Příloha č. 1 Smlouvy

# Bližší specifikace předmětu plnění

### Název zakázky: **Bezpečnostní vybavení serverových** **farem**

### Dodávka HW

#### Dodávka čtyř zařízení Next Generation Firewall velký

V oblasti dodávky čtyř zařízení Next Generation Firewall včetně potřebných subskripcí nebo potřebných licencí a podpory výrobce na 36 měsíců v režimu E1 ve smyslu čl. 12.2. Přílohy č. 5 Zvláštní obchodní podmínky definuje zadavatel následující požadavky pro každé z nich:

|  |  |  |  |
| --- | --- | --- | --- |
| **Next-Generation firewall pro DC - velký** | Výrobce produktu: [Doplní Dodavatel] | | |
| Produktové číslo (typ) nabízené položky (v případě, že je položka popsána více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízené položky) | | [Doplní Dodavatel] | |
| Odkaz na www stránky výrobce položky, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | | [Doplní Dodavatel] | |
| Požadovaná funkcionalita/vlastnost | | | Nabízený produkt splňuje [ANO/NE] |
| Typ NG firewall | | | [Doplní Dodavatel] |
| Platforma postavená na HW akcelerované architektuře (tj. zařízení vybavené specializovanými obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází,…) | | | [Doplní Dodavatel] |
| Maximální velikost 5RU | | | [Doplní Dodavatel] |
| Příslušenství pro montáž do 19" rozvaděče součástí dodávky přepínače | | | [Doplní Dodavatel] |
| Minimální počet neblokovaných portů 1/10s volitelným fyzickým rozhraním typu SFP28 – 16 ks | | | [Doplní Dodavatel] |
| Minimální počet neblokovaných portů 40/100 GE s volitelným fyzickým rozhraním typu QSFP28 – 4 ks | | | [Doplní Dodavatel] |
| Dedikovaný 2x management port – RJ 45 | | | [Doplní Dodavatel] |
| Dedikovaná konzolový port – typ RJ45 nebo miniUSB | | | [Doplní Dodavatel] |
| Lokální úložiště pro logy atp. (SSD/NVMe disk) o minimální kapacitě 960GB v režimu RAID1 | | | [Doplní Dodavatel] |
| Podpora nasazení v HA Clusteru (porty nutné pro zapojení do HA nesmí ovlivnit počet požadovaných portů výše) | | | [Doplní Dodavatel] |
| Interní redundantní napájecí zdroj – vyměnitelné za chodu | | | [Doplní Dodavatel] |
| Interní redundantní ventilátory | | | [Doplní Dodavatel] |
| Stavové filtrování IPv4, IPv6 UDP paket 64 byte min. 130 Gbps | | | [Doplní Dodavatel] |
| Stavové filtrování IPv4, IPv6 UDP paket 512 byte min. 190 Gbps | | | [Doplní Dodavatel] |
| Stavové filtrování IPv4, IPv6 UDP paket 1518 byte min. 190 Gbps | | | [Doplní Dodavatel] |
| Počet souběžných TCP spojení min. 22 000 000 | | | [Doplní Dodavatel] |
| Počet nových spojení za sekundu min. 1 000 000 | | | [Doplní Dodavatel] |
| Propustnost funkce ochrany proti škodlivému kódu min. 24.5 Gbps | | | [Doplní Dodavatel] |
| Propustnost funkce aplikační analýzy na L7 (měřeno pro http 64 kB provoz) min. 64 Gbps | | | [Doplní Dodavatel] |
| Propustnost NGFW (IPS, Application control) min. 18 Gbps | | | [Doplní Dodavatel] |
| Propustnost IPSEC VPN (AES256, SHA256) min. 50 Gbps | | | [Doplní Dodavatel] |
| Propustnost SSL VPN min 10 Gbps | | | [Doplní Dodavatel] |
| SSL inspekce (IPS, HTTPS) min. 20 Gbps | | | [Doplní Dodavatel] |
| SSL inspekce souběžných spojení min. 2 500 000 | | | [Doplní Dodavatel] |
| Počet IPSec VPN tunelů Gateway-to-Gateway min. 18 000 | | | [Doplní Dodavatel] |
| Počet IPSec VPN tunelů Client-to-Gateway min. 60 000 | | | [Doplní Dodavatel] |
| Počet uživatelů současně připojených pomocí SSL VPN klienta – 2000, součástí musí být licence na minimálně 500 uživatelů, podpora připojení z MACOS, Windows a běžných LINUX distribucí | | | [Doplní Dodavatel] |
