Firewally - Fortinet FortiGate 400F	Dodavatelem nabízená hodnota (vyplní dodavatel, v případě, že splňuje parametr, uvede ANO)	Poznámka
HW parametry		
Počet síťových rozhraní copper, RJ45 10/100/1000 - 16x	Ano	
Počet rozhraní GE SFP – 8x	Ano	
Dedikovaný konzolový port – 1x	Ano	
Dedikované porty pro komunikaci v režimu vysoké dostupnosti 10 GE SFP+ - 4x	Ano	
Dedikované porty pro správu – 2x	Ano	
USB port umožňující připojení USB flash paměti pro zálohování konfigurace, zároveň umožňující připojení USB modemu pro záložní připojení internetu – 1x	Ano	
Výkonnostní parametry		
Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B - minimálně 79 Gbps, 78 Gbps, 70 Gbps	Ano	
Latence firewallu (64 B UDP paket) - maximálně 4,5 µs	Ano	
Počet naráz otevřených spojení – minimálně 7 600 000	Ano	
Počet nových spojení za sekundu - 500 000	Ano	
Počet firewall pravidel 10 000	Ano	
Podpora virtualizace až 10 oddělených kontextů	Ano	
Podpora funkce bezdrátový kontrolér – minimálně 500 access pointů (AP)	Ano	min. 500 u bridge mode
Podpora funkce kontroleru minimálně pro 70 ks PoE switchů stejného výrobce (pro připojení wifi AP).	Ano	
Networking a vysoká dostupnost		
Podpora režimu vysoké dostupnosti Active-Active, Active-Passive, Clustering	Ano	
Režim fungování L2 – transparentní režim, L3 – NAT/Router	Ano	
Podpora VLAN	Ano	
Podopora multicast, vytváření politiky pro multicast routování	Ano	
Podpora 802.3ad link aggregation	Ano	
Funkce Load Balancing – rozdělování zátěže směrující na virtuální IP na reálné servery, podpora health check funkcí, podpora SSL offloading	Ano	
Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace	Ano	
Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP	Ano	
Policy-based routing	Ano	
Podpora uplatňování základních pravidel pro kontrolu na přístupové vrstvě (NAC pravidla, politiky)	Ano	
Zařízení podporuje možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky (SD-WAN).	Ano	
Funkce SD-WAN není licenčně omezena. V rámci nabízeného řešení bude v podobě, jež umožňuje neomezené využívání i v případě, že dojde k nárůstu počtů zařízení komunikujících skrze SD-WAN do internetu, tak i v případě, že dojde k navýšení počtu konektivit a jejich rychlostí.	Ano	
Integrované SD-WAN řešení podporuje 200 ks virtuálního rozhraní, které sdružuje konektivitu a jsou na něj uplatněna pravidla provozu a routingu.	Ano	
Funkce SSL VPN		
Podpora možnosti připojení klientů do VPN pomocí proprietární SSL VPN.	Ano	
Aplikace pro VPN podporuje nejběžnější operační systémy, jako například: Windows, macOS, Linux, Android nebo IOS.	Ano	
Podpora klientského připojení do VPN na úrovni webového portálu, pomocí standardního internetového prohlížeče.	Ano	
Možnost zabezpečení připojení do VPN vynucením dvoufaktorového ověření pomocí proprietární aplikace dostupné pro Android i IOS, např. CISCO DUO.	Ano	
Zařízení umožňuje rozšíření pro využití dostupného dvoufaktorového ověření.	Ano	
Vynucení ověření klientského certifikátu pro zvýšení zabezpečení.	Ano	
Počet současně navázaných SSL VPN tunelů: max 5 000	Ano	
Propustnost SSL VPN: minimálně 3,4 Gbps	Ano	
Funkce IPsec VPN		
Podpora site-to-site VPN	Ano	
Podpora klientských VPN	Ano	
VPN klienta pro koncové stanice (Windows, MacOS) lze stáhnout z veřejně dostupných webových stránek	Ano	
Funkce klientských IPSec VPN není licencovaná na počet uživatelů.	Ano	
Počet IPSEC VPN tunelů typu lokalita-lokalita: 2000	Ano	
Počet klientských IPSEC VPN tunelů: 50 000	Ano	
Propustnost IPsec VPN 55 Gbps (měřeno při AES256-SHA256)	Ano	
Podpora konfigurace redundantních IPsec VPN tunelů za pomoci statického směrování	Ano	
Podpora konfigurace redundantních IPsec VPN tunelů za pomoci dynamického směrování	Ano	
Podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace	Ano	
Podpora VXLAN	Ano	
Podpora L2TP, PPTP, GRE	Ano	
Podpora dynamických routovacích protokolů OSPF, BGP ve VPN IPsec	Ano	
UTM funkce		
Funkce detekce aplikací na L7 (Application Control)		
o Detekce známých aplikací na základě signatur	Ano	
o Signaturový database automaticky aktualizované výrobcem	Ano	
o Více než 5200 podporovaných aplikací	Ano	
o Pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login atd. (relevantní k dané aplikaci)	Ano	
o Možnost tvorby vlastních signatur	Ano	
o Detekované aplikace je možné: povolit, monitorovat, blokovat	Ano	
o Na základě typu aplikace je možné omezit šířku pásma pro danou aplikaci	Ano	
o Funkce detekce aplikací se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně možnost využití v rámci tzv. NGFW pravidel popsaných výše.	Ano	
Funkce detekce a potlačení narušení (IPS/IDS)		
o Signatury automaticky aktualizované výrobcem	Ano	
o 11 000 rozpoznávaných hrozeb (signatur) definovaných výrobcem	Ano	
o Možnost tvorby vlastních signatur	Ano	
o Funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům	Ano	
