Předmětem plnění části 4 veřejné zakázky je řešení následujících potřeb zadavatele:

1. Konsolidace sítě – rozšíření počítačové sítě do další budovy a zvýšení spolehlivosti sítě
2. Konsolidace sítě – zajištění vysokorychlostní a spolehlivé WiFi sítě pro vnitřní provoz úřadu i pro občany – návštěvníky úřadu
3. Zabezpečení – Zvýšení bezpečnosti perimetru sítě
4. Zálohování dat – NAS úložiště

*Pokyn pro dodavatele:*

*Dodavatel vyplní v níže uvedených tabulkách specifikací jednotlivých prvků / požadovaných řešení všechna prázdná pole.*

*Ve sloupci "Popis řešení, názvy a popis produktů" dodavatel uvede konkrétní popis, hodnoty a způsob splnění daného požadavku / podmínky tak, jak je jím nabízené řešení splňuje (zejm. schéma zapojení, popis pracovního postupu, atd), názvy nabízených zařízení, SW a dalších produktů a jejich popis.*

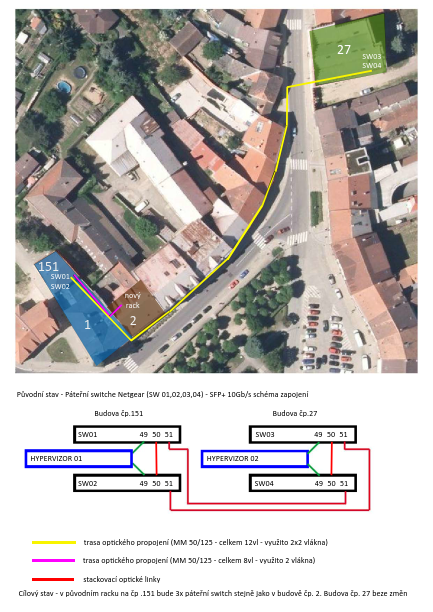
## **Konsolidace sítě – rozšíření počítačové sítě do další budovy a zvýšení spolehlivosti sítě**

Stávající řešení počítačové sítě využívá jako centrální prvky přepínače, které již nelze z pohledu stohovatelnosti rozšiřovat o nově pořízené a které jsou již mimo záruku a s omezenými možnostmi servisu. Dále současné řešení nevyhovuje z pohledu napájení plánovaných bezdrátových bodů, protože nejsou k dispozici PoE přepínače. Páteřní přepínače v současném řešení slouží i pro připojování klientů a vzhledem k potřebám počtu portů a podpory PoE budou takto sloužit i nadále.

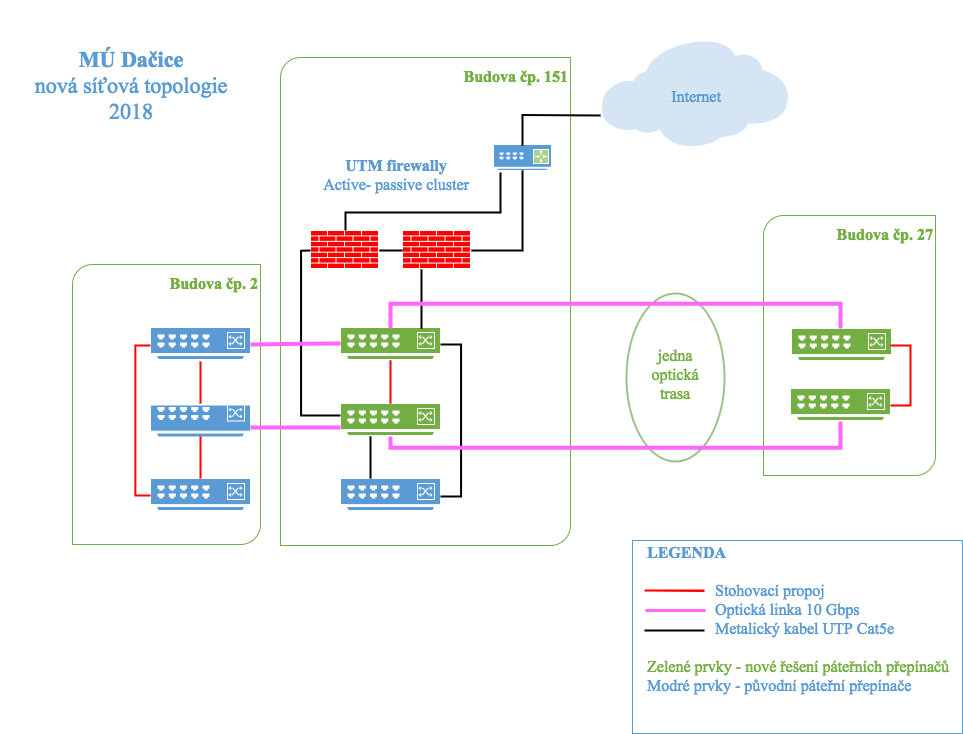
Dodávkou 4 ks nových páteřních přepínačů dojde ke zvýšení dostupnosti sítě a vzhledem k využití stávajících přepínačů Netgear dojde jak k rozšíření počtu portů, tak k posílení kapacity mezi novými páteřními a stávajícími Netgear switchi, které budou v roli přístupových switchů.

Nové páteřní přepínače pak zajistí i servisní pokrytí nejdůležitější části počítačové sítě, a tedy zvýšení spolehlivosti a dostupnosti sítě.

