**Akceptační kritéria pro části plnění a) – d), jež musí být ověřeny nejpozději v rámci milníku č. 4 dle Harmonogramu**

**Testy provedené dodavatelem**

* Firewall i managementy jsou nainstalované a plně funkční v DC1 i DC2.
* V obou lokalitách běží správné verze OS a GA hotfixů.
* SIC komunikace mezi managementy a firewally v obou DC je funkční.
* Plná synchronizace konfigurace a politik mezi DC1 (primární) a DC2 (sekundární) včetně všech Check Point kontextů (VS).
* ThreatPrevention politika „Recommended“ je nasazená a synchronizovaná v rámci všech kontextů.
* Try&buy licence byly během pilotu aktivní na všech systémech.
* Logy jsou úspěšně odesílány na log servery z obou DC.
* Lokální clustery jsou distribuovány na všechny SG členy v obou DC.
* Geo-cluster Active/Standby byl otestován – failover DC1 → DC2 → DC1 proběhl bez dopadu na provoz.
* Signatury i politiky se synchronizují mezi lokalitami včetně kontextů.
* SecureXL a CoreXL jsou aktivní a optimálně nakonfigurované.
* Všechny Check Point služby běží stabilně, Health Check bez kritických varování.
* Přístupová politika zákazníka je nasazena konzistentně v DC1 i DC2 v rámci všech kontextů.
* Pravidelné zálohy jsou nastaveny v obou lokalitách.
* Logy neobsahují kritické chyby ani přerušení funkcí.

**Testy provedené zákazníkem**

* Správná distribuce lokálních clusterů a geo-clusteru byla ověřena.
* **Check Point kontexty (VS)** a routování uvnitř kontextů jsou správně vytvořené a funkční v DC1 i DC2.
* Základní konfigurace managementu, firewallů a testovacích endpointů byla úspěšně ověřena.
* Aktivované blades a ThreatPrevention politika „Recommended“ byly potvrzeny ve všech kontextech.
* Události generované NGFW jsou logovány a dostupné z obou DC.

**Výkonové a funkční testy (včetně geo-failoveru)**

* IPSec a RA VPN byly otestovány v DC1 i po přepnutí na DC2 v rámci příslušných kontextů.
* Public + DMZ i Pobočky + DPL služby byly otestovány v DC1 i následně po geo-failoveru v DC2 — v obou případech s funkčními příslušnými kontexty.
* V zátěžových testech bylo dosaženo max. 70 % využití zdrojů při definovaných propustnostech včetně plné SSL inspekce.
* Simulovaný výpadek DC1 prokázal bezproblémové přesměrování provozu do DC2 (dedikovaná linka zůstala aktivní).

| **Požadavek** | **Parametr / Funkcionalita** | **Výsledek** |
| --- | --- | --- |
| 1 | Vysoký výkon a dostupnost při propustnosti >5 Gb/s (Public/DMZ) a >3 Gb/s (pobočky/DPL) v aktivním DC |  |
| 2 | Plná NGFW + NGTX funkcionalita v obou DC |  |
| 3 | Maestro Hyperscale orchestrace a clusterování v každém DC |  |
| 4 | Geo-redundance Active/Standby (DC1 ↔ DC2) přes dedikovanou linku s automatickou synchronizací a failoverem |  |
| 5 | Centrální management s českým GUI (primární + sekundární management) |  |
| 6 | Integrace do stávajícího SIEM z obou lokalit |  |
| 7 | Pilotní provoz s testy geo-failoveru DC1 ↔ DC2 |  |
| 8 | Výkonové a funkční testy všech služeb před i po geo-failoveru |  |
| 9 | Podpora 24×7 s garantovaným SLA výrobce |  |
| 10 | Kompatibilita HW/virtualizační platformy dle HCL v obou DC |  |