# Firewall včetně vzdáleného přístupu (VPN)

## Řešení ochrany perimetru počítačové sítě

Současná ochrana perimetru poč. sítě neodpovídá aktuálním požadavkům na síťovou bezpečnost a klade neúměrné nároky na údržbu a správu. S ohledem na důležitost zařízení, výpadek této služby má vliv na chod celé instituce.

Z tohoto důvodu je poptáván hardwarový box. Oproti stávajícímu řešení, požadujeme služby antivirové kontroly provozu, antispam, application control, web filtering a intrusion prevention systém s možností aktualizací reputačních či jiných databází po dobu 5-ti let. Systém také musí využívat databázi IP reputation pro blokaci DoS útoků. Firewal musí taktéž obsahovat funkce web aplikačního firewalu pro ochranu webových aplikací, předpokládá se základní ochrana pomocí statických signatur. Redundantní konektivita se zbytkem síťové infrastruktury je samozřejmostí. Next Generation Firewall (dále jen NGFW) ve formě hardware appliance, s podporou výrobce v režimu 24x7 a aktualizací všech požadovaných bezpečnostních funkcí po dobu 5-ti let, musí také zabezpečit šifrovaný vzdálený přístup (VPN) do lokální poč. sítě.

Zadavatel si vyhrazuje právo otestování shody udávaných parametrů propustnosti jednotlivých bezpečnostních funkcí s reálným měřením/chováním zařízení v testovacím prostředí. S ohledem na požadavky zadávací dokumentace mohou být/budou testovány zejména tyto funkce:

• test kapacity firewallu (UDP PPS test, test propustnosti UDP/64B),

• test počtu konkurenčních spojení (TCP),

• test počtu nově navazovaných spojení,

• test propustnosti NGFW,

• možnosti správy, logování a reporting.

## Specifikace minimálních požadavků technického řešení

### NGFW - 1 kusy

**Obecné minimální požadavky na NGFW**

- hardware appliance o velikosti 1 RU

- podpora režimu vysoké dostupnosti (active/passive, active/active)

- správa zařízení pracujících v režimu vysoké dostupnosti musí probíhat prostřednictvím jednoho konfiguračního rozhraní, je požadována automatická synchronizace provozních a stavových informací mezi jednotlivými zařízení v jednom celku vysoké dostupnosti

- grafické konfigurační rozhraní a příkazový řádek

- minimální počty požadovaných síťových rozhraní:

o 16x GE RJ 45

o 4x 10 GE SFP+

o management rozhraní 1x RJ 45

o konzole sériové linky pro přístup k příkazovému řádku

- Podpora plnohodnotné inspekce sítového provozu v režimech

o NAT/router

o L2 transparentní režim (dva a více sítových rozhraní)

**Minimální výkonové požadavky**

Požadované výkonové parametry je nutné doložit oficiálním produktovým listem výrobce. Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání.

- minimální požadovaná propustnost stavového firewallu pro IPv4 i IPv6 provoz 27 Gbps (udp pakety o velikosti 512 B)

- nízké vložené zpoždění zařízení (latence)

- minimální počet současně navázaných spojení firewallu 3M

- minimální počet nových spojení za sekundu 100 k

- propustnost při zapnutí bezpečnostních a inspekčních funkcí (měřeno na reálném provozu)

o propustnost NGFW (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, logování) min. 3,1 Gbps

o propustnost ochrany proti hrozbám a škodlivému kódu (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, ochrana proti škodlivému kódu, logování) min. 2,8 Gbps

o propustnost ochrany proti hrozbám (IPS, ochrana proti sítovým útokům, logování) min. 5 Gbps

- propustnost funkce SSL inspekce provozu min. 3 Gbps

- min. počet konfigurovatelných virtuálních kontextů na každém zařízení 10

**Funkční požadavky**

- Podpora a zabezpečení IT systémů minimálně s ohledem na tyto bezpečnostní funkce:

o funkce rozpoznávání aplikací na L7 – aplikační vrstvě, podpora alespoň 4000 aplikací, protokolů; jednotlivé aplikace/protokoly uspořádány do kategorií; výrobce automaticky udržuje a aktualizuje databázi podporovaných aplikací

o funkce ochrany před sítovými útoky vycházející z výrobcem udržované a aktualizované databáze, ochrana před útoky typu DoS, verifikace protokolů

o ochrana před výskytem škodlivého kódu v síťovém provozu (antivirus/antimalware) s podporou zabezpečení kancelářských (IT); předání zkoumaných souborů pro analýzu v prostředí typu sandbox

o funkce kategorizace webových stránek (web filtering) s podporou minimálně 300 mil. známých URL (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), výrobcem aktualizovaná a udržovaná databáze.

o funkce SSL inspekce pro kontrolu protokolů s možností vytváření výjimek. Výjimky z SSL inspekce požadujeme minimálně:

* na základě administrátorem definovaných adres
* na základě kategorie URL, brané z URL filtrační databáze (např. kategorie bankovnictví, zdravotnictví, atd.)

- ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius)

- funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, tak licence musí být součástí dodávky

- funkce QoS, traffic shaping

- funkce klientské VPN (přístup do vpn v tunelovém režimu s vpn klientem; možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky vpn uživatelů; ssl vpn nebo ipsec vpn)

- site-to-site ipsec vpn s podporou statického i dynamického routování

**- ochrana proti SQL Injection a obecným útokům**

**- detekce a blokování** známých útoků na webové aplikace pomocí signatur a omezení

Součástí dodávky je instalace a konfigurace včetně připojení do počítačové sítě příslušnými moduly a kabely.

**Vlastnosti zařízení**

|  |  |  |
| --- | --- | --- |
| **Požadovaná funkcionalita** | **Specifikace minimálních požadavků** | **Dodavatelem nabízená hodnota** |
| Firewal mód | Routed/Transparent |   |
| Podpora HA active/standby, active/active | ANO |  |
| Minimální počet 1Gb RJ-45 portů | 16 |   |
| Minimální počet 10Gb SFP+ portů | 4 |   |
| Min. 1x integrovaný management port | 1Gb RJ-45 |   |
| Min. 1x sériový port | RJ-45 console |   |
| Racková montáž | ANO |   |
| Podpora rozdělení na více virtuálních jednotek | ANO |  |
| Intrusion Prevention System | ANO |   |
| Visibilita aplikací | ANO |   |
| Detekce malware, sandboxing | ANO |   |
| Podpora SSL/TLS dešifrace | ANO |   |
| URL filtering  | ANO |   |
| Remote access VPN (SSL VPN i IPSec) | ANO |   |
| Podpora Site-to-Site VPN | ANO |   |
| Podpora IPv4, IPv6 | ANO |   |
| Min. VLAN subinterfaces | ANO |   |
| Podpora EtherChannel 802.3ad | ANO |   |