| Podpora virtuálních kontextů hadrware appliance min. 10 kontextů – pokud jsou licencovány, musí být licence součástí nabídky | | | [Doplní Dodavatel] |
| Součástí dodávky musí být i veškeré potřebné licence pro služby NGFW do všech kontextů | | | [Doplní Dodavatel] |
| Každý z virtuálních kontextů může pracovat buď v L2 režimu (transparentní režim inspekce) nebo L3 režimu (NAT/router režim s inspekcí) | | | [Doplní Dodavatel] |
| Virtuální kontexty musí být možné propojit pomocí virtuálních propojů (bez nutnosti propojovat pomocí fyzických síťových rozhraní) bez omezení výkonu | | | [Doplní Dodavatel] |
| Podpora Active Active i Active Passive HA, full mesh HA, synchronizace stavové tabulky mezi nódy clusteru | | | [Doplní Dodavatel] |
| Režim vysoké dostupnosti (L2 HA, tj. virtuální MAC adresy) | | | [Doplní Dodavatel] |
| Správa všech zařízení pracujících v režimu vysoké dostupnosti musí probíhat jednotně přes společné grafické konfigurační rozhraní | | | [Doplní Dodavatel] |
| Grafické konfigurační rozhraní pro správu celého clusteru, dostupné pomocí webového prohlížeče (HTTPS) bez omezení na počet administrátorů a bez nutnosti instalovat dodatečnou management platformu nebo aplikaci. | | | [Doplní Dodavatel] |
| Podpora LACP (802.3ad) | | | [Doplní Dodavatel] |
| Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, licence, a to časově i místně neomezená, musí být součástí dodávky a to jak pro IPv4 tak i IPv6 | | | [Doplní Dodavatel] |
| VXLAN s BGP EVPN – podpora v HW (pokud je nutná licence, musí být součástí) | | | [Doplní Dodavatel] |
| Funkce BFD (Bidirectional Forwarding Detection) pro routovací protokoly BGP a OSPF s možností upravit Min TX Interval, Min RX Interval, Discriminator pro jednotlivé rozhraní zařízení, a to i virtuální (VLAN interface) | | | [Doplní Dodavatel] |
| Podpora SSL offload | | | [Doplní Dodavatel] |
| Podpora TLS 1.3 i pro aplikační inspekce | | | [Doplní Dodavatel] |
| Podpora L2 (transparentní) režimu i L3 (NAT/Router) režimu | | | [Doplní Dodavatel] |
| Podpora IPv6 pro všechny funkce (tj L3 protokoly a všechny NGFW funkce) | | | [Doplní Dodavatel] |
| Podpora NAT64/NAT46 | | | [Doplní Dodavatel] |
| Podpora multicastu včetně routování a firewall funkcí (tvorba multicast FW politiky) | | | [Doplní Dodavatel] |
| Možnost nastavovat firewall politiku na základě geografických údajů – GeoIP | | | [Doplní Dodavatel] |
| Podpora firewall pravidel na základě identity uživatele pro MS AD prostředí – nastavení bezpečnosti uživateli na základě členství v AD skupině na doménovém kontroléru | | | [Doplní Dodavatel] |
| Podpora detekce klientského zařízení s možností nastavovat firewall politiku na základě typu klientského zařízení (telefon, tablet, PC) včetně operačního systému (Android, iPhone, …) bez nutnosti instalovat klienty na koncové stanice | | | [Doplní Dodavatel] |
| Podpora VPN SSL - portálový režim i tunelovací režim | | | [Doplní Dodavatel] |
| IPSEC gateway to gateway, hub and spoke, dial up konfigurace, podpora více tunelů (redundantní VPN) | | | [Doplní Dodavatel] |
| Podpora Site-to-site IPSec VPN s podporou statického i dynamického routování | | | [Doplní Dodavatel] |
| Ověřování uživatelů proti LDAP, Active Directory, Single Sign On, Radius, TACACS+ | | | [Doplní Dodavatel] |
| Podpora dynamických profilů (možnost přiřadit konkrétní profil uživateli na základě ověření) | | | [Doplní Dodavatel] |
| Traffic Shaping (QoS, prioritizace atd.) | | | [Doplní Dodavatel] |
| Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu | | | [Doplní Dodavatel] |