o Funkce tzv. fail-open - při přetížení IPS je možné definovat, zda dojde k blokaci nebo propuštění provozu	Ano	
o Propustnost IPS inspekce 12 Gbps	Ano	
Funkce antivirové kontroly		
o Ochrana před škodlivým kódem (malware, trojské koně apod.), včetně ochrany před polymorfním kódem	Ano	
o Signatury automaticky aktualizované výrobcem	Ano	
o AV kontrola rozšířena o inspekci tzv. sandbox technikou, poskytovanou formou služby výrobcem FW (licence je součástí dodávky)	Ano	
o Možnost rozšíření o inspekci tzv. sandbox technikou formou lokálné HW appliance stejného výrobce	Ano	
o Propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním - 9 Gbps	Ano	
o Funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.	Ano	
o Podpora služby výrobce, která umožní detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů	Ano	
o Funkce odstranění škodlivého aktivního obsahu z dokumentů kancelářských aplikací.	Ano	
Funkce ochrany před únikem citlivých informací (DLP)		
o analýza běžných typů dokumentů a protokolů	Ano	
o Možnost definice pravidel na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum	Ano	
Podpora SSL dekrypce		
o Podpora SSL dekrypce a inspekce pro ochranu koncových zařízeních anebo serverů	Ano	
o Funkce SSL dekrypce se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.	Ano	
o Propustnost SSL inspekce 8 Gbps	Ano	
Podpora pravidel pro obranu proti útokům typu DoS		
o Pravidla proti DoS útokům na základě politik, které se aplikují na konkrétní interface zařízení.	Ano	
o Podpora detekce anomálií na 3. a 4. vrstvě	Ano	
o Podpora např. TCP SYN FLOOD, ICMP FLOOD, SCTP SRC SESSION	Ano	
o Funkce umožňuje provoz nejen blokovat, ale i sledovat pro možnost orientace na síti	Ano	
Explicitní proxy		
o Podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)	Ano	
o Podpora transparentního ověřování uživatele proti MS AD protokolem Kerberos	Ano	
o Funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta	Ano	
o Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatelů na terminálovém serveru	Ano	
Firewall		
Možnost nastavovat firewall politiku na základě geografických údajů	Ano	
Aplikace firewall policy na známé internetové služby. Databáze těchto služeb je pravidelně aktualizována výrobcem	Ano	
Možnost snadné integrace cloudové služby. Podpora: MS Azure, Amazon Web Services, Google Cloud	Ano	
Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroleru	Ano	
Viditelnost do provozu na aplikační úrovni	Ano	
Možnost dynamického stahování externích seznamů IP adres a jejich následné použití ve firewall policy	Ano	
Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo).	Ano	
Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu	Ano	
Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.	Ano	
Traffic Shaping, QoS v podporou prioritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii	Ano	
Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu	Ano	
Podpora funkce reverzní proxy	Ano	
Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů	Ano	
Podpora zabezpečení administrátorských účtů pomocí dvoufaktorového ověření	Ano	
Integrovaný kontroler bezdrátových sítí		
Wifi kontroler integrovaný do NGFW platformy	Ano	
Bezdrátová síť (SSID) může být reprezentována virtuálním síťovým rozhraním – provoz tunelován z AP do kontroleru	Ano	
Podpora bezpečnostních profilů (AV, AppControl, WebFilter, DLP) přímo na wifi kontroleru	Ano	
Podpora SSL dekrypce uživatelského provozu přímo na wifi kontroleru	Ano	
Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení	Ano	
Možnost volby z různých modelů (802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor, WiFi 6)	Ano	
Podpora BSS Coloring	Ano	
On-wire rogue AP detekce a mitigace	Ano	
Podpora fast-roamingu (802.11 k,v,r)	Ano	
Podpora více PSK u jednoho SSID	Ano	
Podpora IPSEC tunelu pro šifrování dat plane (uživatelských dat)	Ano	
Podpora WPA3 protokolu	Ano	
Multi-tenance (virtualizace)		
Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext je plnohodnotné řešení včetně oddělného GUI, management účtů atp.	Ano	
Každý virtuální kontext je zároveň samostatným wifi kontrolerem	Ano	
Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)	Ano	
Management		
FW cluster je možné plnohodnotně spravovat pomocí webového rozhraní HTTPS, lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici	Ano	
Podpora SNMP včetně SNMP MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě	Ano	
Podpora otevřeného API (možnost integrace wybraných funkcí do stávající management infrastruktury)	Ano	
Napojení na SIEM zadavatele	Ano	FG má otevřené API, takže napojení na SIEM by neměli být problém je ale potřeba vědět konkrétní SIEM a zjistit kompatibilitu
Podpora		
Technická podpora prostřednictvím webového portálu/telefonu poskytována 8 hodin denně, 5 dnů v týdnu	Ano	