**Příloha č. 6a zadávací dokumentace ve veřejné zakázce**

**„ZVÝŠENÍ KYBERNETICKÉ BEZPEČNOSTI MĚSTA LOVOSICE“**

**ČÁST 01: OCHRANA SÍTĚ A PERIMETRU**

**TECHNICKÁ SPECIFIKACE**

# PŘEDMĚT PLNĚNÍ

*Zadavatel tímto informuje, že v rámci své infrastruktury využívá technologii****Next-Generation Firewall (NGFW)****od výrobce****Fortinet****, virtualizační platformu* ***VMware****. Uchazeči jsou proto povinni přizpůsobit své návrhy řešení firewallu, konfigurace a implementační postupy této platformě tak, aby byla zajištěna plná kompatibilita a optimalizace funkcionality v souladu s aktuálními standardy a specifikacemi.*

Součástí plnění je dodávka a implementace všech dále uvedených zařízení, jejich konfigurace a vzájemná orchestrace s vyjmenovanými bezpečnostními technologiemi zadavatele. Další součástí je poskytnutí záruky, záruční a technické podpory výrobce a předplatné bezpečnostních funkcí na dobu 60 měsíců.

Žádné z nabízených řešení nesmí být v době podání nabídky v režimu End of sales / End of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.

**Požadavky na uchazeče:**

* Vybraný dodavatel je povinen zadavateli na písemnou výzvu předložit formou elektronické komunikace certifikát výrobce o partnerství a oprávnění dodavatele pro nabízené technologie

|  |  |  |
| --- | --- | --- |
| **ID** | **Popis** | **Množství** |
| 1 | Firewall | 2 ks (zapojení do HA) |
| 2 | Agregační switch | 2 ks |
| 3 | Switche 24 Full PoE | 5 ks |
| 4 | Switche 48 PoE | 2 ks |
| 5 | Ověřovací autorita | 1 ks |
| 6 | Mobilní tokeny pro 2FA | pro 50 uživatelů |
| 7 | VPN s centrální správou | pro 50 uživatelů |
| 8 | Konfigurační práce | soubor |