## **Schéma topologie sítě zanesené do mapy s vyznačením stávajícího řešení**



## **Návrh nové topologie páteřní sítě – schéma zapojení**



## **Požadované řešení – páteřní přepínače**

**2 ks páteřních přepínačů bez PoE**

|  |  |  |  |
| --- | --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje ANO/NE** | **Popis řešení, názvy a popis produktů** |
| **Třída zařízení** | L3 switch |  |  |
| **Formát zařízení a velikost** | do racku 19“, 1U |  |
| **Metalické porty** | 48×10/100/1000 RJ45 |  |
| **SFP porty** | 4x 10Gbit SFP+ |  |
| **Interní hot-swap AC napájecí zdroje** | ano, 2x stejný model |  |
| **Celková propustnost přepínače** | Minimálně 320 Gb/s |  |
| **Celkový paketový výkon přepínače** | Minimálně 190 mpps |  |
| **Paměťový buffer** | Minimálně 12MB |  |
| **Podpora VLAN podle IEEE 802.1Q** | Nejméně 1000 aktivních VLAN |  |
| **Vlastnosti stohování** | Stohování např. modulem |  |
| Stoh podporuje distribuované přepínání paketů |  |
| Minimální počet přepínačů ve stohu 8 |  |
| Minimální kapacita stohovacího propojení 40 Gb/s |  |
| Součástí dodávky 1m stohovací kabel |  |
| Stoh podporuje linkovou agregaci přes členy (MLAG) |  |
| **Základní funkce a protokoly** | Podpora "jumbo rámců" včetně velikosti 9000 Byte |  |
| Podpora Energy Efficient Ethernet (802.3az) |  |
| Podpora linkové agregace IEEE 802.1AX |  |
| Podpora rozkládání zátěže na LACP dle L2, L3 a L4 parametrů |  |
| Počet záznamů v tabulce MAC adres nejméně 32 000 |  |
| Protokol pro definici šířených VLAN - MVRP |  |
| Podpora MAC based VLAN |  |
| Podpora Private VLAN |  |
| IEEE 802.1s - Multiple Spanning Tree |  |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) |  |
| Detekce protilehlého zařízení pomocí LLDP (včetně rozšíření LLDP-MED) |  |
| Detekce jednosměrnosti optické linky (např. UDLD) |  |
| Tunelování 802.1Q v 802.1Q |  |
| DHCP server |  |
| DHCP relay pro IPv4 a IPv6 včetně option 82 a 79 |  |
| NTP pro IPv4 a IPv6 včetně MD5 autentizace |  |
| Statické směrování IPv4 a IPv6 |  |
| Podpora zapouzdření provozu: 6in4 |  |
| Dynamické směrování RIPv2 a RIPng a OSPF a OSPFv3 včetně podpory BFD |  |
| Policy based routing na základě ACL |  |
| Podpora VRRP podle RFC 3768 včetně podpory BFD |  |
| IGMP v2 a v3 |  |
| MLD v1 a v2 |  |
| Směrování multicast: PIM-DM a PIM-SM |  |
| **Bezpečnost** | Hardware podpora IPv4 a IPv6 ACL |  |
| ACL definice na základě skupiny fyzických portů |  |
| ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN |  |
| BPDU guard |  |
| Root guard |  |
| DHCP snooping pro IPv4 a IPv6 |  |
| HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na % rychlosti portu a množství paketů za vteřinu |  |
| ICMP rate-limiting |  |
| Podpora ověřování 802.1X nejméně 32 uživatelů na port |  |
| RADIUS MAC autentizace, probíhající před 802.1x pro případy, že koncové zařízení není softwarově vybaveno pro 802.1x autentizaci |  |
| Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675 |  |
| Podpora 802.1X Guest VLAN |  |
| Podpora IPv6 RA Guard |  |
| IP source guard / dynamic IP lockdown |  |
| Podpora Dynamic ARP protection |  |
| Port security |  |
| Ochrana control plane před útoky typu DoS |  |
| **QOS** | IEEE 802.1p - minimální počet front 8 |  |
| Class of Service (CoS) |  |
| Traffic prioritizace (IEEE 802.1p) - minimálně 8 front |  |
| Přiřazení 802.1p tagu na základě L3 (IP adresy, protokolu), L4 (TCP/UDP čísla portu) a DiffServ |  |
| Přiřazení priority na základě L2 (portu nebo VLAN) |  |
| Rate limiting |  |
| Strict priority queuing (SP) |  |
| Weighted round robin (WRR) queuing |  |
| IPV6 QOS |  |
| **Management, monitoring** | CLI formou RJ45 serial konsole port |  |
| USB konzolový port |  |
| OoB management port s podporou ethernetu |  |
| Konfigurace zařízení v člověku čitelné textové formě |  |
| USB port pro přenos konfigurace a firmware |  |
| Podpora managementu přes IPv4 i IPv6 |  |
| SSHv2 a SCP |  |
| Podpora SNMPv2c a SNMPv3 |  |
| RMON |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL |  |
| Lokálně vynucené RBAC na úrovni přepínače |  |
| Dualní flash image |  |
| Podpora oddělených čítačů paketů pro IPv4 a IPv6 provoz |  |
| Podpora RADIUS včetně RADIUS CoA (RFC3576) |  |
| Aktivní monitorování dostupnosti RADIUS serveru přednastaveným jménem a heslem |  |
| Podpora TACACS+ |  |
| Podpora konfiguračních změn pomocí naplánovaných pracovních úloh (Job scheduler) |  |
| Analýza síťového provozu sFlow podle RFC 3176 |  |
| Port mirroring, alespoň 4 různé obousměrné session, SPAN, RSPAN |  |
| Zrcadlení provozu na základě filtrů: Mac-adressa, VLAN, ACL (traffic mirroring) |  |
| Podpora IP SLA pro měření zpoždění provozu |  |
| Podpora OpenFlow verze 1.3 |  |
| Podpora Zero Touch Provisioning (ZTP) |  |
| Software REST API pro automatizaci nastavení sítě |  |
| Podpora Chromecast Gateway |  |
| Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty |  |
| Podpora service insertion včetně technologie VXLAN |  |
| Automatická konfigurace portu dle připojeného zařízení |  |

