Technické požadavky na dodávané řešení

Administrace dodaného řešení musí být umožněna přes webové rozhraní s podporou textového rozhraní (tzv. „cli“).

Nepřetržitá podpora od výrobce je požadována v rozsahu 24 hodin/7 dní v týdnu/365 dní v roce.

1. Vyžadované funkce nabízeného řešení

1.1. Základní

Požadavek
Stavové filtrování paketů
Překlady komunikace (příchozí i odchozí)
Podpora funkcionality typu SD-WAN (včetně funkce rozkládání zátěže mezi primární a záložní internetovou linku a WAN failover na základě dostupnosti WAN konektivity).
Montáž do standardních 19" skříní (rack).
100% administrace pouze přes webové rozhraní (bez nutnosti použít textové rozhraní typu telnet/ ssh konzole)
Propojení a využívání Active Directory
Podpora bezagentového přihlášení uživatelů nezávislé na portu komunikace
DHCP server a DNS forwarder pro konkrétní sítě
Možnost automatické zálohy systému a v případě potřeby kompletní obnovy konfigurace nahráním ze zálohy
Vynucení šifrování záloh
Logování a rozšířený reporting (vč. statistik uživatelských aktivit)
Podpora vrácení se na předchozí verzi software (po aktualizaci na novou verzi systému)
Vlastní API rozhraní pro propojení s dalšími interními nástroji
Licenčně neomezený počet uživatelů a internetových domén.

1.2. Proaktivní ochrana perimetru

Požadavek
IDS/IPS filtr nastavitelný na konkrétní komunikaci (pravidla firewall)
Možnost vytvářet vlastní IPS pravidla
Blokování komunikace C&C a typu Botnet a možnost specifikace výjimek
Identifikování kompromitovaného systému na základě C&C komunikace
Aplikační kontrola (blokování konkrétních aplikací z pravidelně aktualizovaného seznamu výrobce).
Logování a reportování

1.3. VPN – vzdálené přístupy

Požadavek
IPSEC – propojení vzdálených lokalit, včetně podpory IKEv2
SSL VPN i IPSEC – připojení vzdálených PC
SSL VPN - Odlišný certifikát / uživatel
Možnost vzdálené instalace VPN klienta
Zobrazení aktuálně připojených uživatelů v GUI
Licenčně neomezený počet VPN tunelů, připojených uživatelů a přenosu dat
Neomezený počet SSL VPN a IPSEC klientů v ceně
Logování a reportování

1.4. Ochranu přístupů na internet

Požadavek
Filtrování HTTP, HTTPS a FTP
SSL / TLS skenování neomezené jen na HTTPS protokol
Ochrana skenováním antimalware
URL filtrování (min. 75+ kategorií)
Blokování datových typů na základě přípony souboru a MIME hlavičky
Propojení s Active Directory
Možnost definovat výjimky (minimálně na zdrojové IP, cílové IP a webové stránky)
Podpora platnosti pravidel pouze ve specifikovaný čas
Pravidla musí být možno specifikovat na skupinu/uživatele z Active Directory
Podpora Sandboxingu
Logování a reportování

1.5. Reverzní proxy pro ochranu interních webových serverů a aplikací

Požadavek
Ochrana skenováním antimalware motorem
Filtrování http a https komunikace
Automatické přesměrování http komunikace na https
Podpora nahrávání vlastních certifikátů pro jednotlivé virtuální servery
Možnost monitorovat nebo blokovat (odmítnout) komunikaci
Přeposílání originální hlavičky (pro zobrazení skutečných zdrojů komunikace na cílovém serveru)
Podpora zabezpečení koncových aplikací vytvářením přihlašovacích formulářů navázaných na Active Directory
Ochrana proti útokům na aplikace
Ochrana proti podvržení cookies (podepisování)
Blokování komunikace na základě reputační služby výrobce
Blokování útoků typu SQL injection
Možnost specifikace výjimek

Logování a reportování

1.6. Ochrana emailové komunikace (SMTP)

Požadavek
Skenování odchozího i příchozího provozu
Podpora neomezeného množství domén
Možnost profilů nastavení pro každou doménu
Funkce relay nastavitelná na konkrétní doménu (na jakou IP adresu mail serveru se emaily doručí)
Skenování příloh emailů
Ochrana skenováním antimalware motorem
Sandboxing
Blokace příloh dle typu souborů na základě MIME hlaviček
Možnost blokace šifrovaných příloh
Ochrana proti spamům / phishing emailům
Greylisting
Ověření adresy příjemce z emailového serveru na úrovni SMTP dotazu
Blokace na základě SPF a RBL
Kontrola DKIM příchozích emailů a podepisování DKIM odchozích emailů
Blokování emailů na základě reputační služby výrobce
Ochrana proti DoS útokům
Nastavitelná a vynutitelná TLS komunikace pro konkrétní SMTP servery
Volitelný TLS certifikát pro SMTP službu
Šifrování odchozích emailů (nastavitelné a volitelné)
Kontrola emailové fronty ze stejného webového rozhraní
Emailová karanténa uložená přímo na zařízení bez nutnosti využívat externích služeb (další server, externí databáze apod.)
Náhled uživatele do karantény pomocí GUI „uživatelského portálu“ (jen pro emaily konkrétního uživatele) a možnost uvolnění spamů
Možnost specifikace výjimek minimálně v rozsahu odesílatel, příjemce, zdrojová IP adresa
Logování a prohledávání logů min. na úrovni: Odesílatel, Příjemce, Předmět
Logování a reportování

1.7. Možnost rozšíření o správu WiFi

Zadavatel požaduje možnost rozšíření o správu wifi zařízení (vše od stejného výrobce) a nesmí k tomu vyžadovat žádnou další licenci (pokud ano musí být součástí nabídky pro neomezený počet WiFi AP a neomezené funkcionality, které řešení v této kategorii poskytuje).

2. Minimální technické požadavky a propustnosti deklarované výrobcem

Požadavek	
Hardware akcelerace	například pomocí ASIC čipu
Active/passive cluster	2 fyzická zařízení

Propustnost	**Hodnota**
Firewall	>35 Gbps
IPSEC VPN	>18 Gbps
IPS	>6,5 Gbps
NGFW	>6 Gbps
Latence	<5 µs
Konkurenční spojení	>6 miliónů
Nová spojení / sekunda	>130000