Příloha č. 1 kupní smlouvy

Technická specifikace

k nadlimitní veřejné zakázce na dodávky s názvem „Pořízení a implementace NGFW II“.

Zadavatel poptává redundantní zařízení typu Next Generation Firewall (NGFW), Zero Trust klient pro VPN, 2 faktorovou autentizaci pro VPN klienta a implementaci dle specifikace níže v tabulkách.

1. Požadavky na zařízení NGFW

Požadavek	Splněno ANO/NE	Popis splnění
Obecné podmínky		
Bezpečnostní zařízení typu NGFW	ANO	Bezpečnostní zařízení typu NGFW
Dvě fyzická zařízení v redundantním režimu	ANO	Dvě fyzická zařízení v redundantním režimu
Výrobce zařízení	Fortinet, Inc.	Výrobce Fortinet, Inc. se sídlem v USA
Typové označení zařízení	**FG-900G** **FC-10-FG9H0-950-02-60**	FortiGate 900G Series FG-900G NG Firewall Předplatné Unified Threat Protection (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) – 60 měsíců
HW požadavky		
HW provedení o maximální velikosti 1U (VM provedení ani jiné software řešení není akceptovatelné)	ANO	HW provedení s velikostí 1U
Podpora režimu vysoké dostupnosti v režimech active/active a active/passive (v tomto režimu může být provozován HA cluster)	ANO	Podpora režimu vysoké dostupnosti v režimech active/active a active/passive (v tomto režimu může být provozován HA cluster)
Duální napájení s možností výměny napájecího zdroje za chodu zařízení (redundantní zdroj je součástí dodávaného zařízení včetně napájecí kabeláže pro použití v CZ)	ANO	Duální napájení s možností výměny napájecího zdroje za chodu zařízení (redundantní zdroj je součástí dodávaného zařízení včetně napájecí kabeláže pro použití v CZ)
HW s integrovaným TPM řešením	ANO	HW s integrovaným TPM řešením
Minimální počet vysokorychlostních síťových rozhraní: 4x 10/25 GbE SFP28 4x 1/10 GbE SFP/SFP+	ANO	Počet vysokorychlostních síťových rozhraní: 4x 25/10 GbE SFP28/SFP+ Ultra Low Latency 4x 10/1 GbE SFP+/SFP
Minimálně 12x 1 GbE RJ45 síťová rozhraní	ANO	16x 1 GbE RJ45 síťová rozhraní 8x 1 GbE SFP síťová rozhraní
Dedikovaný HA RJ45 port, dedikovaný RJ45 management port a dedikovaný RJ45 konzolový port	ANO	Dedikovaný HA RJ45 port, dedikovaný RJ45 management port a dedikovaný RJ45 konzolový port
Celková minimální propustnost stavového firewallu pro IPv4 a IPv6 provoz je alespoň 150 Gbps při IMIX 7:4:1 64:512:1518B.	ANO	Výrobce propustnost v IMIX neuvádí. Propustnost stavového firewallu pro IPv4 i IPv6 provoz je 164 Gbps (1518B), 163 Gbps (512B), 153 Gbps (64B). Z toho vyplývá, že v jakékoli kombinaci velikosti paketů (včetně IMIX vzorku) je rychlost větší než 153 Gbps.
Kapacita současně navázaných spojení firewallu je alespoň 15 000 000 a kapacita nově sestavených spojení za sekundu je alespoň 550 000 spojení za sekundu	ANO	Kapacita současně navázaných spojení firewallu je 16 000 000 a kapacita nově sestavených spojení za sekundu je 720 000 spojení za sekundu