#### Dodávka osmi zařízení Next Generation Firewall malý

V oblasti dodávky osmi zařízení Next Generation Firewall včetně potřebných subskripcí nebo potřebných licencí a podpory výrobce na 36 měsíců v režimu E1 ve smyslu čl. 12.2. Přílohy č. 5 Zvláštní obchodní podmínky definuje zadavatel následující požadavky pro každé z nich:

|  |  |  |  |
| --- | --- | --- | --- |
| **Next-Generation firewall pro DC - malý** | Výrobce produktu: | | [Doplní Dodavatel] |
| Produktové číslo (typ) nabízené položky (v případě, že je položka popsána více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízené položky) | | [Doplní Dodavatel] | |
| Odkaz na www stránky výrobce položky, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | | [Doplní Dodavatel] | |
| Požadovaná funkcionalita/vlastnost | | | Nabízený produkt splňuje [ANO/NE] |
| Typ NG firewall | | | [Doplní Dodavatel] |
| Platforma postavená na HW akcelerované architektuře (tj. zařízení vybavené specializovanými obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází,…) | | | [Doplní Dodavatel] |
| Maximální velikost 2RU | | | [Doplní Dodavatel] |
| Příslušenství pro montáž do 19" rozvaděče součástí dodávky přepínače | | | [Doplní Dodavatel] |
| Minimální počet neblokovaných portů 10/25GE s volitelným fyzickým rozhraním typu SFP28 – 4 ks | | | [Doplní Dodavatel] |
| Minimální počet neblokovaných portů 1 GE s volitelným fyzickým rozhraním typu SFP – 8 ks | | | [Doplní Dodavatel] |
| Minimální počet neblokovaných portů 1 GE typu RJ45 –8 ks | | | [Doplní Dodavatel] |
| Dedikovaný 1x management port/HA – RJ 45 | | | [Doplní Dodavatel] |
| Dedikovaná konzolový port – typ RJ45 nebo miniUSB | | | [Doplní Dodavatel] |
| Lokální úložiště pro logy atp. (SSD/NVMe disk) o minimální kapacitě 220GB v režimu RAID1 | | | [Doplní Dodavatel] |
| Podpora nasazení v HA Clusteru (porty nutné pro zapojení do HA nesmí ovlivnit počet požadovaných portů výše) | | | [Doplní Dodavatel] |
| Interní redundantní napájecí zdroj – vyměnitelné za chodu | | | [Doplní Dodavatel] |
| Interní redundantní ventilátory | | | [Doplní Dodavatel] |
| Stavové filtrování IPv4, IPv6 UDP paket 64 byte min. 65 Gbps | | | [Doplní Dodavatel] |
| Stavové filtrování IPv4, IPv6 UDP paket 512 byte min. 90 Gbps | | | [Doplní Dodavatel] |
| Stavové filtrování IPv4, IPv6 UDP paket 1518 byte min. 90 Gbps | | | [Doplní Dodavatel] |
| Počet souběžných TCP spojení min. 8 000 000 | | | [Doplní Dodavatel] |
| Počet nových spojení za sekundu min. 445 000 | | | [Doplní Dodavatel] |
| Propustnost funkce ochrany proti škodlivému kódu min. 10 Gbps | | | [Doplní Dodavatel] |
| Propustnost funkce aplikační analýzy na L7 (měřeno pro http 64 kB provoz) min. 32 Gbps | | | [Doplní Dodavatel] |
| Propustnost NGFW (IPS, Application control) min. 11 Gbps | | | [Doplní Dodavatel] |
| Propustnost IPSEC VPN min. 50 Gbps | | | [Doplní Dodavatel] |
| Propustnost SSL VPN min 4 Gbps | | | [Doplní Dodavatel] |
| SSL inspekce (IPS, HTTPS) min. 8,5 Gbps | | | [Doplní Dodavatel] |
| SSL inspekce souběžných spojení min. 800 000 | | | [Doplní Dodavatel] |
| Počet IPSec VPN tunelů Gateway-to-Gateway min. 2 000 | | | [Doplní Dodavatel] |
| Počet IPSec VPN tunelů Client-to-Gateway min. 49 000 | | | [Doplní Dodavatel] |
| Počet uživatelů současně připojených pomocí SSL VPN klienta – 2000, součástí musí být licence na minimálně 500 uživatelů, podpora připojení z MACOS, Windows a běžných LINUX distribucí | | | [Doplní Dodavatel] |
| Podpora virtuálních kontextů hadrware appliance min. 10 kontextů – pokud jsou licencovány, musí být licence součástí nabídky | | | [Doplní Dodavatel] |
| Součástí dodávky musí být i veškeré potřebné licence pro služby NGFW do všech kontextů | | | [Doplní Dodavatel] |
| Každý z virtuálních kontextů může pracovat buď v L2 režimu (transparentní režim inspekce) nebo L3 režimu (NAT/router režim s inspekcí) | | | [Doplní Dodavatel] |
| Virtuální kontexty musí být možné propojit pomocí virtuálních propojů (bez nutnosti propojovat pomocí fyzických síťových rozhraní) bez omezení výkonu | | | [Doplní Dodavatel] |
| Podpora Active Active i Active Passive HA, full mesh HA, synchronizace stavové tabulky mezi nódy clusteru | | | [Doplní Dodavatel] |
| Režim vysoké dostupnosti (L2 HA, tj. virtuální MAC adresy) | | | [Doplní Dodavatel] |
| Správa všech zařízení pracujících v režimu vysoké dostupnosti musí probíhat jednotně přes společné grafické konfigurační rozhraní | | | [Doplní Dodavatel] |
| Grafické konfigurační rozhraní pro správu celého clusteru, dostupné pomocí webového prohlížeče (HTTPS) bez omezení na počet administrátorů a bez nutnosti instalovat dodatečnou management platformu nebo aplikaci. | | | [Doplní Dodavatel] |
| Podpora LACP (802.3ad) | | | [Doplní Dodavatel] |
| Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, licence, a to časově i místně neomezená, musí být součástí dodávky a to jak pro IPv4 tak i IPv6 | | | [Doplní Dodavatel] |
| VXLAN s BGP EVPN – podpora v HW (pokud je nutná licence, musí být součástí) | | | [Doplní Dodavatel] |
| Funkce BFD (Bidirectional Forwarding Detection) pro routovací protokoly BGP a OSPF s možností upravit Min TX Interval, Min RX Interval, Discriminator pro jednotlivé rozhraní zařízení, a to i virtuální (VLAN interface) | | | [Doplní Dodavatel] |
| Podpora SSL offload | | | [Doplní Dodavatel] |
| Podpora TLS 1.3 i pro aplikační inspekce | | | [Doplní Dodavatel] |
| Podpora L2 (transparentní) režimu i L3 (NAT/Router) režimu | | | [Doplní Dodavatel] |
| Podpora IPv6 pro všechny funkce (tj L3 protokoly a všechny NGFW funkce) | | | [Doplní Dodavatel] |
| Podpora NAT64/NAT46 | | | [Doplní Dodavatel] |
| Podpora multicastu včetně routování a firewall funkcí (tvorba multicast FW politiky) | | | [Doplní Dodavatel] |
| Možnost nastavovat firewall politiku na základě geografických údajů – GeoIP | | | [Doplní Dodavatel] |
| Podpora firewall pravidel na základě identity uživatele pro MS AD prostředí – nastavení bezpečnosti uživateli na základě členství v AD skupině na doménovém kontroléru | | | [Doplní Dodavatel] |
| Podpora detekce klientského zařízení s možností nastavovat firewall politiku na základě typu klientského zařízení (telefon, tablet, PC) včetně operačního systému (Android, iPhone, …) bez nutnosti instalovat klienty na koncové stanice | | | [Doplní Dodavatel] |
| Podpora VPN SSL - portálový režim i tunelovací režim | | | [Doplní Dodavatel] |
| IPSEC gateway to gateway, hub and spoke, dial up konfigurace, podpora více tunelů (redundantní VPN) | | | [Doplní Dodavatel] |
| Podpora Site-to-site IPSec VPN s podporou statického i dynamického routování | | | [Doplní Dodavatel] |
| Ověřování uživatelů proti LDAP, Active Directory, Single Sign On, Radius, TACACS+ | | | [Doplní Dodavatel] |
| Podpora dynamických profilů (možnost přiřadit konkrétní profil uživateli na základě ověření) | | | [Doplní Dodavatel] |
| Traffic Shaping (QoS, prioritizace atd.) | | | [Doplní Dodavatel] |
| Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu | | | [Doplní Dodavatel] |

