

### Technická specifikace

Součástí plnění bude dodávka níže specifikovaného HW a licencí, vč. souvisejících servisních činností ve stanoveném rozsahu člověkodní.

#### 1.1. Technická specifikace a předpokládané množství

Produkt	Předpokládaný počet ks
SONICWALL TZ80 SECURE CONNECT 1YR	18
SECURE CONNECT SERVICE SUITE FOR TZ80 2YR	24
SECURE CONNECT SERVICE SUITE FOR TZ80 3YR	13
ADVANCED PROTECTION SECURITY SUITE FOR TZ80 2YR	12
ADVANCED PROTECTION SECURITY SUITE FOR TZ80 3YR	7
SONICWALL TZ480	108
SONICWALL TZ480 RACKMOUNT KIT + 2nd POWER SUPPLY	108
24X7 SUPPORT FOR TZ480 2YR	16
24X7 SUPPORT FOR TZ480 3R	1
24X7 SUPPORT FOR TZ480 5YR	16
ADVANCED PROTECTION SECURITY SUITE FOR TZ480 2YR	92
ADVANCED PROTECTION SECURITY SUITE FOR TZ480 3YR	1
ADVANCED PROTECTION SECURITY SUITE FOR TZ480 5YR	92
SONICWALL NSA2800	36
ADVANCED PROTECTION SECURITY SUITE FOR NSA2800 2YR	36
ADVANCED PROTECTION SECURITY SUITE FOR NSA2800 3YR	1
ADVANCED PROTECTION SECURITY SUITE FOR NSA2800 5YR	36
SONICWALL NSA3800	3
ADVANCED PROTECTION SECURITY SUITE FOR NSA3800 2YR	3
ADVANCED PROTECTION SECURITY SUITE FOR NSA3800 3YR	1
ADVANCED PROTECTION SECURITY SUITE FOR NSA3800 5YR	3
SONICWALL FIREWALL SSL VPN 5 USER LICENSE	20
SONICWALL FIREWALL SSL VPN 10 USER LICENSE	60
SONICWALL CLOUD SECURE EDGE SECURE PRIVATE ACCESS BASIC PER USER 3 YR	10
ČLOVĚKODEN (MD)	250

## **1.2. Člověkodeni (MD) – definice**

- 1.2.1. Jeden člověkodeni je definován jako odborná práce vykonaná jedním kvalifikovaným specialistou v rozsahu 8 hodin čistého pracovního času. Tyto práce se budou vykonávat zpravidla v sídle jednotlivých organizací (jejich výčet je přiložen) a cena za člověkodeni tak musí zahrnovat i dopravné do místa realizace a zpět.
- 1.2.2. Odborné služby musí být realizovány osobou s prokazatelnou odborností v oblasti kybernetické a síťové bezpečnosti. Minimální požadavky na odborníka zahrnují:
- Minimálně 3 roky praxe v oblasti informační nebo síťové bezpečnosti.
  - Zkušenosti s návrhem, implementací a správou bezpečnostních opatření v IT prostředí.
  - Znalost technologií jako jsou firewally, IDS/IPS, SIEM systémy, VPN, segmentace sítí, šifrování, autentizační mechanismy.
- 1.2.3. V rámci každého člověkodeny musí být realizovány činnosti, které odpovídají odborné úrovni požadované oblasti. Příklady činností zahrnují (nikoli výlučně):
- Analýza a revize stávajících bezpečnostních politik a technických opatření.
  - Návrh a implementace bezpečnostních prvků v síťové infrastruktuře dané organizace.
  - Plná odborná znalost konfigurace dodaných firewallů/zařízení a její provedení včetně schopnosti zajištění převodu stávajících pravidel, politik a nastavení, pokud daná organizace taková již má.
  - Vyšetřování bezpečnostních incidentů a návrh nápravných opatření.
  - Poskytování konzultací nebo školení pro zaměstnance organizace.
  - Tvorba technické a provozní dokumentace topologie.
- 1.2.4. Každý člověkodeni musí být doložen výstupem, který bude předložen zadavateli ke schválení. Výstupem se rozumí například:
- Technická zpráva o provedené činnosti.
  - Záznam o konzultaci nebo školení.
  - Návrh dokumentace nebo konfigurace.
  - Záznam o provedeném testování nebo analýze.
- 1.2.5. Zadavatel si vyhrazuje právo schválit nebo odmítnout výstup, pokud nebude odpovídat požadované odborné úrovni nebo rozsahu činnosti. V takovém případě nebude člověkodeni považován za řádně splněný.

