



Příloha č. 2 Technická specifikace projektu

Pro účely segmentace a zabezpečení síťového provozu požadujeme dodávku odpovídajících technologií, které splňují definované parametry.

Architektonická migrace bude krokem k centralizaci služeb všech subjektů v technické i procesní rovině. Proto je nutné koncipovat řešení jako homogenní a plně integrovatelné.

V lokalitách 1 a 2 je vyžadováno řešení s vysokou dostupností a schopností kapacitně pokrýt potřeby po architektonické migraci do dvou datacenter dle přiložených parametrů.

V lokalitách 3 a 4 je vyžadováno řešení s vysokou dostupností, přičemž se předpokládá umístění do datových center po architektonické migraci.

Účastník předloží architekturu řešení, včetně rozpisu položek a jejich cen pro pokrytí lokalit 1,2,3,4 dle technických parametrů.

Obecné požadavky

Výrobce FW řešení musí být umístěn v "Gartner quadrant for Network Firewalls" nejméně po dobu posledních tří let (2018, 2019, 2020) v Leaders quadrantu.

Certifikace - Zadavatel požaduje předložení certifikátu prokazující partnerství s výrobcem dodávané technologie a to na úrovni vyšší než „základní“.

Technické požadavky

Zadavatel požaduje splnění všech bodů z tabulky technických požadavků. Detaily k architektuře, způsobu zapojení a související technickou dokumentaci přiloží účastník výběrového řízení spolu s cenovou nabídkou a potvrzením výrobce použité technologie, že je autorizovaným prodejcem daného řešení.

Technické parametry pro lokality 1 a 2:

Požadovaná funkcionalita/vlastnost pro každou jednotlivou lokalitu
Požadované funkcionality / licence: L3/L4 firewall, IPS, maximální licenční set pro úplnou ochranu všech podporovaných typů datových toků.
Propustnost NGFW minimálně 22 Gbps, v případě výpadku jednoho HW firewall boxu.



Počet požadovaných fyzických síťových rozhraní použitelných pro připojení segmentů minimálně 4x 10GbE a 4x 100GbE.
Vysoce dostupné řešení bezpečnostních bran s možností režimu active-active.
Počet dodávaných licencí pro virtuální firewall instance, min. 10 ks.
Součástí řešení jsou klientské SSL VPN bez omezení počtu uživatelů.
Všechny prvky řešení musí být dodány formou appliances. Řešení formou virtuálních zařízení, nebo SW nastavba pro HW jiného výrobce nejsou přípustná.
Firewall musí být dodán jako funkční celek složený z komponent jednoho výrobce, a to včetně všech poskytovaných funkcionalit (např. typu IPS, AV, AS signatur, databází pro URL kategorizaci, sandbox definic, případně dalších).
Výrobce musí být zajištěno, že po dobu udržitelnosti investice musí být dodané zařízení podporováno výrobcem, tzn. nesmí spadat do kategorie zařízení, která jsou END OF SUPPORT .
FW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů a uživatelů.
FW musí být kompatibilní s 19" rozvaděčem.
FW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP).
FW musí obsahovat dva nezávislé redundantní zdroje napájení AC 230V.
FW musí obsahovat plnohodnotné textové rozhraní (CLI) pro správu, bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI musí podporovat šifrování.
FW musí obsahovat nativní nástroje pro debugging v úrovni L2 – L7 ISO/OSI modelu.
FW musí podporovat nativní nástroj pro odchycení provozu.



FW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu.
Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla.
Definovaná aplikace musí představovat "match kritérium" při policy lookup.
FW musí podporovat identifikaci aplikací napříč všemi porty/protokoly.
FW musí podporovat identifikaci aplikací na nestandardních portech.
FW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit.
Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla.
Uživatelská identita musí představovat "match kritérium" při policy lookup.

Technické parametry pro lokality 3 a 4:

Požadovaná funkcionalita/vlastnost pro každou jednotlivou lokalitu
Požadované funkcionality / licence: L3/L4 firewall, IPS, maximální licenční set pro úplnou ochranu všech podporovaných typů datových toků.
Propustnost NGFW minimálně 5 Gbps, v případě výpadku jednoho HW firewall boxu.
Počet požadovaných fyzických síťových rozhraní použitelných pro připojení segmentů minimálně 2x 10GbE.
Vysoce dostupné řešení bezpečnostních bran s možností režimu active-active.



Počet dodávaných licencí pro virtuální firewall instance, min. 10 ks.
Součástí řešení jsou klientské SSL VPN bez omezení počtu uživatelů.
Minimální počet současných síťových spojení je 2.000.000
Všechny prvky řešení musí být dodány formou appliances. Řešení formou virtuálních zařízení, nebo SW nastavba pro HW jiného výrobce nejsou přípustná.
Firewall musí být dodán jako funkční celek složený z komponent jednoho výrobce, a to včetně všech poskytovaných funkcionalit (např. typu IPS, AV, AS signatur, databází pro URL kategorizaci, sandbox definic, případně dalších).
Výrobce musí být zajištěno, že po dobu udržitelnosti investice musí být dodané zařízení podporováno výrobcem, tzn. nesmí spadat do kategorie zařízení, která jsou END OF SUPPORT .
FW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů a uživatelů.
FW musí být kompatibilní s 19" rozvaděčem.
FW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP).
FW musí obsahovat dva nezávislé redundantní zdroje napájení AC 230V.
FW musí obsahovat plnohodnotné textové rozhraní (CLI) pro správu, bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI musí podporovat šifrování.
FW musí obsahovat nativní nástroje pro debugging v úrovni L2 – L7 ISO/OSI modelu.
FW musí podporovat nativní nástroj pro odchycení provozu.
FW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu.



Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla.
Definovaná aplikace musí představovat "match kritérium" při policy lookup.
FW musí podporovat identifikaci aplikací napříč všemi porty/protokoly.
FW musí podporovat identifikaci aplikací na nestandardních portech.
FW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit.
Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla.
Uživatelská identita musí představovat "match kritérium" při policy lookup.

Technické parametry pro management:

Požadovaná funkcionální/vlastnost
Management pro minimální počet 10 FW clusterů.
Dodávka formou virtuálního serveru do infrastruktury zadavatele, nebo HW zařízení stejného výrobce jako FW řešení.
FW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem.



Implementace

Součástí projektu je kompletní implementace řešení v tomto rozsahu:

- tvorba solution design dokumentu pro začlenění technologie do infrastruktury
- definice harmonogramu a potřebné součinnosti ze strany zadavatele
- HW instalace zařízení do lokalit a propojení
- konfigurace základního systému a bezpečnostní hardening
- migrace konfigurací ze stávajících FW řešení
- nastavení bezpečnostních politik nad rámec původních pravidel - ladění IPS modulu atp.
- integrace s Active Directory pro práci s dynamickými objekty
- nastavení administrátorských rolí pro správce řešení
- konfigurace reportovacích nástrojů pro přehledové statistiky
- zaškolení administrátorů formou certifikovaného školení výrobce, nebo intenzivního kurzu v délce 4 pracovních dní
- předání kompletní provozní dokumentace
- úspěšné provedení funkčních a DR testů pro akceptaci řešení