**Dodržení termínu instalace a konfigurace do 90 dnů od podpisu smlouvy.**

# TECHNICKÁ SPECIFIKACE

## Firewall

|  |  |
| --- | --- |
| **Firewall** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| **Obecné požadavky na platformu** | |
| Platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC |  |
| Zařízení ve formátu HW appliance o velikosti 1RU |  |
| Zařízení musí být dodáno v režimu vysoké dostupnosti. Bez výpadkový cluster bude sestaven celkem ze 2 zařízení – součástí dodávky musí být všechna zařízení včetně všech potřebných licencí |  |
| Zařízení musí být vybavené redundantním napájecím zdrojem. |  |
| **HW parametry** | |
| Počet rozhraní 10 GE SFP+ – min 4x |  |
| Počet rozhraní 1 GE SFP – min 8x |  |
| Počet rozhraní 1 GE RJ45 – min 16x |  |
| Dedikovaný konzolový port – min 1x |  |
| Dedikovaný port pro komunikaci v režimu vysoké dostupnosti RJ45 - min 1x |  |
| USB port umožňující připojení USB flash paměti pro zálohování konfigurace, zároveň umožňující připojení USB modemu pro záložní připojení internetu – min 1x |  |
| **Výkonnostní parametry** | |
| Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 38 Gbps, 38 Gbps, 27 Gbps |  |
| Latence firewallu (64 B UDP paket) - max 3,20 mikro sec |  |
| Počet naráz otevřených spojení – min 2 500 000 |  |
| Počet nových spojení za sekundu - min. 130 000 |  |
| Podpora virtualizace, min 10 oddělených kontextů |  |
| Podpora funkce bezdrátový kontrolér – min 128 |  |
| Podpora funkce integrovaného kontroléru pro switche, min 48. |  |
| **Networking a Vysoká dostupnost (HA)** | |
| Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru |  |
| Režim fungování L2 – transparentní režim, L3 – NAT/Router |  |
| Podpora VLAN |  |
| Podpora multicast, vytváření politiky pro multicast routování |  |
| Podpora 802.3ad link aggregation |  |
| Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading |  |
| Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace |  |
| Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP |  |
| Policy-based routing |  |
| Zařízení musí podporovat 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). |  |
| Funkce SD-WAN nesmí být licenčně omezeno. V rámci nabízeného řešení musí být dodáno v podobě, jenž umožňuje neomezené využívání i v případě, že dojde k nárůstu počtů zařízeních komunikující skrze SW-WAN do internetu, tak i v případě, že dojde k navýšení počtu konektivit a jejich rychlosti. |  |
| **Funkce SSL VPN** | |
| Nabízené řešení musí podporovat možnost připojení klientů do VPN pomocí proprietární SSL VPN. Aplikace pro do VPN musí být podporována nejběžnějšími operačními systémy, jako například: Windows, macOS, Linux, Android nebo iOS. |  |
| Podpora bez klientského připojení do VPN na úrovni webového portálu, pomocí standardního internetového prohlížeče. |  |
| Možnost zabezpečení připojení do VPN vynucením dvou faktorového ověření. Například pomocí emailu, SMS, hardwarovou klíčenkou, nebo proprietární aplikace dostupná pro Android i iOS. |  |
| Zařízení musí umožňovat rozšíření pro využití dostupného dvou faktorového ověření |  |
| Vynucení ověření klientského certifikátu pro zvýšení zabezpečení. |  |
| Minimální počet současně navázaných SSL VPN tunelů: 500 |  |
| Minimální propustnost SSL VPN: 1,4 Gbps |  |
| **Funkce IPsec VPN** | |
| Podpora site-to-site VPN |  |
| Podpora klientských VPN |  |
| Dostupnost VPN klienta pro koncové stanice (Windows, MacOS) z veřejně dostupných webových stránek |  |
| Funkce klientských IPSec VPN nesmí být licencovaná na počet uživatel. V opačném případě požadujeme dodání neomezené licence. |  |
| Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 1800 |  |
| Minimální počet klientských IPSEC VPN tunelů: 15 000 |  |
| Propustnost IPSec VPN min. 34 Gbps (měřeno při AES256-SHA256) |  |
| Podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování |  |
| Podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování |  |
| Podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace |  |
| Podpora VXLAN |  |
| Podpora L2TP, PPTP, GRE |  |
| Podpora dynamických routovacích protokolů OSPF, BGP ve VPN IPsec |  |
| **UTM funkce** | |
| **Funkce detekce aplikací na L7 (Application Control)** | **-** |
| Detekce známých aplikací na základě signatur |  |
| Signaturový database automaticky aktualizované výrobcem |  |
| Alespoň 4 000 podporovaných aplikací |  |
| Pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login atd. (relevantní k dané aplikaci) |  |
| Možnost tvorby vlastních signatur |  |
| Na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci |  |
| Funkce detekce aplikací se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše. |  |
| Minimální propustnost funkce application control: 6.5 Gbps |  |
| **Funkce detekce a potlačení narušení (IPS/IDS)** | **-** |
| Signatury automaticky aktualizované výrobcem |  |
| Alespoň 11 000 rozpoznávaných hrozeb (signatur) definovaných výrobcem |  |
| Možnost tvorby vlastních signatur |  |
| Funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům |  |
| Ffunkce tzv. fail-open - při přetížení IPS je možné definovat, zda dojde k blokaci nebo propuštění provozu |  |
| Deklarovaná propustnost IPS inspekce min 5.2 Gbps |  |
| **Funkce antivirové kontroly** | **-** |
| Ochrana před škodlivým kódem (malware, trojské koně apod.), včetně ochrany před polymorfním kódem |  |
| Signatury automaticky aktualizované výrobcem |  |
| Požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky) |  |
| Možnost rozšíření o inspekci tzv. sandbox technikou formou lokálné HW appliance stejného výrobce |  |
| Deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 2.7 Gbps |  |
| Funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. |  |
| 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 |  |
| Funkce odstranění škodlivého aktivního obsahu z dokumentů kancelářských aplikací. |  |
| Funkce kategorizace a blokace webových stránek |  |
| Funkce DNS filtru |  |
| Funkce ochrany před únikem citlivých informací (DLP) |  |
| Funkce pokročilé prevence malware s využitím AI |  |
| Funkce pokročilého mapování útočné plochy s důrazem na IoT zařízení |  |
| Funkce/služba konverze konfiguračního souboru stávajícího firewallu na nový poptávaný firewall |  |
| Podpora SSL inspekce/SSL dekrypce s minimální propustností 2.9 Gbps |  |
| DoS Policy prevence proti základním útokům typu DoS |  |
| **Firewall** | |
| Možnost nastavovat firewall politiku na základě geografických údajů |  |
| Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem |  |
| Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru |  |
| Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu |  |
| Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření. |  |
| Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii |  |
| Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu |  |
| Podpora funkce reverzní proxy |  |
| Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů |  |
| Funkce explicitní proxy |  |
| Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp. |  |
| Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech) |  |
| Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů) |  |
| FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici |  |
| Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě |  |
| Podpora otevřeného API |  |

