Wymagania funkcjonalne i systemowe dla urządzenia brzegowego typu firewall następnej generacji (NFGW).

Codziennie korzystamy z Internetu. Podatności, wirusy, ataki hakerów, włamania na konta pocztowe, phishing czy po prostu czynnik ludzki to tylko niektóre z istniejących zagrożeń. Nawet jeśli praca przy komputerze ogranicza się tylko do wysyłania, odbierania maili i przeglądania stron internetowych, warto zabezpieczyć się przed zagrożeniami, które mogą zainfekować naszą infrastrukturę informatyczną w efekcie przyczyniając się do utraty bądź wycieku danych osobowych, schematów, projektów czy po prostu know-how. Obserwowany w ostatnim czasie wzrost cyberzagrożeń sprawia, że rynek cybersecurity rozwija się coraz bardziej. Jednym ze sposobów walki z atakami są zapory sieciowe nowej generacji znane jako NGFW (ang. Next Generation Firewall). Jest to jeden z klasycznych sposobów zabezpieczania sieci i systemów przed intruzami. Zapewnia kompleksową ochronę przed zagrożeniami dodatkowo usprawniając zarządzanie bezpieczeństwem oraz minimalizuje ryzyka związane z wyciekiem danych. Systemy klasy NGFW są bardzo wydajne, inteligentne oraz wymagające zupełnie innego podejścia do roli, jaką mają odgrywać w kwestii bezpieczeństwa. Dokonują analizy ruchu sieciowego za pomocą skomplikowanych algorytmów, rejestrując wszelkie próby ataku oraz automatycznie podejmując działania obronne angażując w ten proces dostępne dla niego narzędzia w chmurze producenta czy sztuczną inteligencję. Wszelkie niebezpieczne incydenty są rejestrowane, a system informuje o takich zdarzeniach na bieżąco.

Jako firma chcemy aby nasza sieć była chroniona nie tylko od zewnątrz ale także od wewnątrz dlatego NGFW powinien być dostarczony w formie dedykowanego systemu i co za tym idzie musi zapewniać:

- ochronę przed nieuprawnionym wyciekiem danych z sieci lokalnej,
- analizę ruchu wchodzącego i wychodzącego,
- zapisywanie logów (filtrowanie połączeń przychodzących i wychodzących),
- kontrolę ruchu sieciowego w oparciu o analizę używanych aplikacji i przy zastosowaniu różnych polityk bezpieczeństwa,
- mechanizm identyfikacji i kontroli aplikacji niezależnie od portu,
- inspekcję danych sieciowych z wykorzystaniem analizy zagrożeń,
- na bieżąco aktualizowane oprogramowanie wewnętrzne (firmware),
- możliwość nawiązania połączenia VPN oraz posiadać dedykowanego do tego celu klienta,
- nie obciążać nadmiernie przepustowości ruchu sieciowego,

1. Ogólne założenia projektu

- System ma zapewnić połączenia oddziału Starachowickiego z oddziałem w Sokołowie. Pomiędzy lokalizacjami musi być zapewnione szyfrowanie AES 256-bit. Zakres projektu obejmuje dostawę niezbędnego sprzętu, oprogramowania, licencji oraz instalację i konfigurację systemu zgodnie z wymaganiami Zamawiającego.
- Produkt musi zapewniać zaawansowaną heurestykę zagrożeń w sieci w oparciu chmurę i sztuczną inteligencję będącą uzupełnieniem zainstalowanego oprogramowania antywirusowego. Ma to na celu zapewnienie ochrony infrastruktury sieciowej.

- Logowanie ruchu sieciowego przynajmniej w cyklach tygodniowych, z możliwością backupu i przeglądania historii zapisanych logów przynajmniej do 3 miesięcy wstecz.
- Polityki bezpieczeństwa w systemie mają pozwalać na kontrolę ruchu przychodzącego i wychodzącego na poziomie aplikacji odwiedzanych stron, adresów IP oraz protokołów sieciowych i portów. Przez kontrolę rozumie się także możliwość przeglądania ruchu sieciowego i inspekcji zagrożeń w czasie rzeczywistym

2. Wymagane integracje

- Integracja logowania jednokrotnego firmy (SSO) z usługą SSL VPN. Rozumie się przez to integrację z Active Directory na zasadzie utworzenia grupy domenowej – tylko użytkownicy domenowi dodani do tej grupy mają mieć możliwość połączenia się z VPN-em.
- Ogólna współpraca z serwerem po LDAP z zainstalowanym systemem Windows Server 2019/2022.

