Systém preventivní ochrany IPS pro ICT ČSÚ

Příloha č. 2

- technický popis předmětu plnění

Požadované funkce	Parametr
Agregovaná propustnost IPS při plném zatížení se všemi zapnutými filtry ověřená nezávislou testovací organizací ICSA Labs, Tolly Group nebo NSS.	min. 1,5 Gbit/s
Požadované skupiny filtrů: exploity, zranitelnosti, krádeže identity, spyware, viry, vynucování bezpečnostních politik, filtry proti průzkumným aktivitám, síťové infrastruktuře, IM aplikacím (instantní messangery), P2P sítím a nástroje na kontrolu toku multimédií	Ano
Podpora automatické aktualizace filtrů/signatur a databáze IPv4, IPv6 a DNS jmen systémů na internernetu s poškozenou reputací	Ano
Databáze IPv4, IPv6 a DNS jmen musí umožňovat třídění podle země původu IP adresy, potencionální nebezpečnosti a typu zjištěné nebezpečnosti	Ano
Podpora aplikace pro psaní zákaznických filtrů	
Maximální zpoždění IPS při plném zatížení se všemi zapnutými filtry, ověřeno nezávislou testovací organizací ICSA Labs, Tolly Group nebo NSS.	< 200 mikrosekund
Počet segmentů	Min. 10 gigabitových segmentů pro in-line inspekci
Zařízení musí podporovat níže uvedené typy portu bez nutnosti externích převodníků: - 10/100/1000 Base-T , - 1000 Based-SX SFP, - 1000 Base-LX/LH SFP	Ano
Počet inspektovaných spojení v reálném čase	min. 6.000.000
Syn Proxy - množství nově otvíraných spojení za sekundu, inspektovaných na IPS	min. 100.000 spojení/s
Požadovaná inspekce následujících protokolů: VLAN 802.1Q, VLAN QinQ 802.1ad, GRE, MPLS, IPv4, IPv6	Ano
Podpora Zero Power High Availability (ZPHA) pro optické i metalické porty	Ano
Redundantní napájení	Ano
Požadované akce IPS: - Blokování - Blokování s logováním, - Blokování s logováním včetně zachycení paketu, - Povolení, - Povolení a logování, - Povolení s logováním včetně zachycení paketu, - Omezení datového toku, - Síťová karanténa	Ano
Podpora asymetrického provozu (rozdílná konfigurace IPS bezpečnostního profilu pro rozdílný směr v rámci inspekčního segmentu)	Ano
Podpora Hitless upgrade Operačního systému IPS	Ano

Podpora translace 802.1Q VLAN ID v rámci bezpečnostního segmentu	
Možnost omezování a řízení šířky pásma pro streamovaná multimedia a P2P sítě.	Ano
Navrhované IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy/organizace, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii.	Ano
Navrhované IPS musí umět odvracet Denial of Service útoky jako ICMP floods, UDP floods, SYN floods a TCP Establish Connection floods.	Ano
Navrhované IPS musí obsahovat ochranu proti výše zmíněným DoS/DDoS útokům s výkonem minimálně 100 tisíc invalid Syn za sekundu pro Syn Flood útoky a i během útoků provádět inspekci normálního provozu.	Ano
Navrhované IPS musí být plně transparentní k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků.	Ano