**Konkrétní typ a označení nabízeného řešení:**

1. **NABÍZENÉ ŘEŠENÍ:** [DODAVATEL JEDNOZNAČNĚ URČÍ, JAKÝ TYP NEBO VERZE VÝROBKU NEBO NABÍZENÉHO ŘEŠENÍ (HW i SW SOUČÁSTI UVEĎTE SAMOSTATNĚ) JE PŘEDMĚTEM JEHO NABÍDKY – minimálně uvede název výrobce, obchodní název výrobku, typ nebo verzi]

## Switche

|  |  |
| --- | --- |
| **Switche** |  |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| Záruka výrobce na výměnu vadného HW platná po celou dobu životnosti zařízení, minimálně 5 let od ukončení prodeje daného zařízení |  |
| Zařízení ve formátu HW appliance o velikosti 1RU |  |
| Podpora výrobce pro řešení technických problému platná po dobu 5 let s dostupností 24/7 |  |
| Pravidelné a automaticky instalované bezpečnostní a funkční aktualizace sítových prvku po celou dobu platnosti podpory výrobce |  |
| Veškerá konfigurace a monitoring všech síťových prvků, které jsou předmětem poptávky, musí probíhat jak centralizovaně, a to buďto pomocí samostatného centralizovaného switch kontroléru od stejného výrobce, nebo prostřednictvím cloudové webové aplikace nebo případně lokálně na daném zařízení přes příkazovou řádku/webové rozhraní daného přepínače |  |
| Centrální administrativní rozhraní je jednotné pro přepínače i firewall stejného výrobce |  |
| Automatická karanténa připojených zařízení po signálu z bezpečnostní brány |  |

**Konkrétní typ a označení nabízeného řešení:**

1. **NABÍZENÉ ŘEŠENÍ:** [DODAVATEL JEDNOZNAČNĚ URČÍ, JAKÝ TYP NEBO VERZE VÝROBKU NEBO NABÍZENÉHO ŘEŠENÍ (HW i SW SOUČÁSTI UVEĎTE SAMOSTATNĚ) JE PŘEDMĚTEM JEHO NABÍDKY – minimálně uvede název výrobce, obchodní název výrobku, typ nebo verzi]

### Agregační switch

|  |  |
| --- | --- |
| **Agregační switch** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| **HW parametry** | |
| Počet rozhraní 1GE/10GE/25GE SFP/SFP+/SFP28 – min 8x |  |
| Počet rozhraní 1GE/2.5GE/5GE RJ45 – min 16x |  |
| Počet rozhraní 32x 1GE/2.5GE – min 32x |  |
| Duální napájecí AC zdroje s možností výměny za chodu přepínače |  |
| 1x RJ45 Sériový port pro připojení konzole |  |
| 1x RJ45 Management port |  |
| **Výkonnostní parametry** | |
| Výkon switche alespoň 720Gbps |  |
| Minimální paketový výkon přepínače 1070 Mpps |  |
| **Ostatní** | |
| Podpora Jumbo Frame (9600 B ethernetový rámec) |  |
| DHCP Relay |  |
| DHCP snooping - detekce a blokování |  |
| Podpora QoS 802.1p |  |
| Podpora 802.1q VLAN tagging |  |
| Možnost duálního firmwaru |  |
| Podpora RSTP, MSTP včetně rozšíření BPDU guard, Root guard, Loop guard |  |
| Zrcadlení síťových rozhraní |  |
| Podpora 802.1x |  |
| Podpora ACL (IPv4 a IPv6) až 3000 záznamů, MAC whitelisting/blacklisting |  |
| Podpora SNMP v1/v2c/v3, sFlow, Syslogu a Radius protokolu |  |
| Podpora Multi-Chassis Link Aggregeation protokolu |  |
| Možnost aktivace podpory protokolů RIPv2, BGP, OSPFv2, IS-IS, VRRP pomocí přídavné licence |  |
| Podpora multicastového provozu |  |
| Dodávka 32 ks SFP+ modulů včetně optických patch cordů |  |