**2 ks páteřních přepínačů včetně PoE+ napájení**

|  |  |  |  |
| --- | --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje ANO/NE** | **Popis řešení, názvy a popis produktů** |
| **Třída zařízení** | L3 switch |  |  |
| **Formát zařízení a velikost** | do racku 19“, 1U |  |
| **Metalické porty** | 48×10/100/1000 RJ45 PoE+ |  |
| **SFP porty** | 4x 10Gbit SFP+ |  |
| **Interní hot-swap AC napájecí zdroje** | ano, 2x stejný model |  |
| **Dostupný výkon pro PoE+ 802.3at napájení** | 740 W |  |
| **Celková propustnost přepínače** | Minimálně 320 Gb/s |  |
| **Celkový paketový výkon přepínače** | Minimálně 190 mpps |  |
| **Paměťový buffer** | Minimálně 12MB |  |
| **Podpora VLAN podle IEEE 802.1Q** | Nejméně 1000 aktivních VLAN |  |
| **Vlastnosti stohování** | Stohování např. modulem |  |
| Stoh podporuje distribuované přepínání paketů |  |
| Minimální počet přepínačů ve stohu 8 |  |
| Minimální kapacita stohovacího propojení 40 Gb/s |  |
| Součástí dodávky 1m stohovací kabel |  |
| Stoh podporuje linkovou agregaci přes členy (MLAG) |  |
| **Základní funkce a protokoly** | Podpora "jumbo rámců" včetně velikosti 9000 Byte |  |
| Podpora Energy Efficient Ethernet (802.3az) |  |
| Podpora linkové agregace IEEE 802.1AX |  |
| Podpora rozkládání zátěže na LACP dle L2, L3 a L4 parametrů |  |
| Počet záznamů v tabulce MAC adres nejméně 32 000 |  |
| Protokol pro definici šířených VLAN - MVRP |  |
| Podpora MAC based VLAN |  |
| Podpora Private VLAN |  |
| IEEE 802.1s - Multiple Spanning Tree |  |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) |  |
| Detekce protilehlého zařízení pomocí LLDP (včetně rozšíření LLDP-MED) |  |
| Detekce jednosměrnosti optické linky (např. UDLD) |  |
| Tunelování 802.1Q v 802.1Q |  |
| DHCP server |  |
| DHCP relay pro IPv4 a IPv6 včetně option 82 a 79 |  |
| NTP pro IPv4 a IPv6 včetně MD5 autentizace |  |
| Statické směrování IPv4 a IPv6 |  |
| Podpora zapouzdření provozu: 6in4 |  |
| Dynamické směrování RIPv2 a RIPng a OSPF a OSPFv3 včetně podpory BFD |  |
| Policy based routing na základě ACL |  |
| Podpora VRRP podle RFC 3768 včetně podpory BFD |  |
| IGMP v2 a v3 |  |
| MLD v1 a v2 |  |
| Směrování multicast: PIM-DM a PIM-SM |  |
| **Bezpečnost** | Hardware podpora IPv4 a IPv6 ACL |  |
| ACL definice na základě skupiny fyzických portů |  |
| ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN |  |
| BPDU guard |  |
| Root guard |  |
| DHCP snooping pro IPv4 a IPv6 |  |
| HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na % rychlosti portu a množství paketů za vteřinu |  |
| ICMP rate-limiting |  |
| Podpora ověřování 802.1X nejméně 32 uživatelů na port |  |
| RADIUS MAC autentizace, probíhající před 802.1x pro případy, že koncové zařízení není softwarově vybaveno pro 802.1x autentizaci |  |
| Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675 |  |
| Podpora 802.1X Guest VLAN |  |
| Podpora IPv6 RA Guard |  |
| IP source guard / dynamic IP lockdown |  |
| Podpora Dynamic ARP protection |  |
| Port security |  |
| Ochrana control plane před útoky typu DoS |  |
| **QOS** | IEEE 802.1p - minimální počet front 8 |  |
| Class of Service (CoS) |  |
| Traffic prioritizace (IEEE 802.1p) - minimálně 8 front |  |
| Přiřazení 802.1p tagu na základě L3 (IP adresy, protokolu), L4 (TCP/UDP čísla portu) a DiffServ |  |
| Přiřazení priority na základě L2 (portu nebo VLAN) |  |
| Rate limiting |  |
| Strict priority queuing (SP) |  |
| Weighted round robin (WRR) queuing |  |
| IPV6 QOS |  |
| **Management, monitoring** | CLI formou RJ45 serial konsole port |  |
| USB konzolový port |  |
| OoB management port s podporou ethernetu |  |
| Konfigurace zařízení v člověku čitelné textové formě |  |
| USB port pro přenos konfigurace a firmware |  |
| Podpora managementu přes IPv4 i IPv6 |  |
| SSHv2 a SCP |  |
| Podpora SNMPv2c a SNMPv3 |  |
| RMON |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL |  |
| Lokálně vynucené RBAC na úrovni přepínače |  |
| Dualní flash image |  |
| Podpora oddělených čítačů paketů pro IPv4 a IPv6 provoz |  |
| Podpora RADIUS včetně RADIUS CoA (RFC3576) |  |
| Aktivní monitorování dostupnosti RADIUS serveru přednastaveným jménem a heslem |  |
| Podpora TACACS+ |  |
| Podpora konfiguračních změn pomocí naplánovaných pracovních úloh (Job scheduler) |  |
| Analýza síťového provozu sFlow podle RFC 3176 |  |
| Port mirroring, alespoň 4 různé obousměrné session, SPAN, RSPAN |  |
| Zrcadlení provozu na základě filtrů: Mac-adressa, VLAN, ACL (traffic mirroring) |  |
| Podpora IP SLA pro měření zpoždění provozu |  |
| Podpora OpenFlow verze 1.3 |  |
| Podpora Zero Touch Provisioning (ZTP) |  |
| Software REST API pro automatizaci nastavení sítě |  |
| Podpora Chromecast Gateway |  |
| Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty |  |
| Podpora service insertion včetně technologie VXLAN |  |
| Automatická konfigurace portu dle připojeného zařízení |  |

**Požadavky na záruku a podporu a další podmínky pro páteřní přepínače**

* Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství).
* Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů na dobu alespoň 5 let provozu.
* Dodavatel se zavazuje poskytnout záruku na hardware s odesláním náhradního dílu nejpozději následující pracovní den v délce 60 měsíců. Tato záruka musí být zajištěna u osoby autorizované výrobcem zařízení k provádění oprav.
* Dodavatel se zavazuje poskytovat aktualizace software (nové verze programového vybavení) po dobu minimálně 60 měsíců.
* Dodavatel zajistí technickou podporu výrobce zařízení po dobu min. 60 měsíců.
* Dodávka musí obsahovat veškerý spotřební materiál nezbytný pro řádné zapojení a zprovoznění zařízení (např. propojovací kabeláž, …).

## **Požadované řešení – přístupové přepínače s metalickými porty 10/100/1000**

Nové podružné přepínače budou sloužit zejména pro rozšíření počtu zásuvek v budově č.p. 27.