## **1.3. Typické související činnosti v odhadované pracnosti**

Představa typických činností v odhadované pracnosti 2MD v případě implementace jednoho firewallu Sonicwall TZ480, případně 3MD v případě implementace Sonicwall NSA2800:

- 1.3.1. Aktualizace firmware firewallu na poslední stabilní verzi OS.
- 1.3.2. Implementace firewallu v místě organizace včetně kompletního převodu konfigurace ze stávajícího firewallu.
- 1.3.3. Zmapování aktuálního stavu síťové infrastruktury (zařízení, servery, aplikace, komunikační toky – např. i mezi jednotlivými lokalitami – více FW).
- 1.3.4. Revize současného stavu a realizace případných úprav segmentace sítě dle dostupných možností (např. DMZ, interní sítě, tiskárny, servery, aplikace, management, wifi, prvky třetích stran, guest síť apod.).
- 1.3.5. Nastavení routování mezi sítěmi na firewallu s respektováním jejich typu a nutnosti prostupu.
- 1.3.6. Revize všech pravidel firewallu dle současného stavu organizace, návrh a realizace úprav za účelem omezení kybernetických hrozeb.
- 1.3.7. Revize a úpravy DHCP serveru a podsítí v případě potřeby.
- 1.3.8. Revize, nastavení a úpravy bezpečnostních služeb firewallu (GeoIP, Antivir, IPS, SPI, SPI DPI, Web ContentFilter, Application Control) podle potřeb organizace.
- 1.3.9. Vytvoření bezpečnostního tunelu a připojení firewallu do dohledového centra.
- 1.3.10. Nakonfigurování log reportingu firewallu do dohledového centra.

- 1.3.11. Po dohodě s organizací zajištění možnosti napojení aktivních prvků organizace (např. UPS, servery, switche apod.) do monitoringu dohledového centra.
- 1.3.12. Nastavení a konfigurace klientské VPN, pokud je daná organizace využívá, případné navázání ověření vůči Active Directory.
- 1.3.13. V případě dostupnosti redundantní konektivity, její konfigurace (Load Balancing).
- 1.3.14. Po domluvě se organizací konfigurace QOS bandwidth.
- 1.3.15. Doprava tam i zpět do místa instalace organizace.
- 1.3.16. Revize stávajícího připojení WAN. V případě využití optického připojení ukončit toto připojení v případě možnosti přímo v konektoru na firewallu.
- 1.3.17. V případě organizací s více lokalitami zajištění jejich propojení šifrovaným spojením.
- 1.3.18. V případě potřeby konfigurace připojení do krajské sítě CamelNET zajištění komunikace a součinnosti s techniky CamelNETu.
- 1.3.19. V případě velkých nedostatků v kyberbezpečnosti u organizace, které v rámci implementace nepůjdou realizovat, soupis doporučení a jejich předání organizaci k samostatnému dořešení.
- 1.3.20. Příprava digitální dokumentace (příprava síťové mapy s popisem segmentace).

#### 1.4. **Technická specifikace zálohovacího systému**

##### 1.4.1. **NAS zařízení**

2ks NAS zařízení osazené disky podle níže uvedených parametrů. Každý NAS musí být od jiného výrobce a s jiným operačním systémem z důvodu kyberbezpečnosti záloh.

