,
c) blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
Filtr URL musi uwzględniać komunikację po protokole HTTPS.
Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME, stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

UWIERZYTELNIANIE

Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
a) bazę użytkowników (LDAP),

b) usługę katalogową Microsoft Active Directory.
Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:

a) równoważenie względem adresu źródłowego,
b) równoważenie względem połączenia.

Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).

ROUTING (TRASOWANIE)

Urządzenie ma umożliwiać statyczne trasowanie pakietów, trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing), dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami, zarządzenie z poziomu konsoli (SSH).
Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup, musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS), eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:

a) manualnego eksportu do pliku w dowolnym momencie czasu,

b) automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu.
Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania, ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego, ma umożliwiać eksport wyników raportu.

POZOSTAŁE USŁUGI I FUNKCJE

Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny), ma posiadać usługę DNS Proxy.
Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.

SERWISY I LICENCJE

W ramach zamówienia Wykonawca dostarczy licencje aktywacyjne dla wymienionych przez Zamawiającego funkcjonalności, uprawniające do używania ww. funkcji oraz pobierania aktualizacji baz zabezpieczeń przez okres minimum 2 lat licząc od dnia aktywacji.

DYREKTOR Centrum Usług Wspólnych w Mikołowie

Signed by / Podpisano przez:
Aleksandra Anna Czech
Date / Data:
2024-09-20 12:15