### Implementace Next Generation Firewallu na segmentaci sítě

V oblasti implementace Next Generation Firewallu na segmentaci sítě jsou definovány následující činnosti, resp. požadavky:

|  |  |
| --- | --- |
| **Oblast** | Činnost |
| Dodávka zařízení | Zadavatel požaduje dodávku všech zařízení do lokalit v rámci ČR včetně instalace do připraveného prostoru. |
| Základní konfigurace | * Ověření zařízení na absenci HW vad * Registrace zařízení * Instalace výrobcem doporučené verze operačního systému   + Konfigurace základních parametrů (management rozhraní, hostname, DNS, NTP, administrátorské přístupy, napojení na centrální uživatelský systém (LDAP/RADIUS), odesílání událostí do externího zařízení). |
| Konfigurace clusteru | Nasazení dvou klastrů v režimu Active-Pasive. |
| Síťová konfigurace | * Linková agregace * IP adresace a VLAN tagy * Směrování včetně dynamického směrování * DHCP relay. |
| Přenos objektů a bezpečnostní politiky | * Migrace pravidel max 5 000 pravidel na jeden cluster * Migrace 1000 objektů (IP adresy, FQDN, skupiny apod.) * Hygiena pravidel (například překrývající se pravidla). |
| SSO Autentizace | Napojení na Active Directory řízení přístupů na základě identit. |

### Technická podpora výrobce

|  |  |
| --- | --- |
| **Oblast** | **Požadavky** |
| Oficiální podpora výrobce | Dodavatel zajistí oficiální podporu výrobce po dobu 36 měsíců v období dle harmonogramu   * Režim podpory dle servisního modelu E1 * Podpora musí být dostupná minimálně na webovém portálu výrobce, e-mailu a telefonu |