Řešení firewall typu NGFW

Základní popis

Zařízení určené k ochraně síťového prostředí před hrozbami na bázi pokročilých útoků. Kromě funkcí tzv. Next-Generation FW (typicky chápané jako aplikační a identity-based FW) je schopno provádět inspekci provozu s detekcí a ochranou před útoky na úrovni síťového provozu. V oblasti ochrany proti malware je možnost aktivovat analýzu souborů včetně dynamické analýzy (tzv. sandboxing) i ukládání nebezpečných souborů do karantény. Zařízení lze rozšířit i pro URL filtraci na úrovni kategorií, konkrétních URL či podle reputace serverů v Internetu. Integrované „Security Intelligence" databáze poskytují informace o nebezpečných IP adresách, URL, DNS doménách v Internetu. Centralizovaný management disponuje funkcemi korelace a automatizace: filtrace důležitých událostí, automatické nastavení detekčních jednotek podle typu provozu v síti, zohlednění útoků podle jejich nebezpečnosti v konkrétním prostředí, interakce s externími systémy v případě detekování nebezpečné aktivity v síti. Kromě bezpečnostních funkcí poskytuje centralizovaný management pohled na kompletní síťovou aktivitu: směr komunikace na úrovni států, objemy datového přenosu podle URL, uživatele, aplikace, typu soborů, apod., viditelnost až do úrovně typů operačních systémů v síti. Interní korelační nástroje automaticky vyhodnocují stanice, které mohly být kompromitovány či jsou vzdáleně ovládány. V neposlední řadě je k dispozici flexibilní reporting i možnost napojení prakticky na libovolný SIEM. Pro specifické aplikace může být využito API pro přístup k informacím a interním databázím centrálního managementu.

Technická specifikace

Dvě zařízení musí splnit (nebo převýšit) všechny technické parametry uvedené v následující tabulce

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
A) Výkon a funkcionalita firewallu		
Zařízení musí umět alespoň základní možnosti vysoké dostupnosti a to v režimech active/active a active/pasive	Ano	
Formát zařízení	Appliance, 1RU	
Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených	1	
Minimální počet 1Gb 10/100/1000 BaseT Ethernet	12	
Minimální počet 10Gb SFP+ rozhraní portů pro data, standardně osazených	4	
Možnost rozšíření o moduly rozhraní	1	
Možnost rozšíření o další 10Gb SFP+ rozhraní	8	
Redundantní zdroje	Ano	
Podporovaný počet současně otevřených spojení stavový FW/aplikační FW	Min.2M/2M	
Rychlost vytváření nových spojení přes stavový FW	Min. 24K/s	
Propustnost stavového firewallu (multiprotokolový režim)	Min. 5 Gbps	
Propustnost aplikačního FW (next-gen FW) – (top parametry)	Min. 4.75 Gbps	
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (top parametry)	Min. 4.75 Gbps	
Propustnost aplikačního FW (next-gen FW) – (transakční profil, 450B průměrná velikost paketu)	Min. 1.65 Gbps	
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (transakční profil, 450B průměrná velikost paketu)	Min. 1.65 Gbps	
VPN propustnost	Min. 1.5 Gbps	
Současný počet VPN spojení (IPSec/SSL)	Min. 7 500	
Podpora L2 (transparentního) módu s podporou NAT a PAT	Ano	
Podpora L3 (routovaného) módu s podporou NAT a PAT	Ano	
Podporovaný počet VLAN	Min. 750	
Podpora stateful failover	active/standby	
Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podporou LACP	Ano	
Dynamické směrování - podpora alespoň RIP, OSPF, BGP	Ano	
Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	Ano	
Podpora Policy based Routing	Ano	

Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	Ano	
Podpora filtrace IPv4, IPv6	Ano	
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	Ano	
Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích	Ano	
Podpora inspekce IPv6 provozu	Ano	
Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	Ano	
Podpora NAT64 a DNS64	Ano	
Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód připadně pro řízení přístupu podle uživatelské identity, typu aplikace, apod.	Ano	
Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	Ano	
Možnost rozšíření o funkce NextGen FW	Ano	
Možnost rozšíření o funkce NextGen IPS	Ano	
Možnost rozšíření o funkce URL filtrace	Ano	
Možnost rozšíření o ochranu tzv. „Zero-day“ Anti-Malware	Ano	
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	Ano	
Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech	Ano	
API rozhraní pro sdílení kontextových informací s dalšími systémy	Ano	
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	Ano	
B) Požadované vlastnosti funkcionality IPS		
Možnost definovat typ provozu předávaný k inspekci do IPS	Ano	
Podpora také IDS režimu – pasivního monitorování (TAP režim)	Ano	
Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)	Ano	
Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti	Ano	
Podpora 802.1Q tagovaných rámců	Ano	
Podpora různých IPS politik pro různé typy provozu	Ano	
Inspekce pro IPv4 i IPv6	Ano	
Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému	Ano	
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií	Ano	
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	Ano	
Podpora aplikace pro psaní zákaznických filtrů	Ano	
Podpora importu komunitních filtrů/signatur Snort	Ano	
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	Ano	
IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	Ano	
IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C	Ano	
IPS musí umět 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	Ano	
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	Ano	
Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku	Ano	
Funkce pro kontrolu DLP (např. pomocí Snort preprocesorů)	Ano	
Podpora vrstvev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	Ano	
Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	Ano	
Možnost definice uživatelské vrstvy politik	Ano	
Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik	Ano	
Různé politiky lze sdílet a aplikovat na různé senzory	Ano	
IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	Ano	
Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“	Ano	