3. Wymagania dodatkowe

- Zapewnienie możliwości nawiązania połączenia VPN poprzez dedykowanego do tego celu klienta. Klient musi być dostępny przynajmniej na systemy Windows, macOS oraz urządzenia mobilne.
- Możliwość dodania w przyszłości uwierzytelniania 2FA na zasadzie tokenu mobilnego dostępnego na urządzenia mobilne.
- Zagwarantowane automatyczne aktualizacje oprogramowania, systemu, baz i sygnatur w okresie przynajmniej 36 miesięcy do uruchomienia.
- Dostępne wsparcie techniczne w języku polskim lub angielskim z odpowiednim dla firmy poziomem SLA tj. dla krytycznego błędu czas odpowiedzi powinien wynosić 1h, a dla zwykłych przypadków – następny dzień roboczy.
- Dostęp do dokumentacji technicznej w języku polskim lub angielskim, tak aby w prosty sposób można było przeprowadzić zmianę ustawień.
- Możliwość backupu systemu i łatwego przeniesienia konfiguracji na nowe urządzenie.
- Możliwość wdrożenia mechanizmu DLP (ang. Data Leak Protection) z poziomu systemu.
- Dostarczony system musi być poparty odpowiednim portfolio produktu i wieloletnim doświadczeniem producenta.
- Dostawca musi posiadać doświadczenie w prowadzeniu podobnych projektów i odpowiedni zespół specjalistów/inżynierów.
- Szkolenie dwóch administratorów systemu w pełnym wymiarze obsługi i konfiguracji urządzeń.
- Wsparcie techniczne dostarczonego systemu w okresie 24 miesięcy od uruchomienia.

4. Wymagane parametry systemu

Minimalne parametry określa poniższa tabela – są to wymagania zrobione przez wcześniejsze zwymiarowanie sieci czyli tzw. „sizing”.

Liczba portów RJ45	Nie mniej niż 8
Liczba portów RJ45 zarządzalnych	Nie mniej niż 2
Liczba slotów SFP	Nie mniej niż 8
Liczba portów SFP+	Nie mniej niż 4
Liczba portów USB	Nie mniej niż 1
Port konsolowy	Nie mniej niż 1
Trusted Platform Module (TPM)	TAK
Bluetooth Low Energy (BLE)	TAK
Przepustowość IPS w Gbps	Nie mniej niż 5 Gbps
Przepustowość FW (firewalla) w Gbps	Nie mniej niż 3 Gbps
Przepustowość wykrywania zagrożeń w Gbps	Nie mniej niż 2 Gbps
Przepustowość FW (1518 / 512 / 64 bajtów, pakiety UDP) w Gbps	Nie mniej niż 24 / 24 / 24 Gbps
Opóźnienia firewalla (64 bajtów, pakiety UDP)	Dopuszczalne 5 µs
Przepustowość FW (firewalla) w pakietach na sekundę w Mpps	Nie mniej niż 40 Mpps
Aktywne sesje (TCP)	Nie mniej niż 3 000 000
Nowe sesje na sekundę (TCP)	Nie mniej niż 140 000
Maksymalna ilość polityk dla firewalla	Nie mniej niż 10 000
Przepustowość dla IPsec VPN (512 byte) w Gbps	Nie mniej niż 35 Gbps
Maksymalna ilość tuneli Gateway-to-Gateway IPsec VPN	Nie mniej niż 2000
Maksymalna ilość tuneli Client-to-Gateway IPsec VPN	Nie mniej niż 16 000
Przepustowość dla SSL-VPN w Gbps	Nie mniej niż 1 Gbps
Liczba jednoczesnych połączeń SSL-VPN	Nie mniej niż 500
Przepustowość filtrowania dla SSL w Gbps	Nie mniej niż 3 Gbps
Przepustowość filtrowania dla SSL w sesjach na sekundę	Nie mniej niż 2000
Jednoczesne sesje filtrowania dla SSL	Nie mniej niż 300 000
Przepustowość kontroli dla aplikacji w Gbps	Nie mniej niż 5 Gbps
Obudowa typu rack	TAK
Redundantny zasilacz	TAK
Możliwość odkładania logów	TAK
Antywirus + URL filtering	TAK
Możliwość integracji z AD na zasadzie grupy (VPN)	TAK
Możliwość dodania tokenu 2FA dla połączeń zdalnych (VPN)	TAK