Příloha č. 1 zadávací dokumentace
veřejné zakázky: „Dodávka zařízení NGIPS“

Technická specifikace

Na požadovaný systém NGIPS jsou kladeny tyto hlavní technické požadavky:

- Standardní set funkcí IPS první generace – poskytování transparentní ochrany proti zranitelnostem a exploitům se začleněním inspekce na cestě komunikace (in-line).
- Znalost a viditelnost do aplikace – schopnost identifikovat nepřátelské aplikace a prosazovat bezpečnostní politiky na aplikační vrstvě nezávisle na použitém portu či protokolu.
- Kontextové povědomí – schopnost zahrnout do rozhodování o blokování informace z vnějších zdrojů a aplikovat rozhodnutí s přihlédnutím ke geografické lokaci partnera síťové transakce, jeho reputaci a možným informacím z adresářových služeb.
- Povědomí o obsahu – schopnost kontrolovat a třídit příchozí a odchozí soubory, příkazy a celkově rozumět obsahu s hyperlinkovou strukturou.
- Připravenost na vývoj v bezpečnostní oblasti – podporovat možnosti upgrade na nové technologie, které se budou zabývat příštími hrozbami. Systém by měl být připraven na nové výzvy a být modulární tak, aby poskytl prostor pro budoucí osazení specializovanými moduly pro akceleraci a rozšíření výkonu.
- Schopnost výkonového škálování – podporovat možnost rozšíření výkonu přidáním licence na výkon, podporou stohováni a možností agregací více bezpečnostních systémů do logického celku s centralizovanou správou.
- Integrace se SandBox řešením – podporovat možnost rozšíření o anti-malware analýzu souborů přenášených po síti pro rozšířené pokrytí možných vektorů hrozeb, které přináší nové generace malware.
- Viditelnost do všech protokolů, které umožňují přenášet soubory – dodané řešení by mělo podporovat viditelnost do všech běžných nešifrovaných i šifrovaných protokolů, kterými se mohou soubory dostávat do naší organizace.
- Rychlá ochrana proti bezpečnostním rizikům a zranitelnostem systémů a aplikací.
- Ochrana před DoS a DdoS.
- Rovnocenná podpora IPv4 a IPv6 a volitelná možnost inspektovat i SSL provoz.
- Ochrana reputační službou s geografickým systémem rozpoznání zdroje.
- Široká a přesná bezpečnost s limitováním falešných poplachů - systém by neměl používat signatury, ale filtry.
- Integrace funkcí Next-Generation Firewallů – rozpoznávání a viditelnost do aplikací.
- Podpora inspekce v heterogenním prostředí bez ohledu na výrobce síťové infrastruktury.
- Podpora inspekce ve virtualizovaném prostředí.
- Možnost řešení s vysokou dostupností pro zamezení výpadku sítě.
- Podpora vysoké dostupnosti při výpadku napájení.

- Licenčně škálovatelný výkon minimálně do 40 Gbps v rámci jednoho zařízení.
- Minimální přidané zpoždění v průběhu inspekce.
- Zařízení musí být dodané a funkční spolu se síťovým modulem se dvěma segmenty 10GbE s LR porty s ochranou proti přerušení síťové linky v případě výpadku napájení; zadavatel disponuje síťovým modulem TrendMicro NX IPS 2-sgmt 10G Fiber LR Bypass Module a dává jej účastníkům k dispozici pro využití v rámci dodávky - v případě, že zařízení nabídnuté účastníkem bude s tímto modulem kompatibilní, může jej účastník v rámci dodávky využít. .