Možnost automatické i manuální klasifikace stanice jako “kritické” se zohledněním v pravidlech, reportech apod.	Ano	
Podpora „remediation“ modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	Ano	
Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly	Ano	
Podpora databází reputací adres v Internetu (Security Intelligence)	Ano	
C) Funkce Next-Gen FW		
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	Ano	
Podpora pasivního monitorování (TAP režim)	Ano	
Podpora 802.1Q tagovaných rámců	Ano	
Podporovaných aplikací	Min. 4000	
Kategorie aplikací (nebezpečné, důležité, apod.)	Ano	
URL kategorií	Min. 80	
Katagorizovaných světových URL	Min. 280 milionů	
Řízení přístupu k WWW - Web Usage Control (WCU)	Ano	
Filtrace podle typů aplikací webových i ne-webových	Ano	
Filtrace podle reputace serverů	Ano	
SSL inspekce (dekrypce/enkrypce)	Ano	
Security Inteligence database – známé uzly botnet sítí C&C	Ano	
Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, apod.	Ano	
Security Inteligence database – známé nebezpečné URL adresy a jmenné domény	Ano	
Možnost integrovat vlastní reputační databáze	Ano	
Podpora komunitních, otevřených standardů popisu apliací (OpenAppID)	Ano	
Filtry mohou zohlednit roli a identitu uživatele	Ano	
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	Ano	
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	Ano	
Řešení musí být schopné pasivního sběru informací o síťových zařízení a zobrazení:	Typ zařízení Operační systém Dodavatel OS Použité síť. protokoly Použité síť. služby Otevřené porty síť. služeb Potenciální zranitelnosti	
Přehled o síťových spojení má poskytovat minimálně tyto informace:	Čas startu a konce flow Akce (allow, deny,..) Důvod případného blokování Zdroj. a cíl. adresa Vstupní a výstupní zóna Vstupní a výstupní rozhraní Zdroj. a cíl. port Aplikační protokol IPS událost, pokud vznikne Riziková úroveň IPS události Použitá síťová aplikace Rizikovost aplikace „Business impact“ aplikace Množství přenesených dat	
D) Správa		
Vzdálené správa přes grafické rozhraní bez nutnosti instalace zvláštního SW	Ano	
Přístup ke GUI http/https protokolem	Ano	
Možnost vzdáleného přístupem protokolem ssh přímo do FW	Ano	

Možnost přístupu k textovým logům (syslog) přímo ve FW	Ano	
Možnost centrální správy při nasazení více firewallů	Ano	
Při centrální správě: možnost sdílených bezpečnostních politik	Ano	
Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu	Ano	
Zobrazení logů a událostí v grafickém rozhraní správy	Ano	
Možnost zaslání informace o TCP nebo UDP toku procházejícím firewallem (start a konec spojení, identifikovaný uživatel, přenesený objem dat, typ služby, délka trvání spojení) na TACACS nebo RADIUS server.	Ano	
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	Ano	
Funkce IPS a Next-Gen FW vyžadující dlohodobější ukládání dat, korelace, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního sytému (centrální dohledové konzole)	Ano	
Centrální dohledová konzole musí být schopna dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod.	Ano	
Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	Ano	
Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole	Ano	
Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	Ano	
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu	Ano	
Pro reporty lze definovat template definující formát a obsah reportu	Ano	
Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu	Ano	
V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N	Ano	
Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů	Ano	
Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.	Ano	
Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	Ano	
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.	Ano	
Podpora posílání událostí formou syslog, email, SNMP na externí platformy	Ano	
Podpora Event Streamer API (eStreamer) pro sdílení informací se externími systémy. Minimálně pro tyto SIEM:	ArcSight BMC Remedy Trustwave NetForensics Novell Sentinel Hawk Network Defense Q1Labs-QRadar Log Rhythm SIEM 2.0 LogLogic Splunk	
Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay	Ano	
Podpora JDBC API pro přístup z externích systémů k databázím centralizovaného managementu	Ano	
Podpora řízeného přístupu podle rolí administrátorů	Ano	
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	Ano	
Možnost založit pro daný incident „ticket“ přímo v prostředí GUI managementu	Ano	
Workflow pro předávání „ticketů“ mezi administrátory	Ano	
Konkrétní bezpečnostní incident až na úrovni paketu lze přiložit k danému „tiketu“ pro další analýzu	Ano	
Možnost definice politik pro sledování odpovídajících parametrů „zdraví“ na senzorech a centralizované konzoli (zařízení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)	Ano	
Zákaznicky definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví“	Ano	
Různé politiky pro sledování „zdraví“ lze aplikovat na různé senzory nebo centralizovanou konzoli	Ano	

E) Podpora / maintenance		
3 letá podpora typu 8x5 NBD (pro obě zařízení)	Ano	