**3 ks 24port přepínačů včetně podpory PoE+ napájení**

|  |  |  |  |
| --- | --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje ANO/NE** | **Popis řešení, názvy a popis produktů** |
| **Třída zařízení** | L2 switch |  |  |
| **Formát zařízení a velikost** | do racku 19“, 1U |  |
| **Metalické porty Porty** | 24×10/100/1000 RJ45 PoE+ |  |
| **SFP porty** | 4x 1Gbit SFP |  |
| **Dostupný výkon pro PoE+ 802.3at napájení** | 195 W |  |
| **Celková propustnost přepínače** | min. 56 Gb/s |  |
| **Celkový paketový výkon přepínače** | min. 40 milionů paketů/s |  |
| **Velikost tabulky MAC adres** | 16000 záznamů |  |
| **Podpora VLAN podle IEEE 802.1Q** | Nejméně 512 aktivních VLAN |  |
| **Základní vlastnosti a protokoly** | Podpora "jumbo rámců" včetně velikosti 9 000 Byte |  |
| Podpora plnohodnotné správy přes IPv4 a IPv6 rozhraní |  |
| Podpora více L3 VLAN rozhraní správy s možností statického směrování management provozu |  |
| MLD snooping |  |
| Detekce protilehlého zařízení pomocí CDP nebo LLDP (včetně rozšíření LLDP-MED) |  |
| Automatická konfigurace VLAN pro IP telefony s využitím LLDP-MED |  |
| Multiple spanning tree |  |
| Podpora spanning tree instance per VLAN s 802.1Q tagováním BPDU rámců |  |
| Protokol pro definici šířených VLAN - MVRP |  |
| IEEE 802.3ad Link Aggregation Control Protocol (LACP) |  |
| Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty |  |
| Monitoring datových toků v síti pomocí NetFlow nebo sFlow |  |
| Software REST API pro automatizaci nastavení sítě |  |
| Rozpoznání připojeného Wi-Fi AP a VLAN na něm nastavených. Automatické přidání takto detekovaných VLAN na port |  |
| **QOS** | Class of Service (CoS) |  |  |
| Traffic prioritizace (IEEE 802.1p) |  |
| Přiřazení 802.1p tagu na základě L3 (IP adresy, protokolu), L4 (TCP/UDP čísla portu) a DiffServ |  |
| Přiřazení priority na základě L2 (portu nebo VLAN) |  |
| Rate limiting |  |
| Strict priority queuing (SP) |  |
| Weighted round robin (WRR) queuing |  |
| IPV6 QOS |  |
| **Bezpečnost** | Podpora více L3 VLAN rozhraní správy s možností statického směrování management provozu |  |  |
| Podpora filtrování MAC adres |  |
| Podpora ověřování 802.1X včetně více uživatelů per-port |  |
| RADIUS MAC autentizace, probíhající před 802.1x pro případy, že koncové zařízení není softwarově vybaveno pro 802.1x autentizaci |  |
| RADIUS/TACACS+ včetně Radius accounting |  |
| Podpora aktivního monitorování RADIUS serveru přednastaveným jménem a heslem |  |
| Podpora RADIUS Change of Authorization (RFC3576) |  |
| STP BPDU port protection |  |
| STP root guard |  |
| Port Security |  |
| Dynamic ARP protection |  |
| DHCP protection |  |
| ACL a IPV6 ACL |  |
| **Management a monitoring** | Lokální logování + Syslog |  |  |
| SNMP verze 2c a 3 |  |
| Command-line interface |  |
| Web GUI |  |
| out-of-band management (serial RS-232C nebo Micro USB) |  |
| Remote monitoring (RMON) |  |
| Dual flash images |  |

**1 ks 24port přepínače bez PoE**

|  |  |  |  |
| --- | --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje ANO/NE** | **Popis řešení, názvy a popis produktů** |
| **Třída zařízení** | L2 switch |  |  |
| **Formát zařízení a velikost** | do racku 19“, 1U |  |
| **Metalické porty Porty** | 24×10/100/1000 RJ45 |  |
| **SFP porty** | 4x 1Gbit SFP |  |
| **Celková propustnost přepínače** | min. 56 Gb/s |  |
| **Celkový paketový výkon přepínače** | min. 40 milionů paketů/s |  |
| **Velikost tabulky MAC adres** | 16000 záznamů |  |
| **Podpora VLAN podle IEEE 802.1Q** | Nejméně 512 aktivních VLAN |  |
| **Základní vlastnosti a protokoly** | Podpora "jumbo rámců" včetně velikosti 9 000 Byte |  |
| Podpora plnohodnotné správy přes IPv4 a IPv6 rozhraní |  |
| Podpora více L3 VLAN rozhraní správy s možností statického směrování management provozu |  |
| MLD snooping |  |
| Detekce protilehlého zařízení pomocí CDP nebo LLDP (včetně rozšíření LLDP-MED) |  |
| Automatická konfigurace VLAN pro IP telefony s využitím LLDP-MED |  |
| Multiple spanning tree |  |
| Podpora spanning tree instance per VLAN s 802.1Q tagováním BPDU rámců |  |
| Protokol pro definici šířených VLAN - MVRP |  |
| IEEE 802.3ad Link Aggregation Control Protocol (LACP) |  |
| Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty |  |
| Monitoring datových toků v síti pomocí NetFlow nebo sFlow |  |
| Software REST API pro automatizaci nastavení sítě |  |
| Rozpoznání připojeného Wi-Fi AP a VLAN na něm nastavených; automatické přidání takto detekovaných VLAN na port |  |
| **QOS** | Class of Service (CoS) |  |
| Traffic prioritizace (IEEE 802.1p) |  |
| Přiřazení 802.1p tagu na základě L3 (IP adresy, protokolu), L4 (TCP/UDP čísla portu) a DiffServ |  |
| Přiřazení priority na základě L2 (portu nebo VLAN) |  |
| Rate limiting |  |
| Strict priority queuing (SP) |  |
| Weighted round robin (WRR) queuing |  |
| IPV6 QOS |  |
| **Bezpečnost** | Podpora více L3 VLAN rozhraní správy s možností statického směrování management provozu |  |
| Podpora filtrování MAC adres |  |
| Podpora ověřování 802.1X včetně více uživatelů per-port |  |
| RADIUS MAC autentizace, probíhající před 802.1x pro případy, že koncové zařízení není softwarově vybaveno pro 802.1x autentizaci |  |
| RADIUS/TACACS+ včetně Radius accounting |  |
| Podpora aktivního monitorování RADIUS serveru přednastaveným jménem a heslem |  |
| Podpora RADIUS Change of Authorization (RFC3576) |  |
| STP BPDU port protection |  |
| STP root guard |  |
| Port Security |  |
| Dynamic ARP protection |  |
| DHCP protection |  |
| ACL a IPV6 ACL |  |
| **Management a monitoring** | Lokální logování + Syslog |  |
| SNMP verze 2c a 3 |  |
| Command-line interface |  |
| Web GUI |  |
| out-of-band management (serial RS-232C nebo Micro USB) |  |
| Remote monitoring (RMON) |  |
| Dual flash images |  |