Zařízení a jeho dohledová konzole musí mít tyto požadované funkce a vlastnosti:

- Agregovaná inspekční kapacita na jedno NGIPS při plném zatížení se všemi zapnutými filtry, na reálném provozu je min. 10 000 Mbit/s.
- Je možné licenční rozšíření výkonu na jedno NGIPS na min. 40 000 Mbit/s.
- Je možné licenční rozšíření o SSL inspekci s kapacitou inspekce min. 20 000 Mbit/s.
- Síťová propustnost NGIPS pro ostatní neinspektovaný provoz při použití bypass filtrů je min. 100 000 Mbit/s.
- Jsou podporovány porty 1000Base-X SFP, 10GBased-X SFP+ a 40GBase-QSFP+ s možností rozšiřitelnosti pomocí síťových modulů.
- Maximální průměrné zpoždění NGIPS při plném zatížení se zapnutými filtry, na reálném síťovém provozu je menší než 100 µs.
- Počet inspektovaných spojení v reálném čase je min. 100 000 000.
- Počet inspektovaných SSL spojení v reálném čase je min. 75 000.
- Množství nově otvíraných spojení za sekundu, inspektovaných na NGIPS je min. 600 000.
- Minimální počet řízených spojení (security context) je min. 10 000 000.
- Zařízení umožňuje inspekci transportních systémů VLAN 802.1Q, VLAN QinQ 802.1ad, GRE, MPLS, VPLS, LACP, VXLAN, IPv4 a IPv6.
- Zařízení v základu disponuje redundantními hot-swap napájecími zdroji.
- Zařízení má vysokou dostupnost v režimu Active-Active při nasazení druhého systému NGIPS do clusteru.
- Zařízení má podporu L2 Fallback v případě interní chyby software, nebo zahlcení systému.
- Zařízení má integrovanou podporu ochrany proti výpadku napájení pro optické i metalické segmenty.
- Zařízení má podporu asymetrického provozu (zařízení nemusí v rámci inspekčního segmentu vidět do obou směrů TCP spojení - typicky u Link Agregace) a podpora asymetrické inspekce (rozdílná konfigurace NGIPS bezpečnostního profilu pro rozdílný směr v rámci inspekčního segmentu).
- Zařízení má podporu funkce adaptivní konfigurace filtrů, která upozorní, případně vypne neefektivní filtr, který může způsobit zahlcení systému.
- Zařízení má podporu tzv. „hitless upgrade“ operačního systému NGIPS bez nutnosti plánování odstávky systému, má podporu hitless reboot.

- Zařízení obsahuje filtry/signatury popisující exploity, zranitelnosti, krádeže identity, malware, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, filtry na rozpoznávání aplikací, P2P sítě a nástroje na kontrolu toku multimédií.
- Zařízení obsahuje filtry/signatury popisující ochranu proti Zero day zranitelnostem pro operační systémy Linux, Windows, Mac OS a jejich aplikace.
- Zařízení má podporu automatické aktualizace filtrů a databáze IPv4, IPv6 a DNS jmen systémů na internetu s poškozenou reputací; automatická aktualizace musí být prováděna minimálně 1x týdně pro filtry a minimálně 5x denně pro reputační databáze.
- Databáze IPv4, IPv6 a DNS jmen s poškozenou reputací umožňuje třídění podle země původu IP adresy, potencionální nebezpečnosti a typu zjištěné nebezpečnosti.
- Pomocí GUI aplikace lze vytvořit zákaznické filtry.
- Zařízení má podporu importu komunitních filtrů/signatur Snort.
- Zařízení disponuje touto minimální sadou požadovaných akcí po zásahu filtru: Blokovat spojení a informovat, Vyvolat TCP Reset, Povolit a informovat, Provést záznam paketu, Omezit rychlost spojení a Provést karanténu zdrojové nebo cílové IPv4 nebo IPv6 adresy.
- Zařízení má podporu informování uživatele o provedení karantény prostřednictvím převzetí webového obsahu, včetně možnosti definovat v HTML obsah upozornění v českém jazyce.
- Je možné manuální i automatické volání karantény z externího systému přes API.
- Je možné nastavení časování karanténní operace minimálně dle závažnosti rozpoznaného problému.
- Zařízení má podporu translace 802.1Q VLAN ID (VLAN Bridge) v rámci bezpečnostního segmentu, pro inspekci na vnitřních VLAN bez potřeby zapojovat zařízení do všech fyzických cest kde je požadována inspekce provozu.
- Zařízení dokáže detekovat a blokovat útoky průzkumných aktivit.
- Zařízení podporuje automatickou ochranu filtrů proti přetížení či DoS útoku na NGIPS.
- Zařízení dokáže rozpoznávat provoz na základě geo-lokace a umět blokovat nebo aplikovat rozdílné bezpečnostní sety na provoz dle geografického původu zdrojové nebo cílové IP adresy.
- Zařízení dokáže poskytovat informace o True IP (XFF).
- Zařízení dokáže detekovat, blokovat nebo omezovat šířku pásma pro aplikace a zákaznické filtry.
- Zařízení dokáže detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii.
- Zařízení je plně transparentní k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků.
- Zařízení podporuje integraci se SandBox řešením pro síťovou a emailovou komunikaci formou vytvoření kopie provozu (včetně dešifrovaného SSL provozu), kterou autonomně odesílá na SandBox řešení.
- V rámci integrace NGIPS se SandBox řešením je zařízení schopné automaticky přidávat záznamy SandBoxem detekovaných IP, DNS adres C&C serverů a přesné URL/URI, na kterou malware odesílá svoji komunikaci.