	<i>První NAS</i>	<i>Druhý NAS</i>
<b>Formát</b>	max 3U rackmount včetně lyžin do 19" racku	max 3U rackmount včetně lyžin do 19" racku
<b>Procesor (CPU)</b>	Minimálně 4ks CORE s frekvencí min 2.2 GHz	Minimálně 4ks CORE s frekvencí min 3.30 GHz
<b>RAM</b>	Minimálně 16 GB DDR4 (max. 64 GB)	Minimálně 24 GB DDR4 ECC
<b>Diskové pozice</b>	Minimálně 12× 3.5" SATA (hot-swap)	Minimálně 12× 3.5" SATA (hot-swap)
<b>Možné rozšíření</b>	Minimálně 16 pozic	Minimálně 20 pozic
<b>Síťové porty</b>	Minimálně 2× 1GbE RJ-45, 2x SPF+ 10Gbit	Minimálně 2× 1GbE RJ-45, 2x SPF+ 10Gbit
<b>Redundantní napájení</b>	Musí obsahovat 2 nezávislé zdroje	Musí obsahovat 2 nezávislé zdroje
<b>RAID podpora</b>	RAID 0/1/5/6/10, JBOD, hot spare	RAID 0/1/5/6/10, JBOD, hot spare
<b>Virtualizace</b>	Možnost virtualizace včetně Docker kontejnerů	Možnost virtualizace včetně Docker kontejnerů
<b>Zálohování</b>	Vlasní software pro zálohování odlišný od druhého NAS. Možnost snapshotů	Vlasní software pro zálohování odlišný od druhého NAS. Možnost snapshotů
<b>Správa uživatelů</b>	LDAP, AD, granularní oprávnění	LDAP, AD, granularní oprávnění
<b>Bezpečnostní funkce</b>	AES-NI, firewall, VPN, 2FA,	AES-NI, firewall, VPN, 2FA
<b>Síťové funkce</b>	VLAN, QoS, Link Aggregation	VLAN, QoS, Link Aggregation
<b>Monitoring &amp; logování</b>	Resource Monitor, SNMP	Resource Monitor, SNMP
<b>Záruka na NAS</b>	Minimálně 3 roky	Minimálně 3 roky

### **Osazení disky**

Minimálně 13 ks, každý s kapacitou minimálně 22TB.  
Disky musí být určeny pro provoz 24/7.  
Disky musí být pro model NAS podporovány výrobcem.  
Minimální záruční doba disku 5 let.

Minimálně 13 ks, každý s kapacitou minimálně 20TB.  
Disky musí být určeny pro provoz 24/7.  
Disky musí být pro model NAS podporovány výrobcem.  
Minimální záruční doba disku 5 let.

#### **1.4.2. Síťový switch (4ks L3 non-POE switch)**

- Hardware, velikost max. 1U
  - L3 Switch (statické i dynamické směrování)
  - Fyzické porty min.
    - 48x RJ-45 1Gbps
    - 4x SFP+ 10Gbps
    - 1x RJ-45 sériová konzole
    - 1x USB port pro připojení ext. úložiště pro přenos firmware a konfigurace
  - Neblokující architektura přepínacího subsystému (wire speed)
  - Základní bezpečnostní prvky proti zneužití přístupu k síti (např. MAC based omezení port-security, např. vyhrazení portu pro určitou MAC, omezení počtu dynamických MAC)
  - Podpora IPv6 (Dual stack, ICMPv6, ND, stateless auto-config)
  - Podpora 802.3x (Flow control), 802.1Q (VLAN), 802.3ad (LACP), 802.1X (autentizace, s podporou guest VLAN), 802.3az (EEE), 802.1ab (LLDP, s podporou MED)
  - Podpora STP (spanning-tree) 802.1d, 802.1w, 802.1s
  - QoS na základě DSCP a 802.1p
  - Loop guard nezávislý na STP i STP loop guard
  - Podpora min. 12000 MAC adres
  - Switching capacity: >170 Gb/s, forwarding rate: 125 Mpps
  - Konfigurace prostřednictvím Web GUI (TLS 1.3), SSH v2 a sériové konzole
- Možnost konfigurace profilů portů dle připojení koncového zařízení, které na základě předem stanovené konfigurace nastaví na vybraném portu požadované VLAN a příp. další parametry jako např. max. počet dynamických MAC adres na daném portu, konfigurace STP edge, aby nebylo nutné tyto parametry nastavovat pro každý port zvlášť