**1 ks 16port přepínače bez PoE**

|  |  |  |  |
| --- | --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje ANO/NE** | **Popis řešení, názvy a popis produktů** |
| **Třída zařízení** | L2 switch |  |  |
| **Formát zařízení a velikost** | do racku 19“, 1U |  |
| **Metalické porty Porty** | 16×10/100/1000 RJ45 |  |
| **SFP porty** | 2x 1Gbit SFP |  |
| **Celková propustnost přepínače** | min. 40 Gb/s |  |
| **Celkový paketový výkon přepínače** | min. 29 milionů paketů/s |  |
| **Velikost tabulky MAC adres** | 16000 záznamů |  |
| **Podpora VLAN podle IEEE 802.1Q** | Nejméně 512 aktivních VLAN |  |
| **Základní vlastnosti a protokoly** | Podpora "jumbo rámců" včetně velikosti 9 000 Byte |  |
| Podpora plnohodnotné správy přes IPv4 a IPv6 rozhraní |  |
| Podpora více L3 VLAN rozhraní správy s možností statického směrování management provozu |  |
| MLD snooping |  |
| Detekce protilehlého zařízení pomocí CDP nebo LLDP (včetně rozšíření LLDP-MED) |  |
| Automatická konfigurace VLAN pro IP telefony s využitím LLDP-MED |  |
| Multiple spanning tree |  |
| Podpora spanning tree instance per VLAN s 802.1Q tagováním BPDU rámců |  |
| Protokol pro definici šířených VLAN - MVRP |  |
| IEEE 802.3ad Link Aggregation Control Protocol (LACP) |  |
| Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty |  |
| Monitoring datových toků v síti pomocí NetFlow nebo sFlow |  |
| Software REST API pro automatizaci nastavení sítě |  |
| Rozpoznání připojeného Wi-Fi AP a VLAN na něm nastavených. Automatické přidání takto detekovaných VLAN na port |  |
| **QOS** | Class of Service (CoS) |  |
| Traffic prioritizace (IEEE 802.1p) |  |
| Přiřazení 802.1p tagu na základě L3 (IP adresy, protokolu), L4 (TCP/UDP čísla portu) a DiffServ |  |
| Přiřazení priority na základě L2 (portu nebo VLAN) |  |
| Rate limiting |  |
| Strict priority queuing (SP) |  |
| Weighted round robin (WRR) queuing |  |
| IPV6 QOS |  |
| **Bezpečnost** | Podpora více L3 VLAN rozhraní správy s možností statického směrování management provozu |  |
| Podpora filtrování MAC adres |  |
| Podpora ověřování 802.1X včetně více uživatelů per-port |  |
| RADIUS MAC autentizace, probíhající před 802.1x pro případy, že koncové zařízení není softwarově vybaveno pro 802.1x autentizaci |  |
| RADIUS/TACACS+ včetně Radius accounting |  |
| Podpora aktivního monitorování RADIUS serveru přednastaveným jménem a heslem |  |
| Podpora RADIUS Change of Authorization (RFC3576) |  |
| STP BPDU port protection |  |
| STP root guard |  |
| Port Security |  |
| Dynamic ARP protection |  |
| DHCP protection |  |
| ACL a IPV6 ACL |  |
| **Management a monitoring** | Lokální logování + Syslog |  |
| SNMP verze 2c a 3 |  |
| Command-line interface |  |
| Web GUI |  |
| out-of-band management (serial RS-232C nebo Micro USB) |  |
| Remote monitoring (RMON) |  |
| Dual flash images |  |

**6 ks 8port přepínačů bez PoE**

|  |  |  |  |
| --- | --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje ANO/NE** | **Popis řešení, názvy a popis produktů** |
| **Třída zařízení** | L2 switch |  |  |
| **Formát zařízení a velikost** | do racku 19“, 1U |  |
| **Metalické porty Porty** | 8×10/100/1000 RJ45 |  |
| **SFP porty** | 2x 1Gbit SFP |  |
| **Celková propustnost přepínače** | min. 20 Gb/s |  |
| **Celkový paketový výkon přepínače** | min. 14 milionů paketů/s |  |
| **Velikost tabulky MAC adres** | 16000 záznamů |  |
| **Podpora VLAN podle IEEE 802.1Q** | Nejméně 512 aktivních VLAN |  |
| **Základní vlastnosti a protokoly** | Podpora "jumbo rámců" včetně velikosti 9 000 Byte |  |
| Podpora plnohodnotné správy přes IPv4 a IPv6 rozhraní |  |
| Podpora více L3 VLAN rozhraní správy s možností statického směrování management provozu |  |
| MLD snooping |  |
| Detekce protilehlého zařízení pomocí CDP nebo LLDP (včetně rozšíření LLDP-MED) |  |
| Automatická konfigurace VLAN pro IP telefony s využitím LLDP-MED |  |
| Multiple spanning tree |  |
| Podpora spanning tree instance per VLAN s 802.1Q tagováním BPDU rámců |  |
| Protokol pro definici šířených VLAN - MVRP |  |
| IEEE 802.3ad Link Aggregation Control Protocol (LACP) |  |
| Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty |  |
| Monitoring datových toků v síti pomocí NetFlow nebo sFlow |  |
| Software REST API pro automatizaci nastavení sítě |  |
| Rozpoznání připojeného Wi-Fi AP a VLAN na něm nastavených; automatické přidání takto detekovaných VLAN na port |  |
| **QOS** | Class of Service (CoS) |  |
| Traffic prioritizace (IEEE 802.1p) |  |
| Přiřazení 802.1p tagu na základě L3 (IP adresy, protokolu), L4 (TCP/UDP čísla portu) a DiffServ |  |
| Přiřazení priority na základě L2 (portu nebo VLAN) |  |
| Rate limiting |  |
| Strict priority queuing (SP) |  |
| Weighted round robin (WRR) queuing |  |
| IPV6 QOS |  |
| **Bezpečnost** | Podpora více L3 VLAN rozhraní správy s možností statického směrování management provozu |  |
| Podpora filtrování MAC adres |  |
| Podpora ověřování 802.1x včetně více uživatelů per-port |  |
| RADIUS MAC autentizace, probíhající před 802.1x pro případy, že koncové zařízení není softwarově vybaveno pro 802.1x autentizaci |  |
| RADIUS/TACACS+ včetně Radius accounting |  |
| Podpora aktivního monitorování RADIUS serveru přednastaveným jménem a heslem |  |
| Podpora RADIUS Change of Authorization (RFC3576) |  |
| STP BPDU port protection |  |
| STP root guard |  |
| Port Security |  |
| Dynamic ARP protection |  |
| DHCP protection |  |
| ACL a IPV6 ACL |  |
| **Management a monitoring** | Lokální logování + Syslog |  |
| SNMP verze 2c a 3 |  |
| Command-line interface |  |
| Web GUI |  |
| out-of-band management (serial RS-232C nebo Micro USB) |  |
| Remote monitoring (RMON) |  |
| Dual flash images |  |

**Společné požadavky na záruku a podporu a další podmínky pro přístupové přepínače**

* Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství).
* Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů na dobu alespoň 5 let provozu.
* Dodavatel se zavazuje poskytnout záruku na hardware s odesláním náhradního dílu nejpozději následující pracovní den v délce 60 měsíců. Tato záruka musí být zajištěna u osoby autorizované (či jinak pověřené a řádně proškolené) výrobcem zařízení k provádění oprav.
* Dodavatel se zavazuje poskytovat aktualizace software (nové verze programového vybavení) po dobu minimálně 60 měsíců.
* Dodavatel zajistí technickou podporu výrobce zařízení po dobu min. 60 měsíců.
* Dodávka musí obsahovat veškerý spotřební materiál nezbytný pro řádné zapojení a zprovoznění zařízení (např. propojovací kabeláž, ...).