**Konkrétní typ a označení nabízeného řešení:**

1. **NABÍZENÉ ŘEŠENÍ:** [DODAVATEL JEDNOZNAČNĚ URČÍ, JAKÝ TYP NEBO VERZE VÝROBKU NEBO NABÍZENÉHO ŘEŠENÍ (HW i SW SOUČÁSTI UVEĎTE SAMOSTATNĚ) JE PŘEDMĚTEM JEHO NABÍDKY – minimálně uvede název výrobce, obchodní název výrobku, typ nebo verzi]

### Switche 24 Full PoE

|  |  |
| --- | --- |
| **ID3: Switche 24 Full PoE** | |
| **HW parametry** | |
| L2 přepínač |  |
| Výkon switche alespoň 240Gbps |  |
| Minimální paketový výkon přepínače 355 Mpps |  |
| 24x 2.5G/1G/100M/10M RJ-45 portů celkem z toho minimálně 16 portů podporující PoE/PoE+ (802.3af/at) a min. 4 porty s PoE++ (802.3bt) |  |
| 6x 10GE SFP+ porty |  |
| 1x RJ45 Sériový port pro připojení konzole |  |
| Požadujeme PoE switche s min. výkonem alespoň 780 W |  |
| Integrovaný napájený zdroj v těle přepínače |  |

**Konkrétní typ a označení nabízeného řešení:**

**NABÍZENÉ ŘEŠENÍ:** [DODAVATEL JEDNOZNAČNĚ URČÍ, JAKÝ TYP NEBO VERZE VÝROBKU NEBO NABÍZENÉHO ŘEŠENÍ (HW i SW SOUČÁSTI UVEĎTE SAMOSTATNĚ) JE PŘEDMĚTEM JEHO NABÍDKY – minimálně uvede název výrobce, obchodní název výrobku, typ nebo verzi]

### Switche 48 PoE

|  |  |
| --- | --- |
| **ID4: Switche 48 PoE** | |
| **HW parametry** | |
| L2 přepínač |  |
| Výkon switche alespoň 175Gbps |  |
| Minimální paketový výkon přepínače 255 Mpps |  |
| 48x GE RJ45 portů celkem z toho minimálně 24 portů podporující PoE/PoE+ (802.3af/at) |  |
| 4x 10GE SFP+ porty |  |
| 1x RJ45 Sériový port pro připojení konzole |  |
| Požadujeme PoE switche s min. výkonem alespoň 370 W |  |
| Integrovaný napájený zdroj v těle přepínače |  |

**Konkrétní typ a označení nabízeného řešení:**

**NABÍZENÉ ŘEŠENÍ:** [DODAVATEL JEDNOZNAČNĚ URČÍ, JAKÝ TYP NEBO VERZE VÝROBKU NEBO NABÍZENÉHO ŘEŠENÍ (HW i SW SOUČÁSTI UVEĎTE SAMOSTATNĚ) JE PŘEDMĚTEM JEHO NABÍDKY – minimálně uvede název výrobce, obchodní název výrobku, typ nebo verzi]