Propustnost NGFW pro IPSEC VPN je alespoň 10 Gbps (paket o velikosti 512B při šifrování AES256-SHA256)	ANO	Propustnost NGFW pro IPSEC VPN je 55 Gbps (paket o velikost 512B při šifrování AES256-SHA256)
Propustnost NGFW pro SSL VPN je alespoň 10 Gbps (certifikát 2048b)	ANO	Propustnost NGFW pro SSL VPN je 10 Gbps (certifikát RSA-2048)
Propustnost NGFW při zapnuté funkci SSL inspekce je alespoň 15 Gbps	ANO	Propustnost NGFW při zapnuté funkci SSL inspekce je 16,7 Gbps
Minimální kapacita spojení za sekundu, které je možné prověřit SSL inspekcí je 15 000	ANO	Kapacita spojení za sekundu, které je možné prověřit SSL inspekcí je 18 000
Propustnost NGFW Threat Prevention je alespoň 20 Gbps	ANO	Propustnost NGFW při ochraně před hrozbami - současná kombinace funkcí stavového firewallu, IPS (včetně zapnutého logování), analýzy aplikací a ochrany před škodlivým kódem je 20 Gbps
Propustnost NGFW při aplikační inspekci je alespoň 70Gbps, kdy aplikační kontrola používá HTTP transakce ≤64kB	ANO	Propustnost aplikační inspekce při zapnutém IPS a logování provozu je 74,8 Gbps při HTTP transakcích 64kB
Minimální počet současně připojených uživatelů SSL VPN je alespoň 2 000 a IPSec VPN klientů alespoň 5 000 (tyto počty uživatelů nejsou omezeny licenčně)	ANO	Počet současně připojených uživatelů SSL VPN je 10 000 a IPSec VPN klientů 50 000 (tyto počty uživatelů nejsou omezeny licenčně)
Minimální počet současně sestavených Site-To-Site IPSEC tunelů je alespoň 1000	ANO	Počet maximálně současně sestavených Site-To-Site IPSEC tunelů je 2000
Konfigurační rozhraní je integrované do NGFW zařízení, a to jak v grafické, tak CLI podobě bez licenčního omezení na počet administrátorů. CLI rozhraní umožňuje plnou administraci zařízení.	ANO	Konfigurační rozhraní je integrované do NGFW zařízení, a to jak v grafické, tak CLI podobě bez licenčního omezení na počet administrátorů. CLI rozhraní umožňuje plnou administraci zařízení.
Možnost logické segmentace HW s použitím tzv. virtuálních kontextů v minimálním počtu deseti současně běžících kontextů v ceně zařízení; každý virtuální kontext musí pracovat izolovaně. Řešení umožňuje interně propojit jednotlivé logické kontexty na úrovni L2 (sdílení broadcast domény) i L3 včetně NGFW inspekce provozu mezi kontexty.	ANO	Možnost logické segmentace HW s použitím tzv. virtuálních kontextů v počtu deseti současně běžících kontextů v ceně zařízení; každý virtuální kontext pracuje izolovaně. Řešení umožňuje interně propojit jednotlivé logické kontexty na úrovni L2 (sdílení broadcast domény) i L3 včetně NGFW inspekce provozu mezi kontexty.
Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46	ANO	Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46
Možnost nasazení ve všech z následujících režimů: L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline)	ANO	Možnost nasazení ve všech z následujících režimů: L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline)
Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On	ANO	Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On
Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů	ANO	Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů
Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu	ANO	Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu
Funkce QoS, traffic shaping a SD-WAN miminálně v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s	ANO	Funkce QoS, traffic shaping a SD-WAN miminálně v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s

možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek		možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek
Podpora funkcí VPN brány - IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); - SSL VPN pro klientský přístup s podporou tunelového režimu včetně zdarma dostupného klienta pro osobní počítače i mobilní platformy a zároveň NGFW podporuje portálový režim pro bezklientský přístup.	ANO	Podpora funkcí VPN brány - IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); - SSL VPN pro klientský přístup s podporou tunelového režimu včetně zdarma dostupného klienta pro osobní počítače i mobilní platformy a zároveň NGFW podporuje portálový režim pro bezklientský přístup.
Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3	ANO	Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3
Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků	ANO	Antivirový engine být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků
Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče.	ANO	Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče.
Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace	ANO	Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora více než 5000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace
Možnost definice zakázaných slov pro vyhledávání na internetu	ANO	Možnost definice zakázaných slov pro vyhledávání na internetu
Podpora funkce safe search pro populární vyhledavače	ANO	Podpora funkce safe search pro populární vyhledavače
Funkce kategorizace webových stránek (web filtering) s podporou kategorizace na skupiny jako jsou pracovní zájmy, osobní zájmy, hazard, pornografie, sdílená uložiště, stránky se škodlivým kódem, nově registrované domény atp, podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost	ANO	Funkce kategorizace webových stránek (web filtering) s podporou kategorizace na skupiny jako jsou pracovní zájmy, osobní zájmy, hazard, pornografie, sdílená uložiště, stránky se škodlivým kódem, nově registrované domény atp, podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost

autentizace uživatele pro určitou kategorii, možnost definice časových kvót pro uživatele a kategorie webu		autentizace uživatele pro určitou kategorii, možnost definice časových kvót pro uživatele a kategorie webu
Podpora kategorizace stremovaných videí a kanálů min. pro platformu Youtube a Vimeo	ANO	Podpora kategorizace stremovaných videí a kanálů pro platformu Youtube a Vimeo
Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů	ANO	Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů
Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času	ANO	Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času
Funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě vodoznaků, popisu regulárním výrazem atp.	ANO	Funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě vodoznaků, popisu regulárním výrazem atp.
Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů, součástí nabídky musí být 2 testovací HW/mobilní tokeny a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN	ANO	Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů, součástí nabídky jsou 2 testovací mobilní tokeny a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN
Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy	ANO	Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy
Podpora ICAP rozhraní pro obousměrnou integraci s externími servery	ANO	Podpora ICAP rozhraní pro obousměrnou integraci s externími servery
Podpora statického a dynamického směrování minimálně protokoly OSPF a BGP	ANO	Podpora statického a dynamického směrování protokoly OSPF a BGP
Podpora Policy Based Routing na základě IP adresy a aplikace (s možností definovat vlastní aplikace)	ANO	Podpora Policy Based Routing na základě IP adresy a aplikace (s možností definovat vlastní aplikace)
Podpora IPAM funkcionality pro správu přidělených IP adres z NGFW zařízení	ANO	Podpora IPAM funkcionality pro správu přidělených IP adres z NGFW zařízení
Podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí	ANO	Podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí
Analýza a zabezpeční DNS dotazů (ochrana před DNS posoningem), filtrování DNS dotazů na základě kategorizace	ANO	Analýza a zabezpeční DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace
Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu	ANO	Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu
Všechny výkonové a funkční parametry nabízeného zařízení musí být ověřitelné z veřejně dostupných zdrojů výrobce zařízení	ANO	Výkonové a funkční parametry je možné ověřit na následujících stránkách výrobce: Datasheet FG-900G: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-900g-series.pdf Návody a manuály pro FortiOS 7.4: https://docs.fortinet.com/product/fortigate/7.4
Záruka na nabízené zařízení je 24x7xNBD na 5 let od data dodání	ANO	Záruka na nabízené zařízení je 24x7xNBD na 5 let od data dodání

Podpora výrobce na nabízené zařízení a funkce v režimu 24x7 NBD a je součástí nabízeného zařízení na období 5 let	ANO	Podpora výrobce na nabízené zařízení a funkce v režimu 24x7 NBD a je součástí nabízeného zařízení na období 5 let
Všechny licence potřebné ke spuštění požadovaných funkcionalit musí být součásti dodávky každého zařízení	ANO	Všechny licence potřebné ke spuštění požadovaných funkcionalit jsou součásti dodávky každého zařízení
Pokud jsou funkcionality licencované na časové období, musí být součástí dodávky licence na 5 let od data dodání	ANO	Funkcionality licencované na časové období, jsou součástí dodávky licence na 5 let od data dodání