## **Požadované řešení – přepínače – příslušenství a implementace**

**11 ks Přepínač (optický vysílač) minimálně 10 Gbps SPP+**

* ve verzi Singlemode

**1 ks Implementace řešení**

Implementace řešení bude obsahovat nejméně:

* Instalaci prvků do rozvaděčů
* Základní nastavení všech přepínačů
* Zajištění stohování
* Zajištění základních bezpečnostních nastavení a nastavení spanning tree
* Převzetí nastavení portů dle stávajících přepínačů
* Migrace řešení s napojením na optické i metalické sítě a připojení stávajících přepínačů
* Nastavení VLAN sítí (Servery, PC stanice, tiskárny, ….)

Zadavatel poskytne součinnost při potřebné rekonfiguraci stávajících prvků.

# **Požadované řešení – centrální správa síťových prvků**

Zadavatel nedisponuje žádným systémem pro centrální správu sítě. Vzhledem k počtu instalovaných prvků a jejich plánovanému rozšíření je tento stav nevyhovující zejména z pohledu dostupnosti sítě jako takové. Při jakémkoli výpadku se tak zadavatel musí spoléhat na nahlášení uživatelem nebo na statické metody zjišťování stavu sítě. Při nasazení jakékoli změny či řešení opravy pak zadavatel musí spravovat každé zařízení samostatně či se připojit lokálně v místě jeho instalace.

Centrální systém by tedy měl zajistit jak jednodušší správu sítě jako celku, tak zejména rychlejší a přehlednější informace o stavu sítě a jednotlivých prvcích, což přinese v konečném důsledku vyšší dostupnost sítě prostřednictvím předcházení problémům i jejich rychlejší detekce a řešení.

Centrální systém musí plně podporovat všechny nabízené přepínače a stávající přepínače minimálně v rovině SNMP monitoringu.

|  |  |  |  |
| --- | --- | --- | --- |
| **Parametr** | **Požadovaná hodnota** | **Splňuje ANO/NE** | **Popis řešení, názvy a popis produktů** |
| **Typ** | Management nástroj pro správu sítě s podporou správy produktů výrobce nabízených přepínačů a nejméně jednoho dalšího světového dodavatele networking řešení |  |  |
| **Provedení** | Software pro Windows OS, SW appliance nebo HW appliance |  |  |
| **Vlastnosti** | Správa minimálně 50 síťových zařízení (např. přepínačů), možnost rozšíření až do 1000 |  |  |
| Manuální a automatické discovery síťových zařízení |  |  |
| Možnost tvorby SNMP, TELNET a SSH šablon pro hromadný přístup k zařízením |  |  |
| Definice přístupových práv pro jednotlivé operátory na úrovni síťových zařízení a jejich funkcí |  |  |
| Možnost přizpůsobení prostředí ovládací obrazovky (např. pomocí widgetů), zvlášť pro každého síťového operátora |  |  |
| Vizualizace topologie: Layer-2, Layer-3 a spanning tree, možnost tvorby vlastních hierarchických pohledů |  |  |
| Vizualizace datového centra: DC, místnosti, racky, osazení včetně hledání |  |  |
| Správa a vizualizace virtuálních sítí v hypervisorech VMware, Hyper-V a Linux KVM pro přehled spojení virtuální a fyzické infrastruktury |  |  |
| Konfigurační management: zálohy a obnova konfigurace, srovnávání rozdílů, auditování podle přednastavených i vlastních pravidel |  |  |
| Performance management síťových zařízení: dostupnost zařízení i linek, vytížení procesoru, využití operační paměti, vytížení linek |  |  |
| Performance management pro libovolné SNMP statistiky, dlouhodobou historii i real-time grafy obnovované už od každých 5 sekund |  |  |
| Importování vlastních MIB a kompilátor |  |  |
| Podpora SYSLOG |  |  |
| VLAN management: změna nastavení, přidávání, přiřazení portů |  |  |
| ACL management: ACL šablony, optimalizační nástroje, zálohování a deployment |  |  |
| Alarmování, práce se syslog a SNMP trapy včetně vytváření vlastních reakcí na události nebo notifikace ve formě emailu či SMS |  |  |
| Audit zařízení: typ zařízení včetně jednotlivých komponent, verze operačního systému, sériová čísla, informace o jednotlivých portech, historický audit jednotlivých zařízení (např. přesuny) |  |  |
| Vyhledávání a historie zařízení na základě MAC, IP nebo názvu |  |  |
| Bezpečnostní systém analýzy logů s možností integrace IDS/IPS systému schopný dohledat krajní port útočníka a izolovat |  |  |
| Možnost rozšíření zásuvnými moduly o funkce RADIUS, NAC, TACACS+ a správa SLA |  |  |
| Možnost rozšíření o systém pro podporu řízení uživatelů s integrovaným Captive portálem, podporou 802.1X autentifikace, MAC autentifikace, webové autentifikace a autentifikace VPN tunelů |  |  |
| Možnost rozšíření o API postavené na XML volání (RESTful nebo SOAP) pro možnost integrace do aplikací třetích stran |  |  |
| Všechny zásuvné moduly musí umožňovat centrální řízení z jedné aplikace |  |  |
| Podpora vysoké dostupnosti software, možnost běhu v clusteru |  |  |

**Požadavky na podporu a licence**

* Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů na dobu alespoň 5 let provozu.
* Dodavatel se zavazuje poskytovat aktualizace software (nové verze programového vybavení) po dobu minimálně 60 měsíců.
* Dodavatel zajistí technickou podporu výrobce SW po dobu min. 60 měsíců.
* V případě řešení formou HW appliance musí dodávka obsahovat veškerý spotřební materiál nezbytný pro řádné zapojení a zprovoznění zařízení (např. kabeláž, …).

