Okręgowy Urząd Miar w Szczecinie

Szczecin, dnia 25 sierpnia 2021 r.

Znak sprawy: RA.241.68.2021

Znak pisma: RA.4652.2021.AR

Okręgowy Urząd Miar w Szczecinie zwraca się z prośbą o przesłanie do dnia 30 sierpnia 2021 r. oferty cenowej na dostawę **urządzeń UTM Stormshield SN310 z licencjami UTM Security Pack + Kaspersky Antywirus + Breach Fighter – sandboxing – 5 szt. lub równoważnych spełniających następujące minimalne wymagania:**

- Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
- System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000.
- Możliwość tworzenia minimum 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
- W zakresie Firewall'a obsługa nie mniej niż 200 tys. jednoczesnych połączeń oraz 15 tys. nowych połączeń na sekundę.
- System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
- W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:
    - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    - Ochrona przed wirusami – komercyjny antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). System AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.
    - Poufność danych - IPSec VPN oraz SSL VPN
    - Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]

Okręgowy Urząd Miar w Szczecinie
pl. Lotników 4/5
70-414 Szczecin
tel.: 91 434 75 66
fax: 91 434 75 98
e-mail: oum.szczecin@poczta.gum.gov.pl
szczecin.gum.gov.pl

    - Kontrola stron Internetowych – Web Filter [WF]
    - Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3)
    - Kontrola pasma oraz ruchu [QoS i Traffic shaping]
    - Kontrola aplikacji oraz rozpoznawanie ruchu P2P
    - Analiza ruchu szyfrowanego protokołem SSL
- Wydajność systemu Firewall minimum 3 Gbps
- Wydajność ochrony przed atakami (IPS) minimum 2,4 Gbps
- Wydajność VPN IPSec, nie mniej niż 450 Mbps
- W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
    - Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site
    - Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    - Praca w topologii Hub and Spoke oraz Mesh
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth
    - Obsługa ssl vpn w trybach portal oraz tunel
- Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
- Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
- Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
- Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
- Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
- Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
- Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

Okręgowy Urząd Miar
w Szczecinie
pl. Lotników 4/5
70-414 Szczecin
tel.: 91 434 75 66
fax: 91 434 75 98
e-mail: oum.szczecin@poczta.gum.gov.pl
szczecin.gum.gov.pl

- Baza filtra WWW pogrupowana w minimum 50 kategorii tematycznych. Administrator musi mieć możliwość tworzenia wyjątków i reguł omijania filtra WWW.
- Automatyczne ściąganie sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
- System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
    - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
    - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
    - Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych
    - Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny
- W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż:
    - Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego
    - Generowanie co najmniej 25 różnych typów raportów
- System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania
- Wymaga się dostarczenie odrębnego systemu do zbierania logów pochodzącego od producenta rozwiązania, który pozwoli na zbieranie logów z wszystkich rozwiązań NGFW – centralny kolektor logów – co najmniej jako obraz maszyny wirtualnej.
- Urządzenie musi:
    - posiadać certyfikat Common Criteria EAL4+
    - posiadać certyfikat ICSA Labs dla funkcji: VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE
- Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
- Konsola administracyjna musi być w języku polskim
- Wymaga się, aby dostawa obejmowała również:

Okręgowy Urząd Miar
w Szczecinie
pl. Lotników 4/5
70-414 Szczecin
tel.: 91 434 75 66
fax: 91 434 75 98
e-mail: oum.szczecin@poczta.gum.gov.pl
szczecin.gum.gov.pl

- Minimum 12-miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu.
- Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 12 miesięcy liczoną od dnia zakończenia wdrożenia całego systemu.

Okręgowy Urząd Miar
w Szczecinie
pl. Lotników 4/5
70-414 Szczecin
tel.: 91 434 75 66
fax: 91 434 75 98
e-mail: oum.szczecin@poczta.gum.gov.pl
szczecin.gum.gov.pl