- Zařízení podporuje SNMPv3, privátní MIB, Syslog a SNMP Trap.
- NGIPS je spravovatelné z nabízeného centrálního monitorovacího a konfiguračního sytému (centrální dohledové konzole), ale v případě jeho výpadku musí umožnit konfigurační změny i bez dohledového nástroje prostřednictvím webového/SSL rozhraní NGIPS.
- Centrální dohledovou konzoli lze obsluhovat z operačních systémů Linux, Microsoft a Mac-OS.
- Centrální dohledová konzole poskytuje aktualizaci a distribuci filtrů automaticky, manuálně a podle časového harmonogramu.
- Centrální dohledová konzole je schopna udržovat a spravovat operační systém NGIPS.
- Centrální dohledová konzole je schopna vytvářet přehledy manuálně a podle časového harmonogramu alespoň pro tyto kategorie: veškeré události, vybrané typy událostí a nejčastější události, cíl, zdroj, přehled anomálií a zneužití sítě, přehled zásahů omezení přenosu, přehled mezních hodnot provozu, statistika provozu zařízení a detailní přehled o DDoS útocích.
- Centrální dohledová konzole podporuje Syslog NG (syslog na TCP, včetně podpory šifrování).
- Centrální dohledová konzole umožňuje definovat uživatelské formáty pro logování.
- Centrální dohledová konzole podporuje webové API a databázový konektor pro externí přístup k databázi bezpečnostních událostí.

Na záruční podmínky jsou kladeny tyto požadavky:

- Komplexní technická podpora 24*7*365 je nabízena v základu, nahlášení problému je možné telefonicky či e-mailem. Maximální reakční doba pracovníka certifikovaného výrobcem pro servis a konfiguraci dodaného zařízení je 2 hodiny od nahlášení.
- V případě závady celého zařízení a nutnosti jeho nahrazení je možné zapůjčení náhradního, kompatibilního IPS se stejným, nebo vyšším síťovým i inspekčním výkonem včetně jeho instalace dodavatelem.
- Dodavatel poskytuje konzultace při řešení konfiguračních a SW problémů, zprostředkování komunikace s výrobcem zařízení v případě chybné funkce zařízení či požadavku na jeho funkční vylepšení. Zprostředkovává komunikaci s vývojovým týmem filtrů a pravidel výrobce.
- Dodavatel provede instalaci zařízení v místě plnění a zaškolení obsluhy v jeho konfiguraci, používání a osvědčených postupech při jeho správě v minimálním rozsahu osmi hodin.
- Služba aktualizace, výměny HW a technická podpora je nabízena minimálně po dobu tří let od dodání.
- V rámci záruky jsou HW a SW závady diagnostikovány a identifikovány v místě plnění.
- V rámci záruky je bezúplatné odstranění HW a SW závad včetně výměny vadného dílu v místě plnění servisním technikem dodavatele do druhého pracovního dne.
- Dodavatel disponuje minimálně třemi certifikovanými pracovníky (pro zaručení zastupitelnosti), kteří jsou certifikováni výrobcem nabízeného systému pro odbornou a technickou podporu.