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.

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.

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 (rozpad na minimálně 60 dílčích kategorií), sandbox definic, případně dalších).
Všechny prvky řešení musí být dodány formou appliances. Řešení formou virtuálních zařízení, nebo SW nástavba pro HW jiného výrobce nejsou přípustná.
Počet dodávaných licencí pro virtuální firewall instance, min. 10 ks.
Výrobcem 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 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 agregaci portů pomocí protokolu 802.3ad (LACP).
Možnost definice vlastních IPS pravidel/signatur nebo importu SNORT pravidel/signatur.
Podpora pro blokaci indikátorů kompromitace z externích zdrojů pomocí formátu csv, json, stix.
Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3.
Detekce a řízení síťových aplikaci. Minimální počet 3000 rozpoznaných aplikací.
Možnost filtrace provozu podle geoblastí/států. (GeoIP).
Podpora dynamického směrování protokolem OSPFv2 a OSPFv3.
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.
Ověření identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos). Využití identity uživatele v rámci nastavení bezpečnostních politik FW v režimu Single Sign On.
Možnost nastavení časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit.
IPSec S2S VPN, dle platných standardů pro možnost propojení se zařízeními třetích stran.
Součástí řešení jsou klientské IPSec a SSL VPN bez omezení počtu uživatelů.
HW musí být kompatibilní s 19“ rozvaděčem.
HW musí obsahovat dva nezávislé redundantní zdroje napájení AC 230V.

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.
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 (rozpad na minimálně 60 dílčích kategorií), sandbox definic, případně dalších).
Všechny prvky řešení musí být dodány formou appliances. Řešení formou virtuálních zařízení, nebo SW nástavba pro HW jiného výrobce nejsou přípustná.
Počet dodávaných licencí pro virtuální firewall instance, min. 10 ks.
Výrobcem 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**.
Minimální počet současných síťových spojení je 2.000.000.
FW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů a uživatelů.
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 agregaci portů pomocí protokolu 802.3ad (LACP).
Možnost definice vlastních IPS pravidel/signatur nebo importu SNORT pravidel/signatur.
Podpora pro blokaci indikátorů kompromitace z externích zdrojů pomocí formátu csv, json, stix.
Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3.
Detekce a řízení síťových aplikaci. Minimální počet 3000 rozpoznaných aplikací.
Možnost filtrace provozu podle geoblastí/států. (GeoIP).
Podpora dynamického směrování protokolem OSPFv2 a OSPFv3.
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.
Ověření identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos). Využití identity uživatele v rámci nastavení bezpečnostních politik FW v režimu Single Sigh On.
Možnost nastavení časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit.

IPSec S2S VPN, dle platných standardů pro možnost propojení se zařízeními třetích stran.
Součástí řešení jsou klientské IPSec a SSL VPN bez omezení počtu uživatelů.
HW musí být kompatibilní s 19“ rozvaděčem.
HW musí obsahovat dva nezávislé redundantní zdroje napájení AC 230V.

Technické parametry pro management:

Požadovaná funkcionalita/vlastnost
Management pro minimální počet 10 FW clusterů.
Jednotný centrální management, centrální správa politik, analýza logů. Management provozovaný na VM appliance.
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.
Pokročilá detekce hrozeb, včetně korelace incidentů.
Integrovaná reportovací funkcionalita – vytváření vlastních reportů přímo v grafickém rozhraní managementu. Možnost použití předpřipravených (šablon) reportů, možnost úprav jednotlivých komponent pro report (grafy, tabulky, texty, obrázky). Výstup reportu minimálně ve formátech html, pdf, csv.
Centrální ukládání logů, indexace, filtrace logů na úrovní všech napojených bezpečnostních zařízení (FW).
Eliminace vkládání dílčích pravidel přímo na jednotlivých FW mimo centrální management.

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.