## Ověřovací autorita

|  |  |
| --- | --- |
| **Ověřovací autorita** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| Řešení stejného výrobce, jako NGFW a řešení mobilních tokenů pro zajištění oboustranné kompatibility |  |
| Virtuální appliance pro platformu VMWare, kterou používá zadavatel |  |
| Management identit, plnohodnotná AAA funkcionalita, integrované funkce AAA pro připojení z VPN |  |
| Podpora nabízených funkcí pro minimálně 300 uživatelů |  |
| Možnost automaticky synchronizovat uživatele z Active Directory |  |
| Možnost vytvářet lokální uživatele a skupiny |  |
| Podpora 2FA pomocí tokenů (aplikace pro iOS a Android, HW token) |  |
| Podpora 2FA pomocí SMS a emailu |  |
| Podpora ověřováni ze sociálních sítí (facebook, linkedin) |  |
| Možnost definovat zařízení na základě MAC adresy |  |
| Funkce LDAP/LDAPS serveru |  |
| Možnost automatického importu identit ze vzdálených LDAP serverů |  |
| Funkce TACACS+ serveru |  |
| Funkce Radius serveru |  |
| Podpora definice různých Radius politik (zejména pro využití v rámci 802.1x) |  |
| Podpora předdefinovaných Radius atributů, podpora definice vlastních Radius atributů |  |
| Podpora radius accountning v proxy režimu |  |
| Funkce SAML IdP |  |
| Možnost napojení a ověřování z externího Radius, LDAP SAML a OAuth server |  |
| Podpora SSO autentizace uživatelů v prostředí domény MS Windows |  |
| Podpora Kerberos |  |
| Podpora EAP metod EAP-MSCHAPv2, EAP-TLS, PEAP, EAP-GTC |  |
| Funkce certifikační autority |  |
| Podpora SCEP a CRL |  |
| Podpora captive portálu |  |
| Podpora samoobslužných portálů (reset hesla, editace uživatelských údajů, přidělení tokenů) |  |
| Podpora 2FA pro Outlook Web Access pomocí nativního klienta |  |
| Podpora mechanismu 2FA pro koncové stanice a přihlášení do systému Windows |  |
| Podpora push notifikací pro 2FA a mobilní aplikaci |  |
| Podpora REST API (pokud tato funkce vyžaduje licenci, tak musí být součástí dodávky) |  |
| Podpora výrobce pro řešení technických problému platná po 5 let s dostupností 24/7. |  |

**Konkrétní typ a označení nabízeného řešení:**

1. **NABÍZENÉ ŘEŠENÍ:** [DODAVATEL JEDNOZNAČNĚ URČÍ, JAKÝ TYP NEBO VERZE VÝROBKU NEBO NABÍZENÉHO ŘEŠENÍ (HW i SW SOUČÁSTI UVEĎTE SAMOSTATNĚ) JE PŘEDMĚTEM JEHO NABÍDKY – minimálně uvede název výrobce, obchodní název výrobku, typ nebo verzi]

## Mobilní tokeny pro 2FA

|  |  |
| --- | --- |
| **Mobilní tokeny pro 2FA** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| Virtuální token pro generování jednorázových hesel v rámci 2FA na principu OATH (RFC6238, RFC4226) |  |
| Řešení stejného výrobce, jako NGFW a centrálního autentizačního serveru |  |
| Plná podpora ověřovací autority |  |
| Minimální počet kusů v setu: 50 |  |
| Podporované mobilní platformy min. iOS, Android, windows phone 8, 8.1, windows 10, windows universal platform |  |
| Podpora push notifikací (tj. uživatel nemusí přepisovat jednorázové heslo, ale pouze v rámci push notifikace v aplikaci povolí přístup) |  |
| Podpora autentizace pomocí přepsání jednorázového hesla (6ti místný číselný kód) |  |
| Snadná aktivace tokenů (email, pomocí skenování QR kódu) |  |
| Možnost deaktivace tokenu ze strany administrátora bez přístupu ke koncovému zařízení, možnost převedení na jiného uživatele bez ztráty licence |  |
| Zabezpečení pomocí PIN/otisku prstu |  |
| Ochrana před útoky typu brute force (tj. automatické deaktivace při překročení max. počtu neúspěšných pokusů |  |

