**Zabezpečení perimetru technologií UTM**

1. **Specifikace zabezpečení**

Předmětem je řešení klastru firewallů typu UTM (Unified Threat Management nebo také Firewall nové generace).

Pokud se firewall skládá z více modulů, musí jít o moduly jednoho výrobce a tyto moduly musí být integrovány do jednoho celku s jednou, centrální správou na jednom hardware. Součástí dodávky musí být veškeré potřebné programové vybavení, tj. všechny licence potřebné pro instalaci a provoz, pro neomezený počet uživatelů.

Všechny služby musí být poskytovány jedním zařízením typu hardware appliance. Řešení musí mít funkcionalitu vysoké dostupnosti (active-passive) pro všechny prvky poskytující funkce uvedené v bodu 2, s výjimkou logování a rozšířeného reportování, a to bez dalších licenčních nákladů (přípustné jsou pouze náklady na hardware).

Podpora, záruka a licence na dodaný HW – vše na 3 roky.

1. **Požadované funkce**
	1. **Paketový filtr a základní funkce**

|  |  |
| --- | --- |
| Požadavek | Požadováno (ANO,NE) |
| Stavové filtrování paketů | ANO |
| Překlady komunikace (příchozí i odchozí) | ANO |
| Možnost použití více internetů v režimu active-backup nebo balancing (dynamické routování). | ANO |
| Montáž do standardních 19" skříní (rack). | ANO |
| 100% administrace pouze přes webové rozhraní (bez nutnosti použít textové rozhraní typu telnet/ ssh konzole) | ANO |
| Propojení a využívání Active Directory | ANO |
| Podpora bezagentového přihlášení uživatelů (8. vrstva) | ANO |
| DHCP server a DNS forwarder pro konkrétní sítě | ANO |
| Možnost automatické zálohy UTM a v případě potřeby kompletní obnovy konfigurace nahráním ze zálohy | ANO |
| Logování a rozšířený reporting (vč. statistik uživatelských aktivit) | ANO |
| Vlastní API rozhraní pro propojení s dalšími interními nástroji | ANO |
| Podpora routování BGP a OSPF | ANO |

* 1. **Proaktivní ochrana perimetru**

|  |  |
| --- | --- |
| Požadavek | Požadováno (ANO,NE) |
| IDS/IPS | ANO |
| Blokování C&C komunikace | ANO |
| Možnost specifikace výjimek | ANO |
| Identifikování kompromitovaného systému na základě C&C komunikace | ANO |
| Aplikační kontrola (blokování konkrétních aplikací z pravidelně aktualizovaného seznamu výrobce) | ANO |
| Logování | ANO |

* 1. **VPN – vzdálené přístupy**

|  |  |
| --- | --- |
| Požadavek | Požadováno (ANO,NE,POZNÁMKA) |
| IPSEC – propojení vzdálených lokalit | ANO |
| SSL VPN – připojení vzdálených PC | ANO |
| SSL VPN - Odlišný certifikát / uživatel | ANO |
| SSL VPN - Uživatelský portál pro stažení VPN klienta | ANO |
| SSL VPN - Dostupná instalace vč. konfigurace (bez nutnosti další konfigurace na koncových počítačích) | ANO |
| Zobrazení aktuálně připojených uživatelů v GUI | ANO |
| Licenčně neomezený počet VPN tunelů, připojených uživatelů a přenosu dat | ANO |
| Neomezený počet SSL VPN klientů v ceně | ANO |
| Logování | ANO |

* 1. **Reverzní proxy pro ochranu interních webových serverů a aplikací**

|  |  |
| --- | --- |
| Požadavek | Požadováno (ANO,NE) |
| Ochrana skenováním antimalware motorem | ANO |
| Filtrování http a https komunikace | ANO |
| Ochrana proti trojským koním | ANO |
| Ochrana proti podvržení cookies (podepisování) | ANO |
| Možnost monitorovat nebo blokovat (odmítnout) komunikaci | ANO |
| Podpora reverzních formulářů přihlášení navázaných na Active Directory | ANO |
| Blokování komunikace na základě reputační služby výrobce | ANO |
| Možnost specifikace výjimek | ANO |
| Logování | ANO |

* 1. **Ochrana emailové komunikace (SMTP)**

|  |  |
| --- | --- |
| Požadavek | Požadováno (ANO,NE) |
| Ochrana skenováním antimalware motorem | ANO |
| Ochrana proti spamům / phishing emailům | ANO |
| Skenování příloh emailů vč. archivů | ANO |
| Skenování odchozího i příchozího provozu | ANO |
| Blokování komunikace na základě reputační služby výrobce | ANO |
| Ochrana proti DoS útokům | ANO |
| Nastavitelná a vynutitelná TLS komunikace pro konkrétní SMTP servery | ANO |
| Šifrování odchozích emailů (nastavitelné a volitelné) | ANO |
| Kontrola emailové fronty na UTM | ANO |
| Karanténa uložená na UTM | ANO |
| Logování a prohledávání logů min. na úrovni: Odesílatel, Příjemce, Předmět, Datum | ANO |
| Stejné logování a prohledání i pro uživatele pomocí GUI „uživatelského portálu“ (jen pro emaily konkrétního uživatele) | ANO |
| Greylisting | ANO |
| Sandboxing | ANO |
| Možnost specifikace výjimek | ANO |
| Logování | ANO |

* 1. **Ochranu přístupů na internet**

|  |  |
| --- | --- |
| Požadavek | Požadováno (ANO,NE,POZNÁMKA) |
| Ochrana skenováním antimalware motorem | ANO |
| URL filtrování (min. 80+ kategorií) | ANO |
| Filtrování HTTP, HTTPS a FTP | ANO |
| Možnost specifikovat povolené porty | ANO |
| Možnost specifikace porty proxy | ANO |
| Propojení s Active Directory | ANO |
| Možnost definovat výjimky | ANO |
| Pravidla platí pouze ve specifikovaný čas během dne | ANO |
| Pravidla lze specifikovat na skupinu/uživatele z Active Directory | ANO |
| Sandboxing | ANO |
| Logování | ANO |

* 1. **Možnost rozšíření o správu WiFi**

Řešení musí být rozšiřitelné o správu wifi zařízení (vše od stejného výrobce) a nesmí k tomu vyžadovat žádnou další licenci.

1. **Minimální technické požadavky (propustnost deklarovaná výrobcem)**
* Firewall: 18 Gbps
* IPS propustnost: 4 Gbps
* VPN (AES) propustnost: 1,5 Gbps
* Propustnost Web proxy s aktivním AV: 2,5 Gbps
* Souběžná spojení: 8 miliónů
* Nová spojení za sekundu: 100 tisíc