Příloha č. 1

„OBMĚNA FIREWALLOVÉHO ŘEŠENÍ“
–
TECHNICKÁ SPECIFIKACE

I. HW požadavky

Součástí dodávky jsou 2 ks firewallu, každý kus musí splňovat následující požadavky:

- HW appliance (nesmí se jednat o VM appliance ani o SW řešení);
- instalace do standardního racku 19", velikost max. 2U;
- veškeré HW komponenty musí být určeny pro provoz 24x7;
- min. 4x 10GE SFP+ síťová rozhraní a 10x 1 Gbps RJ45 síťová rozhraní;
- možnost rozšíření až na 4x 25 GE SFP+ a na 8x 10 GE SFP+;
- 1 Gbps RJ45 management rozhraní;
- lokální úložiště typu SSD/flash o kapacitě min. 2x 960 GB v RAID;
- min. 2 redundantní hot swap napájecí zdroje;

II. Požadavky na cluster

- zapojení obou firewallů v redundantním HA systému (cluster);
- podpora přepnutí mezi jednotlivými uzly clusteru v řádu maximálně jednotek vteřin;
- automatická synchronizace konfigurace a veškerých databází mezi oběma uzly clusteru;
- zachování statických DHCP rezervací v DHCP serveru i při přepnutí uzlu clusteru;
- aktualizace firmwaru nezávisle pro oba uzly clusteru, bez přerušení provozu;
- možnost ručního přepnutí mezi jednotlivými uzly clusteru do režimu active;
- možnost rozdělení clusteru na dva nezávislé samostatně fungující uzly;

III. Výkonové požadavky

- propustnost firewallu pro IPv4 provoz s analýzou aplikací včetně logování v reálném čase min. 18 Gbps;
- propustnost funcionality IDS/IPS včetně logování min. 10 Gbps;
- propustnost funkcionalit ochrany proti hrozbám (stavový firewall, IPS, antivirus, SSL inspekce, proxy) včetně logování v reálném provozu min. 8 Gbps;
- propustnost OpenVPN nebo SSL VPN v reálném provozu min. 4 Gbps;
- počet současně navázaných spojení min. 2,2 mil. za sekundu;
- počet nových spojení min. 220 tisíc za sekundu;

IV. Požadavky na síťování

- plnohodnotná podpora IPv4 i IPv6 adresace a routování;
- statické routování;
- definice rozhraní LAN, WAN, BOND, VLAN, BRIDGE;
- podpora tagovaných VLAN rozhraní s možností definice tagu;

- adresovatelné bridge rozhraní s možností poskytování síťových služeb na bridge rozhraní;
- možnost agregace fyzických rozhraní podle IEEE 802.3ad;
- možnost dynamické adresace pomocí DHCP klienta na jednotlivých síťových rozhraních;
- možnost blokace provozu na základě příchozího síťového rozhraní;
- nastavení úrovně antispoofingu na jednotlivých síťových rozhraních;
- podpora multihoming (vícero konektivit) v režimu active-backup s možností definice serverů pro testování jednotlivých konektivit;

V. Požadavky na vzdálený přístup

- OpenVPN server s možností min. 25 instancí s unikátní konfigurací každé z nich;
- podpora dvoufaktorové autentizace klientů vůči OpenVPN serveru – min. Google autentikátor a Cisco DUO;
- možnost nastavení síťových parametrů (routovací tabulka, NTP server, DNS server, adresace) jednotlivě pro každého VPN klienta;
- možnost omezit přístup na VPN pouze vyjmenovaným klientům na základě CN v certifikátu;
- automatické stahování CRL z internetu;
- podpora RAS i site-to-site typů VPN klientů;
- podpora VPN klientů v operačních systémech min. MS Windows, Linux, Apple iOS, Android;
- možnost zobrazení aktuálně připojených VPN klientů včetně přidělených adres;
- možnost připojení zařízení v pozici OpenVPN klienta;
- podpora IPSec tunelů s možností definice vícero sítí za jednotlivými uzly;
- možnost zobrazení aktuálního stavu IPSec tunelu (otevření tunelu, čas negociace klíče);
- SNMP vzdálené vyčítání informací o stavu zařízení;
- SSH přístup k CLI pro ovládání zařízení;

VI. Požadavky na služby

- DHCP server s možností min. 10 instancí s unikátní konfigurací každé z nich;
- možnost zobrazení aktuálně přidělených adres včetně klientů;
- definice statických DHCP rezervací se zaručením přidělení konkrétní adresy;
- definice routovací tabulky pro DHCP klienty;
- DNS server s podporou zachytávání dotazů jiným DNS serverům;
- podpora DNSSEC;
- možnost vynucení safesearch pro vyhledávače Google a Bing;
- synchronizace času zařízení pomocí NTP;
- odesílání systémových logů protokolem syslog na definované zařízení;
- zachycení provozu pro následnou analýzu (např. dump pro analýzu ve Wiresharku);

