TECHNICKÁ SPECIFIKACE

Obecné podmínky:

- Z důvodu dosažení plné kompatibility se současným řešením zadavatele a využití stávajících technologií, musí být uchazeč partnerem společnosti CheckPoint s úrovní partnerství minimálně dvě hvězdy. O tomto partnerství musí uchazeč doložit oficiální potvrzení společnosti CheckPoint, které bude potvrzené zástupcem kanceláře CheckPoint v ČR. Toto potvrzení bude v textu obsahovat jednoznačnou identifikaci, že bylo vystaveno pro účely tohoto výběrového řízení.
- Uchazeč musí poskytnout referenci alespoň jedné státní instituce, pro kterou po dobu minimálně posledních 5 let nepřetržitě poskytoval implementační nebo servisní služby k bezpečnostnímu řešení CheckPoint.

Technické podmínky:

Požadavek č.	Kategorie	Parametr	Hodnota (ano/ne)
		Bezpečnostní funkce	
1	Funkce	Nabízené řešení podporuje bezpečnostní funkce "Next Generation Firewall" min. s těmito funkčními vlastnostmi:	
1a	Funkce	Statefull Firewall	
1b	Funkce	Intrusion Prevention System	
1c	Funkce	Akvizice uživatelských identitt a definice politik na základě těchto identit	
1d	Funkce	Kontrola Aplikací a URL Filtering	
1e	Funkce	Ochrana proti známému Malwaru (AV)	
1f	Funkce	Detekce a blokování komunikace na botnet řídící centra	
1g	Funkce	Site-to-Site VPN	
1h	Funkce	Remote Access VPN s klientskými aplikacemi	
1i	Funkce	Remote Access VPN bezklientské (SSLVPN)	
2	Funkce	Firewall politiku je možné definovat na základě IP adres, skupin adres, sítí, uživatelů a uživatelských skupin synchronizovaných s AD	
3	Funkce	Bezpečnostní brána je fyzicky oddělena od bezpečnostního managementu. Komunikace mezi management zařízením a bezpečnostní bránou musí být kryptovaná a autentikovaná pomocí PKI certifikátů.	
4	Funkce	Okamžitě použitelné předdefinované IPS politiky	
5	Funkce	Možnost nastavení monitorovacího nebo blokovacího režimu IPS globálně, na úrovni politiky nebo na úrovni jednotlivé ochrany/signatury	
6	Funkce	Možnost rekonfigurace a ladění IPS engine přímo z log výstupů firewallu	
7	Funkce	Možnost definice IPS výjmek dle kombinace: src IP + dst IP + service + útok/signatura	
8	Funkce	Automatické vypnutí IPS ochrany v případě přetížení HW (využití CPU nebo fyzické paměti) nad definovanou prahovou hodnotu	
9	Funkce	Možnost získávání identit uživatelů z AD vcetne podpory software agenta na koncové stanice pro přesné získavaní identit, min. pro systémy Windows a Mac	
10	Funkce	Identifikaci uživatelů na základě web portálu - podpora ověření jméno/heslo (ne-doménový uživatelé) a SSO Kerberos (doménový uživetelé)	
11	Funkce	Identifikace uživatelů na základě ověření přihlášení klienta Remote Access VPN	
12	Funkce	Detekce a řízení síťových aplikací. Minimální počet rozpoznávaných aplikací 7000	
13	Funkce	Detekce a řízení síťových aplikací. Minimální počet aplikací/pluginů pro sociální sítě 100000	
14	Funkce	Podpora URL filteringu na základě kategorizace	
15	Funkce	Sjednocené řízení politiky pro řízení aplikací a URL filtering. Aplikace a URL musí podprovat více než jednou kategorii a umožňovat vlastní nastavení kategorizace	
16	Funkce	Filtrace škodlivých webových stránek obsahujících malware	
17	Funkce	Ochrana proti aktivitě botnetů - reputace IP adres, DNS a URL záznamů; analýza odcházející email komunikace (SPAM)	
18	Funkce	Blokování komunikace na IP adresy řídících center botnetů. Detekce aktivit botnetů pomocí behavior analýzy.	
19	Funkce	Ochrana proti virům, malware a jinému škodlivému software	
20	Funkce	Vzdálený SSLVPN přístup min. pro 5 současně připojených uživatelů	
21	Funkce	Podpora ActiveSync proxy pro bezpeční mobilní přístup	
22	Funkce	Podpora HTML5 Web socket technologie pro SSLVPN portál	
23	Funkce	Podpora VPN klientů pro operační systémy: Windows a MAC OSX	
24	Funkce	Podpora IPSec VPN tunelů	
25	Funkce	Podpora emulace neznámych vaiant malware (Sandboxing) pomocí licence nebo napojením na externí emulační zařízení	
26	Výkon	Propustnost Firewallu (dle RFC 3511, 2544, 2647, 1242), minimálně 24 Gbps	
27	Výkon	Propustnost IPS (dle RFC 3511, 2544, 2647, 1242), minimálně 7.5 Gbps	
28	Výkon	Propustnost NGFW (FW, IPS, Applikační kontrola), minimálně 5.5 Gbps	
29	Výkon	Počet nových spojení za vteřinu (CPS) minimálně 180.000	
30	Výkon	Počet současných spojení, min. 3.000.000	
31	Platforma	Počet fyzických síťových rozhraní, min. 10x 10/100/1000baseT	
32	Platforma	Možnost rozšíření o 4x 10Gb SFP+ rozhraní	
33	Platforma	Interní disková kapacita firewall, pro lokální logování v případě výpadku centrálního log serveru, min. 500 GB	