**1 ks Implementace řešení**

Implementace řešení bude obsahovat nejméně:

* Instalace SW nebo nasazení virtuální či HW appliance
* Základní konfigurace
* Integrace s Active Directory zadavatele
* Integrace dodávaných přepínačů v režimu centrální správy a monitoringu
* Integrace stávajících přepínačů minimálně v režimu monitoringu prostřednictvím SNMP
* Součinnost při integraci dodávaných přepínačů na stávající externí monitoring.
* Nastavení pravidelných záloh konfigurací

## **Konsolidace sítě – zajištění vysokorychlostní a spolehlivé WiFi sítě pro vnitřní provoz úřadu i pro občany – návštěvníky úřadu**

Cílem rozšíření a konsolidace neveřejného WiFi řešení je pokrytí zasedacích místností a kanceláří zadavatele s důrazem na zvýšení spolehlivosti, dostupnosti a přenosových rychlostí.

Současné řešení WiFi na úřadě využívá samostatných přístupových bodů bez centrálního řízení a tyto body jsou již nedostatečné z pohledu přenosových rychlostí, spolehlivosti a vzhledem k servisním možnostem i dostupnosti.

Stávající řešení pokrývá pouze 3 zasedací místnosti, odbor investic a odbor životního prostředí.

Požadované řešení předpokládá centrálně řízenou síť, která zajistí co nejlepší využití bezdrátového spektra, bude dostatečně robustní a spolehlivá a zároveň s dobrou mírou zabezpečení. Jednotlivé body (AP) budou řízeny řadičem bezdrátové sítě, který bude buď jako samostatné zařízení, nebo bude integrován do firewallu či bude provozován přímo na kterémkoli vysílacím bodě. Řadič bude provozován v režimu vysoké dostupnosti, aby bylo zajištěno řízení sítě i při výpadku jednoho z prvků.

Pro dosažení přenosových rychlostí, které budou dostatečné nejen v době realizace, je pro přístupové body sítě navržena stanovena norma 802.11ac.

Řešení bude pokrývat kanceláře a zasedací místnosti ve všech třech budovách, tedy č. p. 1 + 151, č. p. 2 a č. p. 27. Přístupové body budou rozmístěny s cílem pokrytí definovaných prostor na základě zpracování modelového sitesurvey vycházejícího z plánů jednotlivých budov.

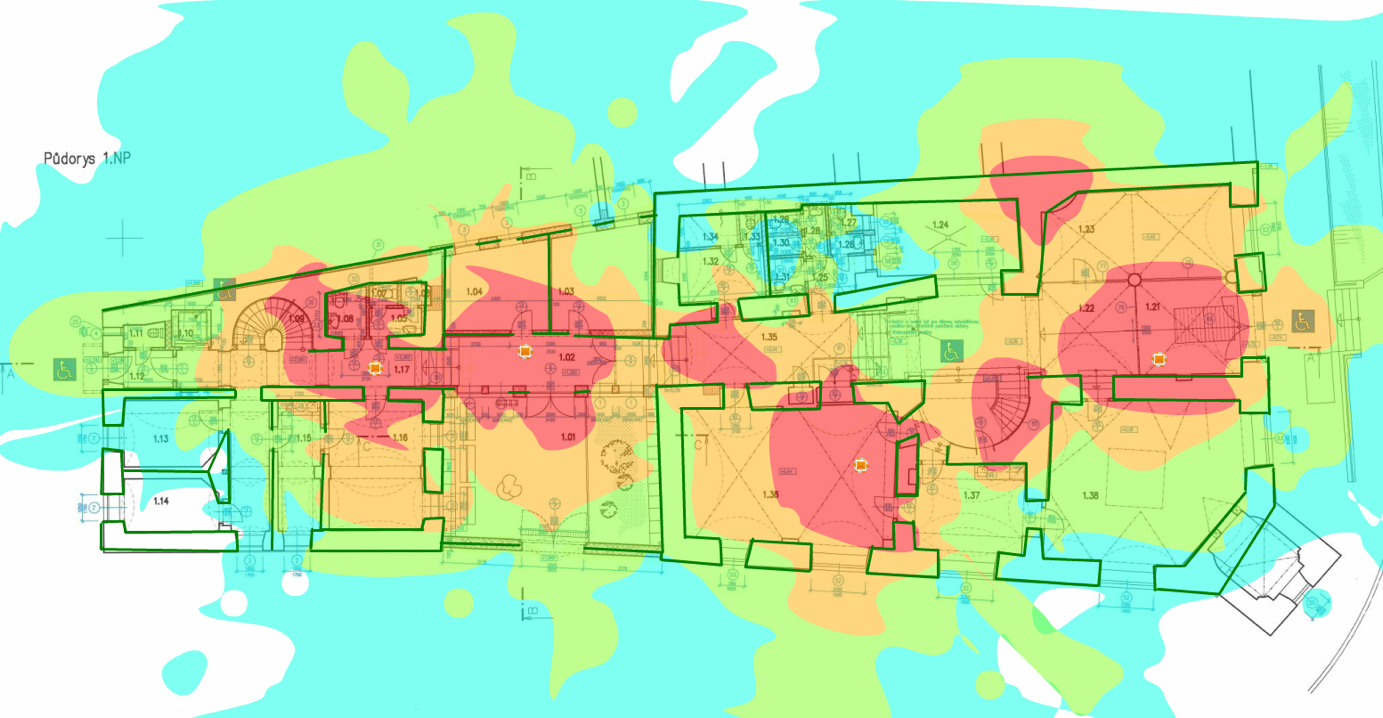
Přístupové body budou připojeny k zásuvkám, které pro tento účel vyhradí zadavatel.