VII. Požadavky na řízení provozu

- stavový paketový filter;
- zdrojový překlad adres (SNAT), cílový překlad adres s překladem cílového portu (DNAT s PAT), statický NAT, dynamický NAT, NAT 1:1, redirect;
- zadávání zdroje a cíle provozu v paketovém filteru pomocí doménových jmen;

- nastavení šířky pásma (garantovaná, maximální) na základě zdroje, cíle, portu a protokolu;
- řízení webového HTTP/HTTPS provozu pomocí proxy serveru s možností min. 10 instancí s unikátní konfigurací každé z nich;
- možnost poskytovat jednu instanci HTTP/HTTPS proxy serveru na více síťových socketech zároveň;
- napojení HTTP/HTTPS proxy na MS Active Directory kvůli autentizaci uživatelů (Kerberos) bez nutnosti instalace klientského software na koncovém zařízení;
- publikace souboru WPAD pro automatické nastavení proxy serveru;
- řízení webového provozu na základě zdroje, cíle, uživatele, skupiny, času nebo webové kategorie;
- možnost nastavení výjimek z autentizace web filteru dle zdrojové nebo cílové IP adresy;
- kategorizace webů do min. 30 skupin dle obsahu s databází uloženou lokálně na zařízení s automatickými aktualizacemi ze serverů výrobce;
- nastavení filtrace webového provozu v transparentním nebo netransparentním režimu, bez nutnosti rozšifrování spojení (např. na základě SNI);
- reverzní web proxy pro účely publikace více webových serverů na jedné IP adrese a stejném portu s terminací SSL/TLS;

VIII. Požadavky na bezpečnost

- automatická blokace nebezpečného provozu pomocí databáze nebezpečných IP adres umístěné přímo na zařízení;
- automatická obnova bezpečnostní databáze nebezpečných IP adres s intervalem obnovy max. 15 minut;
- možnost automatického sdílení bezpečnostních informací o kybernetických hrozbách v rámci kolektivního systému výrobce;
- napojení na min. 5 dalších bezpečnostních databází geograficky významných pro místo nasazení;
- možnost definice výjimek v rámci databáze nebezpečných IP adres;
- možnost přidání vlastních nebezpečných IP adres do databáze nebezpečných IP adres;
- systém honeypot pro detekci útoků přes protokol TCP s automatickou blokací komunikace útočníka do interní sítě s nastavitelným časovým omezením;
- IPS/IDS systém s databází signatur v počtu min. 15 tisíc;
- automatická obnova signatur IDS/IPS systému s intervalem obnovy max. 15 minut;
- možnost definice výjimek v rámci IPS/IDS systému;
- možnost přidání vlastních signatur do IPS/IDS systému;
- blokace webového provozu na weby se škodlivými kódy, P2P pomocí kategorizace;
- integrovaný antivirus pro kontrolu webového provozu s databází vzorků (potřebné licence musí být součástí dodávky);
- automatická obnova databáze antiviru s intervalem obnovy max. 60 minut;

IX. Požadavky na možnosti konfigurace

- webové rozhraní pro konfiguraci zařízení s definicí uživatelských účtů a rolí;
- zabezpečené SSH připojení na CLI zařízení;
- možnost vlastních certifikátů pro přístup do webového rozhraní;

- auditovatelnost konfiguračních změn zařízení (uživatel, čas apod.);
- možnost zobrazení všech historických verzí konfigurace s možností návratu k předchozím verzím;
- automatické varování na expirující certifikáty napříč konfigurací;
- automatická kontrola konfiguračních změn s varováním na potenciálně nevalidní a nebezpečné konfigurace;
- paralelní instalace více verzí firmware s možností bezpečného návratu k předchozí verzi;
- možnost lokálního stažení zálohy konfigurace;
- možnost automatického zálohování konfigurace na server výrobce;
- možnost definice proměnných seznamů IP adres použitelných napříč webovým rozhraním;
- zabezpečené připojení zařízení do sítě výrobce samostatným šifrovaným kanálem pro možnost vzdálené správy a opravy;

X. Ostatní požadavky

- management port pro možnost vzdálené disaster recovery;
- podpora veškerých funkcionalit s výjimkou aktualizace firmware a databází i při expirované licenci;
- podpora a kompatibilita se stávajícím řešením Kernun Security Appliance 10 cluster instalovaném na pobočce objednatele v Praze, tj. v rozsahu připojení druhé lokality objednatele.