34	Platforma	Vysoce dostupné řešení bezpečnostních bran s možností režimu active-standby a active-active	
35	Platforma	Stavová synchronizace TCP, UDP a NAT spojení	
36	Platforma	Konfigurace bezpečnostní politiky prostřednictvím GUI rozhraní. Vzdálené připojení pomocí protokolů SSH a HTTPS.	
37	Platforma	Podporovat debuggování problémových scénářů na úrovni L2 - L7.	
38	Platforma	Podpora pravidelného automatického zálohováni konfigurace (na základě časového rozvrhu), s možností automatického nahrání na vzdálený SCP server.	
39	Platforma	Bezpečnostní logy musí být ukládány na fyzicky oddělenou management platformu.	
40	Platforma	Dodávaná firewall platforma musí byt ve formě samostatné hardware appliance	
		Centrální Management	
1	Management	Jednotný management pro všechny bezpečnostní funkce s možností definice administrátorských rolí	
2	Management	Centrální a jednotná správa politik z grafické aplikace	
3	Management	Definice bezpečnostních pravidel na základě identity uživatele nebo jeho uživatelské skupiny z AD	
4	Management	Funkce centrálního logování s dostupností logů a událostí min. 365 dnů zpět	
5	Management	Management musí být fyzicky oddělený od firewall platformy - na samostatném hardware	
6	Management	Podpora vyhledávaní v pravidlech, vyhledávaní textových výrazů/objektů/IP adres nebo prohledávaní všech objektů.	
7	Management	Management musí být schopen dohledat pro každý objekt jeho výskyt v aktivních i neaktivních pravidlech, nebo v jiných objektech (např. ve skupinách)	
8	Management	Možnost segmentace politik do samostatných logických oddílů.	
9	Management	Hit count statistiky pro jednotlivá pravidla za účelem optimalizace bezpečnostní politiky	
10	Management	Integrovaný monitoring musí poskytovat grafické rozhraní pro sledování parametrů v reálnem čase (využití paměti, CPU, počet navázaných spojení, počet nově otevřených spojení za sekundu, propustnost, atd …).	
11	Management	Centrální ukládaní logů z firewall platforem	
12	Management	Podpora služby vlastní certifikační autority pro vydávaní PKI certifikátů pro bezpečné přihlašovaní uživatelů a administrátorů a pro VPN klientský přístup	
13	Management	Práce s bezpečnostními logy – možnost prohledávaních všech typů logů (fw, ips, urlf) v jedné záložce s definováním vlastních permanentních filtrů.	
14	Management	Podpora pravidelného automatického zálohováni konfigurace (na základě časového rozvrhu), s možností nahrání zálohy na vzdálený SCP server.	
15	Management	Je-li management licence omezena počtěm řízených objektů bezpečnostních bran, musí podporovat řízení min. 5 objektů bran	
16	Management	Management log server musí zpracovat min. 10.000 logů/sek	
17	Management	Minimální velikost diskové kapacity pro dlouhodobé ukládaní log záznamů (jeli disková kapacita omezena licencí, licence pro požadovanou velikost musí byt součástí nabídky) = min. 16 TB	
		Analýza a korelace bezpečnostních událostí / logů	
1	Management	Podpora korelace bezpečnostních logů a incidentů	
2	Management	Možnost vytváření vlastních pravidel pro vzájemnou korelaci bezpečnostních událostí	
3	Management	Výrobce musí poskytovat pravidelné updaty pro nové verze logů nabízeného firewall řešení	
4	Management	Tvorba vlastních definic log parserů	
5	Management	Musí umožnit definici závažnosti jednotlivých událostí na základě korelačních pravidel	
6	Management	Musí graficky zobrazovat jednotlivé kategorie událostí ve formě interaktivních koláčových a časových grafů	
7	Management	Musí implementovat vyhledávaní zadané hodnoty skrze celou databázi událostí (bez nutnosti definice prohledávaných atributů)	
8	Management	Musí umožnit definici a permanentního ukládání vlastních filtrů událostí pro jednotlivé uživatele	
9	Management	Musí umožnit definici a uložení vlastního Dashboard panelu pro jednotlivé uživatele	
10	Management	Musí podporovat automatické reakce na definované bezpečnostní události – minimální akce: poslat email, blokovat zdroj útoku, SNMP trap do interního systému, spustit vlastní skript	
11	Management	Musí podporovat nástroj pro definici a ruční/automatizované generování reportů	
12	Management	Minimální počet zpracovaných korelovaných událostí (jeli omezeno licencí, licence pro požadovaný počet korelovaných log záznamů musí byt součástí nabídky) – min. 4 miliony událostí za den	
13	Management	Minimální podporovaná velikost diskové kapacity pro dlouhodobé ukládaní event záznamů (jeli disková kapacita omezena licencí, licence pro požadovanou velikost musí byt součástí nabídky) - min. 16 TB	