**Konkrétní typ a označení nabízeného řešení:**

1. **NABÍZENÉ ŘEŠENÍ:** [DODAVATEL JEDNOZNAČNĚ URČÍ, JAKÝ TYP NEBO VERZE VÝROBKU NEBO NABÍZENÉHO ŘEŠENÍ (HW i SW SOUČÁSTI UVEĎTE SAMOSTATNĚ) JE PŘEDMĚTEM JEHO NABÍDKY – minimálně uvede název výrobce, obchodní název výrobku, typ nebo verzi]

## VPN s centrální správou

|  |  |
| --- | --- |
| **VPN s centrální správou** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| Dodaný VPN klient SW je centrálně řízený, dohledovaný a spravovaný z jednoho místa – Endpoint Management Serveru |  |
| Celkový počet požadovaných endpointů je 50 |  |
| Celá dodávka musí obsahovat všechny komponenty systému včetně SW pro centrální management server a software na klienty a licence po dobu 5 let na všechny komponenty |  |
| 24x7 support na celé řešení od výrobce |  |
| Centralizovaná správa VPN/ZTNA klientů, včetně možnosti updatů samotného VPN softwaru klientů |  |
| Obousměrná a výrobcem podporovaná integrace s dalšími nabízenými bezpečnostními prvky, především NG Firewall, za účelem sdílení provozně telemetrických informací a informací o odhalených hrozbách |  |
| IPsec VPN s možností MFA dostupná minimálně pro Windows, MAC a Android klienty |  |
| Možnost centrálního logování událostí |  |
| Možnost autentifikace klientů pomocí RADIUSu, LDAPu, TACACS+, certifikátem nebo ověřením oproti lokální databázi na endpoint manageru |  |
| ZTNA agent – vzdálený přístup bez připojení k VPN. Možnost šifrovaného přístupu ke specifickým síťovým cílům na základě identifikace certifikátem koncové stanice bez nutnosti sestavovat VPN |  |

**Konkrétní typ a označení nabízeného řešení:**

1. **NABÍZENÉ ŘEŠENÍ:** [DODAVATEL JEDNOZNAČNĚ URČÍ, JAKÝ TYP NEBO VERZE VÝROBKU NEBO NABÍZENÉHO ŘEŠENÍ (HW i SW SOUČÁSTI UVEĎTE SAMOSTATNĚ) JE PŘEDMĚTEM JEHO NABÍDKY – minimálně uvede název výrobce, obchodní název výrobku, typ nebo verzi]

## Konfigurační práce

|  |  |  |
| --- | --- | --- |
| **Konfigurační práce** | | |
| **MINIMÁLNÍ POŽADAVKY** | | **ANO/NE** |
| Návrh a implementace segmentace sítě | Rozdělení sítě do VLAN dle určeného síťového profilu |  |
| Ověřování 802.1x | Navázání přístupů do sítě (LAN, WLAN) na autorizace/autentizace RADIUS, LDAP, AD, 2FAm autentizační server. |  |
| Instalace a konfigurace | Zprovoznění firewall clusteru, migrace konfigurací ze stávajícího HW, napojení na logování, site-tosite VPN s ostatními lokalitami |  |
| Instalace a konfigurace | Zprovoznění agregačních switchů, konfigurace, VLAN |  |
| Instalace a konfigurace | Zprovoznění pobočních PoE switchů, konfigurace VLAN, napojení 10G na agregační switche |  |
| Instalace a konfigurace | Zprovoznění 2FA tokenů pro VPN uživatele, instalace aplikace na koncových zařízeních |  |
| Instalace a konfigurace | Zprovoznění centrální správy VPN uživatelů |  |
| Instalace a konfigurace | Ověřování konfigurací, akceptační testy |  |
| Instalace a konfigurace | Proškolení lokálních administrátorů ke všem instalovaným oblastem |  |
| Instalace a konfigurace | Zpracování a předání dokumentace |  |

# PROHLÁŠENÍ DODAVATELE

**Dodavatel podáním nabídky potvrzuje, že předmět nabídky se plně shoduje s výše uvedenými požadavky.**

V [DOPLNÍ DODAVATEL] dne [DOPLNÍ DODAVATEL]

................................................

[DOPLNÍ DODAVATEL]