	Minimální požadované parametry
Základná konfigurace Firewall	
Výkon	FW propustnost: 39 Gbps
	FW IMIX propustnost: 20 Gbps
	IPS propustnost: 7 Gbps
	Počet současných spojení alespoň: 6 500 000
	Počet nových spojení za sekundu: 148 000
	IPSec VPN propustnost: 20 Gbps
	Propustnost při zapnutých funkcích FW, IPS, Application Control a AV: 1.2 Gbps
Požadavky na HW	
	Integrovaný SSD disk (alespoň 120 GB)
	min. 8xRJ45 metalických portů (vč. 1x bypass páru)
	min. 2x1G SFP port
	Možnost redundantního zdroje napájení
	min. 1x RJ45 management port
	min. 2x USB 3.0 port + 1x USD 2.0 + 1x Micro USB
	možnost rozšířit konektivitu o min. 8x RJ45 metalických portu
	možnost rozšířit konektivitu o min. 8x SFP 1 GbE
	možnost rozšířit konektivitu o min. 4x SFP+ 10GbE
	možnost rozšířit konektivitu o min. 4x RJ45 (2x bypass pár)
	možnost rozšířit konektivitu o min. 4x RJ45 PoE+
	možnost rozšířit konektivitu o min. 4x 2.5 GbE RJ45 PoE
	možnost rozšířit konektivitu o VDSL2 modul pro DSL připojení
	velikost v racku: 1U
Obecná specifikace	
	Technologie musí mít hodnocení dle Gartner Peer Insights v oblasti Network Firewall alespoň 4,7.
	Certifikace ISCA Labs v oblasti Firewall
	Produktové certifikace CB, CE, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel
	Možnost správy WiFi AP od stejného výrobce on box (integrovaný WiFi controler)
	Řešení nabízí User Portal s možností správy emailové karantény pro uživatele
	Řešení disponuje funkcí tzv. Selective HTTPS Scanning, která umožňuje správci vybrat určitý HTTPS obsah, na kterém má být provedeno skenování a kontrola protokolu SSL/TLS.
	Řešení poskytuje vhled do uživatelské aktivity tzv. User Threat Quocientem – automatickým nástrojem, který uděluje skóre rizikovosti jednotlivým uživatelům
	Řešení je schopno na základě automatizovaného procesu zjistit aktuální bezpečnostní stav koncové stanice (zda nebyla na stanici identifikována nákaza malwarem, agent AV je plně aktualizován atd.) a případně uplatnit restriktivní politiky na konkrétní zařízení. Platí v případě nákupu AV od stejného výrobce.
	Řešení musí umožnit identifikaci všech aplikací, které běží na koncové stanici a v rámci FW uplatnit zvolenou politiku per aplikace . Platí v případě nákupu AV od stejného výrobce.
	FW musí mít integrovaný tester pro FW a web filter politiky
	Řešení musí nabízet on-box reporting
	Podpora Wildcard pro Domain Name Host Objects
Funkcionality	
	Zahrnuje ochranu pomocí Intrusion Prevention (IPS) - možnost definování vlastních signatur
	Zahrnuje cloud Sandbox Protection, ochranu postavenou na algoritmech machine learning (datacentrum s umístěním v zemích EU)
	Možnost rozšíření o Web Application Firewall a reverzní proxy dokoupením licence
	Nabízí plně transparentní proxy pro AV kontrolu a filtrování webu
	Dva nezávislé skenovací AV enginy (různí výrobci) v rámci nabízené licence pro kontrolu webového provozu
	Možnost rozšíření o kontrolu emailového provozu včetně šifrování emailové komunikace a ochraně proti ztrátě dat, tzv. DLP pouze zakoupením licence. Dva nezávislé skenovací AV enginy (různí výrobci) v rámci nabízené licence
	Umožňuje nasazení v clusteru Active/Active nebo Active/Passive s možností redundantního propojení boxů/LACP v rámci propojení boxů, přičemž v režimu A/P není nutné pro pasivní HW applianci kupovat licenci