1. **DIS System automatyzacji backupów konfiguracji firewall**

# Opis techniczny rozwiązania

Zakup subskrypcji i wdrożenie systemu automatyzacji realizacji kopii zapasowych konfiguracji urządzeń bezpieczeństwa sieciowego.

Oprogramowanie Backbox z licencjami pozwalającymi na obsługę:

1. 2 klastry firewalli Check Point (centralne część rozwiązań dostępu do sieci Internet oraz VPN),
2. 2 klastry firewalli Palo Alto (firewall brzegowy DC Energa),
3. 5 klastrów urządzeń F5 Networks (ochrona serwisów publikowanych w sieci Internet przez Grupę Energa),
4. 8 firewalli Paloalto (firewalle Energa Operator w sieci LAN),
5. 80 pojedynczych firewalli Check Point serii 1500 (obsługujące zdalne biura przyłączone połączeniami site-to-site).

Poniższa tabela prezentuje zestawienie niezbędnych licencji:

|  |  |  |
| --- | --- | --- |
| **Nr katalogowy** | **Opis** | **Ilość** |
| BBX-TS-PR-ND | BackBox Subscription Type-Specific Premium Network Device | 20 |
| BBX-TS-PR-SD | BackBox Subscription Type-Specific Premium Security Device | 103 |
| BBX-NVM | BackBox Vulnerability Intelligence Subscription | 123 |

# Zakres usługi Wdrożenia

1. Instalacja maszyny wirtualnej na środowisku wirtualnym VMware Zamawiającego,
2. Konfiguracja ustawień sieciowych,
3. Wgranie licencji,
4. Konfiguracja dostępów administracyjnych,
5. Konfiguracja ustawień systemowych (m.in. SMTP, SNMP, SYSLOG, NTP, LDAP, RADIUS),
6. Przygotowanie skanera Discovery do wykrywania nowych urządzeń,
7. Dodanie urządzeń do Backbox:
   1. 96 urządzeń Firewall ( w tym klastry HA oraz pojedyncze urządzenia),
   2. 20 routerów MPLS,
8. Konfiguracja harmonogramu wykonywania backupu konfiguracji urządzeń,
9. Konfiguracja polityk retencji backupów,
10. Konfiguracja wybranych backupów na zewnętrzny serwer Zamawiającego,
11. Ustawienie powiadomień email w przypadku błędów wykonania backupu,
12. Testy przywrócenie konfiguracji „restore” na urządzeniu wskazanym przez Zamawiającego,
13. Testy aktualizacji oprogramowania na urządzeniu wskazanym przez Zamawiającego,
14. Konfiguracja modułu automatycznego mapowania znanych podatności (CVE) do urządzeń,
15. Konfiguracja 5 reguł „IntelliChecks” wraz z włączoną automatyczną naprawą „remediation” - scenariusze zostaną ustalone na etapie wdrożenia,
16. Konfiguracja 5 zadań „Tasks” - scenariusze zostaną ustalone na etapie wdrożenia,
17. Konfiguracja 5 raportów wskazanych przez Zamawianego,
18. Przekazanie Dokumentacji Powykonawczej,
19. Szkolenie powdrożeniowe 6 godz. z wykonanej konfiguracji oraz administracji produktem.