2. Požadavky na klient pro Zero Trust VPN přístup včetně management serveru

Požadavek	Splněno ANO/NE	Popis splnění
Obecné podmínky		
Management server jako VM appliance, případně aplikace pro Windows server	ANO	Management server jako VM appliance
Licence pro provoz minimálně 500 klientů	ANO	Licence pro provoz 500 klientů
Výrobce	Fortinet, Inc.	Výrobce Fortinet, Inc. se sídlem v USA
Typové označení	**FC2-10-EMS04-428-01-60**	FortiClient VPN/ZTNA Agent Subscriptions for 500 endpoints, includes on-prem EMS and FortiCare Premium.
Požadavky na centrální management klientů na koncových stanicích		
Podpora rozdělení jednotlivých spravovaných stanic dle typu stanice a přihlášeného uživatele	ANO	Podpora rozdělení jednotlivých spravovaných stanic dle typu stanice a přihlášeného uživatele
Možnost napojení na Active Directory s možností ověření koncových stanic proti AD během registrace k klienta k management řešení	ANO	Možnost napojení na Active Directory s možností ověření koncových stanic proti AD během registrace k klienta k management řešení
Možnost definice lokálních skupin uživatelů	ANO	Možnost definice lokálních skupin uživatelů
Komunikace s klienty zabezpečena pomocí certifikátů obnovovaných po každém odpojení klienta od management platformy	ANO	Komunikace s klienty zabezpečena pomocí certifikátů obnovovaných po každém odpojení klienta od management platformy
Tvorba instalačních balíčků klienta v prostředí centrálního managmentu	ANO	Tvorba instalačních balíčků klienta v prostředí centrálního managmentu
Centrální správa připojených klientů (upgrade a odinstalování klienta z koncové stanice)	ANO	Centrální správa připojených klientů (upgrade a odinstalování klienta z koncové stanice)
Možnost definice politik a profilů koncových stanic	ANO	Možnost definice politik a profilů koncových stanic
Politiky aplikované dle členství v AD skupině/lokální skupině	ANO	Politiky aplikované dle členství v AD skupině/lokální skupině
Přidělení politik a profilů klientovi dle detekovaného umístění klienta (firma, mimo firmu, atd.)	ANO	Přidělení politik a profilů klientovi dle detekovaného umístění klienta (firma, mimo firmu, atd.)
Možnost definovat pravidla zjišťující stav koncové stanice: - přítomnost zranitelností na nainstalovaném software - informace z Windows Security Centra (stav antivir software a stav interního firewallu) - přítomnost konkrétního procesu, souboru, záznamu v registru - přítomnost certifikátu včetně definice Subjectu/CN - detekce uživatelské identity, skupiny, IP rozsahu	ANO	Možnost definovat pravidla zjišťující stav koncové stanice: - přítomnost zranitelností na nainstalovaném software - informace z Windows Security Centra (stav antivir software a stav interního firewallu) - přítomnost konkrétního procesu, souboru, záznamu v registru - přítomnost certifikátu včetně definice Subjectu/CN - detekce uživatelské identity, skupiny, IP rozsahu

