	Minimální požadované parametry
Základní konfigurace Firewall	
Výkon	FW propustnost: 74 Gbps
	FW IMIX propustnost: 32 Gbps
	IPS propustnost: 29 Gbps
	Počet současných spojení alespoň: 16 500 000
	Počet nových spojení za sekundu: 367 500
	IPSec VPN propustnost: 62 Gbps
	Propustnost při zapnutých funkcích FW, IPS, Application Control a AV: 6,2 Gbps
Požadavky na HW	
	Integrovaný SSD disk (alespoň 240 GB)
	min. 4xRJ45 metalických portů (vč. 2x bypass páru)
	min. 4x2,5G metalických portů
	min. 4x10G SFP+ port
	Možnost redundantního zdroje napájení
	min. 1x RJ45 management port
	min. 2x USB 3.0 port
	možnosti rozšíření konektivity o jednotlivé moduly:
	o min. 8x RJ45 metalických portu
	o min. 8x SFP 1 GbE
	o min. 4x SFP+ 10GbE
	o min. 4x RJ45 (2x bypass pár)
	o min. 4x RJ45 PoE+
	o min. 4x 2.5 GbE RJ45 PoE
	o VDSL2 modul pro DSL připojení
	velikost v racku: 1U
Obecná specifikace	
	Certifikace ISCA Labs v oblasti Firewall
	Řešení dosáhlo hodnocení alespoň 4,6bodu v Gartner Peer Insight pro oblast Network Firewalls (hodnocení vypočteno na základě více než 800hodnocení od zákazníků)
	Produktové certifikace CB, CE, UKCA, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel, CCC, BSMI, TEC, SDPPI
	Řešení musí nabízet správu WiFi AP od stejného výrobce on box (integrovaný WiFi controler na firewallu) nebo správu přes centrální management FW
	Řešení disponuje funkcí tzv. Selective HTTPS Scanning, která umožňuje správci vybrat určitý HTTPS obsah, na kterém má být provedeno skenování a kontrola protokolu SSL.
	Řešení poskytuje vhled do uživatelské aktivity tzv. User Threat Quocientem – automatickým nástrojem, který uděluje skóre rizikovosti jednotlivým uživatelům
	Řešení musí umožnit 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 automaticky restriktivní politiky na konkrétní zařízení, dokud není hrozba z daného zařízení odstraněna.
	Řešení musí umožnit identifikaci všech aplikací, které běží na koncové stanici a v rámci FW uplatnit zvolenou politiku per aplikace .
	Firewallu musí umožňovat vyčítat identitu uživatelů pro autentizaci provozu pomocí antimalware agenta instalovaného na koncových strojích.

	FW musí mít integrovaný tester pro FW a web filter politiky
	Řešení musí nabízet on-box reporting
	Součástí nabízené licence musí být i licence pro cetrální správu vícero HW firewallů
	Centrální správa musí umožnit spravovat jak firewally, tak i stávající antimalware řešení Sophos provozovaných u zákazníka
	Centrální správa řešení nevyžaduje instalaci dodatečných zařízení ať už fyzických nebo virtuálních do infrastruktury zákazníka
	Podpora Wildcard pro Domain Name Host Objects
	Nabízená licence nesmí omezovat počet sestavených VPN
Funkcionality	
	Zahrnuje ochranu pomocí Intrusion Prevention (IPS) - možnost definování vlastních signatur
	Zahrnuje cloud sandbox, datacentrum, kde jsou zpracovány podezřelé vzorky musí být umístěno v zemích EU
	Zahrnuje ochranu proti zero-day hrozbám postavenou na algoritmech strojového učení, umělé inteligence a sandboxingu
	Zahrnuje licenci rp ochranu webových aplikací pomocí Web Application Firewall a reverzní proxy
	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
	Zahrnuje licenci pro kontrolu emailového provozu včetně šifrování emailové komunikace a nabízí funkcionalitu pro ochranu proti ztrátě dat, tzv. DLP. Ochrana emailové komunikace zahrnuje i dva nezávislé skenovací AV enginy (různí výrobci) v rámci nabízené licence
	Umožňuje nasazení v clusteru Active/Active nebo Active/Passive, přičemž v režimu A/P není nutné pro pasivní HW applianci kupovat licenci
	Fyzická zařízení nabízí hardwarovou akceleraci
	SD-WAN routing na základě zdrojové/cílové IP, aplikací, uživatelů
Služby	**technická podpora od dodavatele na 5MD v níže uvedených činnostech**
	Analýza konfigurace současného řešení a zjištění podrobností o provozu v síti
	Aplikace best practice, update firmware, instalalace do testovacího prostředí
	Sestavení FW politik, konzultace se zákazníkem. Součástí je příprava až 2000 politik, 50x site ot site tunel, uživatelská VPN včetně autentizace proti back end zákazníka
	Implementace do produkčního prostředí, nasazení politik, výměna současného řešení, otestování
	trabelshooting
	součinnost s odběratelem po dobu určených 5MD
	zaškolení obsluhy a ovládání