Nativní možnost distribuce výsledku kontroly stavu koncových stanic na poptávaný NGFW	ANO	Nativní možnost distribuce výsledku kontroly stavu koncových stanic na poptávaný NGFW
Nativní možnost distribuce telemetrických dat připojených klientů na poptávaný NGFW	ANO	Nativní možnost distribuce telemetrických dat připojených klientů na poptávaný NGFW
Požadavky na klienta		
Integrovaný Cloud Access Security Broker	ANO	Integrovaný Cloud Access Security Broker
Skener zranitelností	ANO	Skener zranitelností
Podpora automatického patchingu nalezených zranitelností	ANO	Podpora automatického patchingu nalezených zranitelností
Synchronizace webfilter profilu s NGFW	ANO	Synchronizace webfilter profilu s NGFW
IPSEC VPN klient s podporou 2FA	ANO	IPSEC VPN klient s podporou 2FA
SSL VPN s ověřením proti SAML IdP	ANO	SSL VPN s ověřením proti SAML IdP
SSL VPN klient podporující 2FA s NGFW	ANO	SSL VPN klient podporující 2FA s NGFW
Podpora always-on VPN - automatické připojení k VPN	ANO	Podpora always-on VPN - automatické připojení k VPN
Podpora připojení k VPN před přihlášením k operačnímu systému Windows	ANO	Podpora připojení k VPN před přihlášením k operačnímu systému Windows
Split tunneling na základě rozpoznávání aplikací	ANO	Split tunneling na základě rozpoznávání aplikací
ZTNA agent - vzdálený přístup bez připojení k VPN	ANO	ZTNA agent - vzdálený přístup bez připojení k VPN
Definice ZTNA pravidel manuálně nebo pomocí centrálního mangementu	ANO	Definice ZTNA pravidel manuálně nebo pomocí centrálního mangementu
ZTNA komunikace zabezpečena certifikátem obnovovaným po každém odpojení klienta od management platformy	ANO	ZTNA komunikace zabezpečena certifikátem obnovovaným po každém odpojení klienta od management platformy
Podpora centrálního logování z klienta na management server	ANO	Podpora centrálního logování z klienta na management server
Další požadavky		
Všechny výkonové a funkční parametry nabízeného řešení musí být ověřitelné z veřejně dostupných zdrojů výrobce zařízení	ANO	Výkonové a funkční parametry je možné ověřit na následujících stránkách výrobce: Datasheet FortiClient: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/forticlient.pdf Návody a manuály pro FortiClient a EMS: https://docs.fortinet.com/product/forticlient/7.2
Podpora výrobce na nabízené řešení funguje v režimu 24x7 NBD a je součástí nabízeného řešení na období 5 let	ANO	Podpora výrobce na nabízené řešení funguje v režimu 24x7 NBD a je součástí nabízeného řešení na období 5 let
Všechny licence potřebné ke spuštění požadovaných funkcionalit musí být součásti dodávky	ANO	Všechny licence potřebné ke spuštění požadovaných funkcionalit jsou součásti dodávky
Pokud jsou funkcionality licencované na časové období, musí být součástí dodávky licence na 5 let od data dodání	ANO	Funkcionality licencované na časové období, jsou součástí dodávky licence na 5 let od data dodání

3. Požadavky na dvoufaktorovou OTP aplikaci

Požadavek	Splněno ANO/NE	Popis splnění
Obecné podmínky		
Licence pro provoz minimálně 500 klientů	ANO	Licence pro provoz 500 klientů
Výrobce	Fortinet, Inc.	Výrobce Fortinet, Inc. se sídlem v USA
Typové označení	**FTM-ELIC-500**	FortiTokenMobile (Electronic License) for 500 users)
Požadavky na 2FA OTP		

OTP aplikace s podporou Push notifikací pro 2FA autentizaci dle RFC 6238, RFC 4226	ANO	OTP aplikace s podporou Push notifikací pro 2FA autentizaci dle RFC 6238, RFC 4226
Aplikace je podporována platformami iOS, Android, Windows 10 a 11 a Windows Universal Platform	ANO	Aplikace je podporována platformami iOS, Android, Windows 10 a 11 a Windows Universal Platform
Aplikace je nativně určena pro 2FA autentizaci spolu s poptávaným NGFW a Zero Trust řešením	ANO	Aplikace je nativně určena pro 2FA autentizaci spolu s poptávaným NGFW a Zero Trust řešením
Samotnou aplikaci je možné volně stáhnout na "tržištích" provozovaných přímo tvůrci podporovaných operačních systémů	ANO	Samotnou aplikaci je možné volně stáhnout na "tržištích" provozovaných přímo tvůrci podporovaných operačních systémů
Aplikaci je možné aktivovat zadáním kódu v aplikaci nebo načtením QR kódu přímo z aplikace	ANO	Aplikaci je možné aktivovat zadáním kódu v aplikaci nebo načtením QR kódu přímo z aplikace
Podpora napojení na sandboxing applianci za účelem rozboru zkoumaných souborů na přítomnost škodlivého kódu	ANO	Podpora napojení na sandboxing applianci za účelem rozboru zkoumaných souborů na přítomnost škodlivého kódu
Další požadavky		
Všechny výkonové a funkční parametry nabízeného řešení musí být ověřitelné z veřejně dostupných zdrojů výrobce zařízení	ANO	Výkonové a funkční parametry je možné ověřit na následujících stránkách výrobce: Datasheet FortiToken: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortitoken.pdf Návody a manuály pro FortiToken: https://docs.fortinet.com/product/fortitoken
Všechny licence potřebné ke spuštění požadovaných funkcionalit musí být součásti dodávky	ANO	Všechny licence potřebné ke spuštění požadovaných funkcionalit jsou součásti dodávky
Pokud jsou funkcionality licencované na časové období, musí být součástí dodávky licence na 5 let od data dodání	ANO	Funkcionality licencované na časové období, jsou součástí dodávky licence na 5 let od data dodání

4. Instalace, konfigurace

Požadavky na implementaci a nastavení		
Podpora souběhu nového FW společně se starým tak, aby nedošlo ke globálnímu výpadku služby	ANO	Podpora souběhu nového FW společně se starým tak, aby nedošlo ke globálnímu výpadku služby
Konfigurace VPN pro Remote Access a SiteToSite pro 2 lokality	ANO	Konfigurace VPN pro Remote Access a SiteToSite pro 2 lokality
Vzorová instalace VPN klienta, včetně návodu na instalaci a konfiguraci na platformách iOS, Android a Windows 10/11.	ANO	Vzorová instalace VPN klienta, včetně návodu na instalaci a konfiguraci na platformách iOS, Android a Windows 10/11.
Instalace a konfigurace Dvoufaktorové OTP na NGWF, návod na instalaci pro iOS, Android a Windows 10/11.	ANO	Instalace a konfigurace Dvoufaktorové OTP na NGWF, návod na instalaci pro iOS, Android a Windows 10/11.
Instalace management aplikace pro firewally	ANO viz „Další požadavky“ – bod 2.	Management aplikace (webové konfigurační rozhraní) je součástí operačního systému firewallu.
Konfigurace NAT, Port Forwarding dle konfigurace z nyní používaného firewallu CISCO ASA5585	ANO	Konfigurace NAT, Port Forwarding dle konfigurace z nyní používaného firewallu CISCO ASA5585
Předání provozní dokumentace a analýzy rizik na řešení	ANO	Předání provozní dokumentace a analýzy rizik na řešení

Další požadavky:

1. Konverze konfigurace z nyní používaného firewallu CISCO ASA5585 včetně FMC na nabízené řešení.
2. Instalace management aplikace pro firewally – management aplikace nebude samostatně instalována, její instance je nedílnou součástí operačního systému firewallu a běží přímo na firewallu.
3. Instalace management aplikace pro Zero Trust klienta.
4. Vzorová instalace Zero Trust klienta, včetně návodu na instalaci a konfiguraci na platformách iOS, Android a Windows 10/11.
5. Instalace a konfigurace Dvoufaktorové OTP na NGWF, návod na instalaci pro iOS, Android a Windows 10/11.

Svým podpisem stvrzuji, že mnou nabízené plnění dle kupní smlouvy má výše nabízené vlastnosti.

V Praze dne – dle elektronického podpisu

.....

Jiří Volf, jednatel

ARISTIA, spol. s r.o.