## **Výstup z provedeného sitesurvey – pro frekvenci 5 GHz**

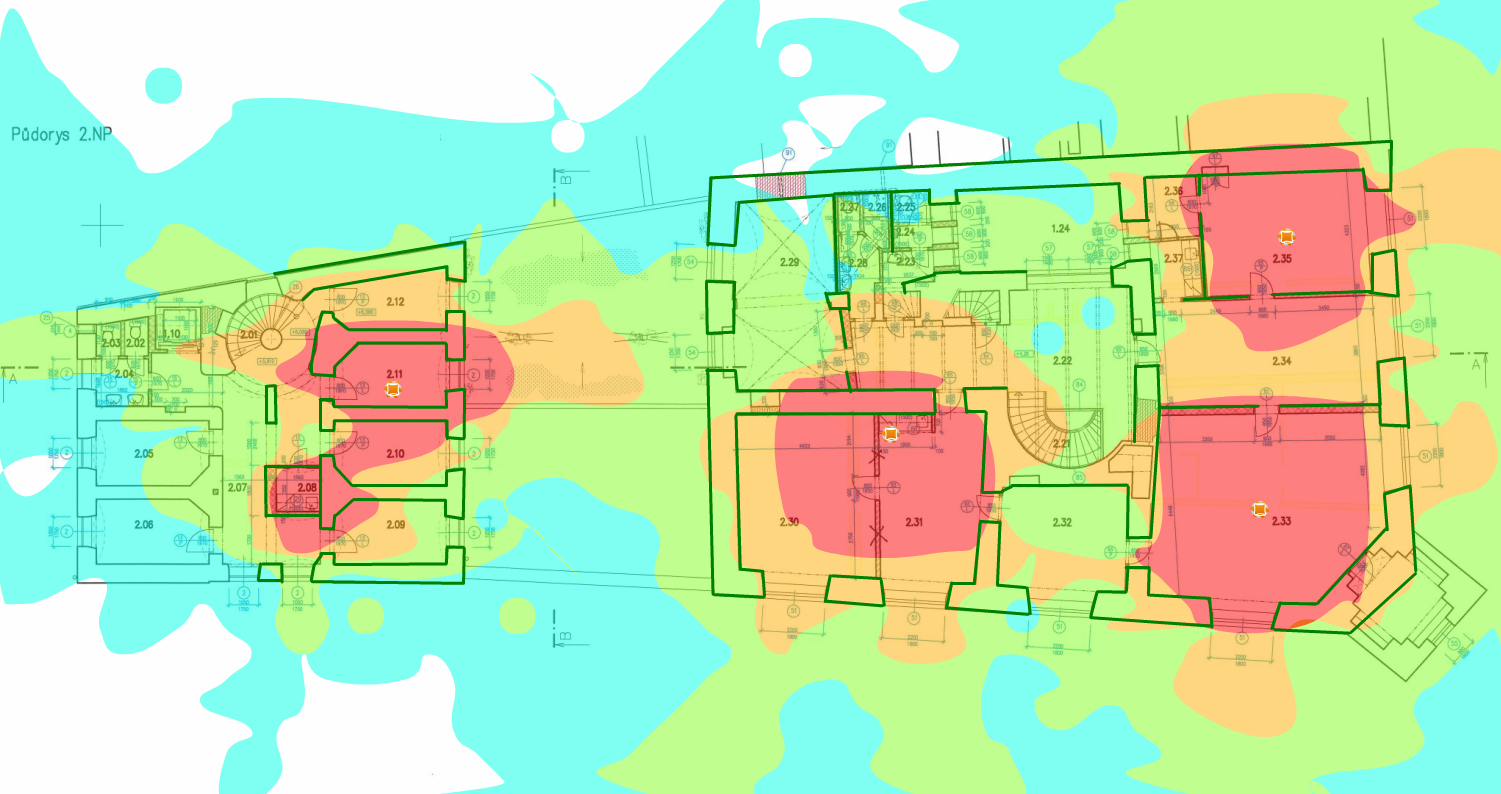
## (s frekvencí 2,4 GHz je situace lepší díky lepšímu šíření signálu)

Zelená barva reprezentuje ještě dostatečně kvalitní signál.

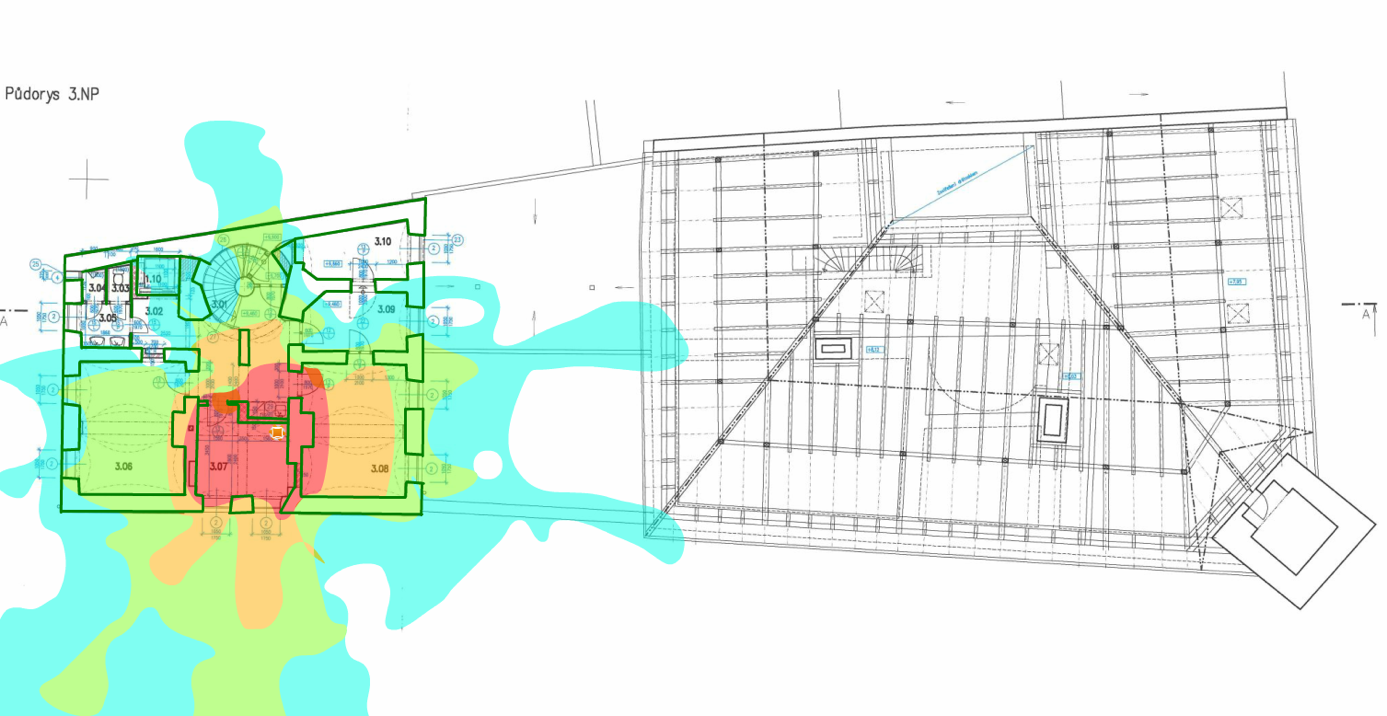
### Č.P. 1 + 151 1.NP



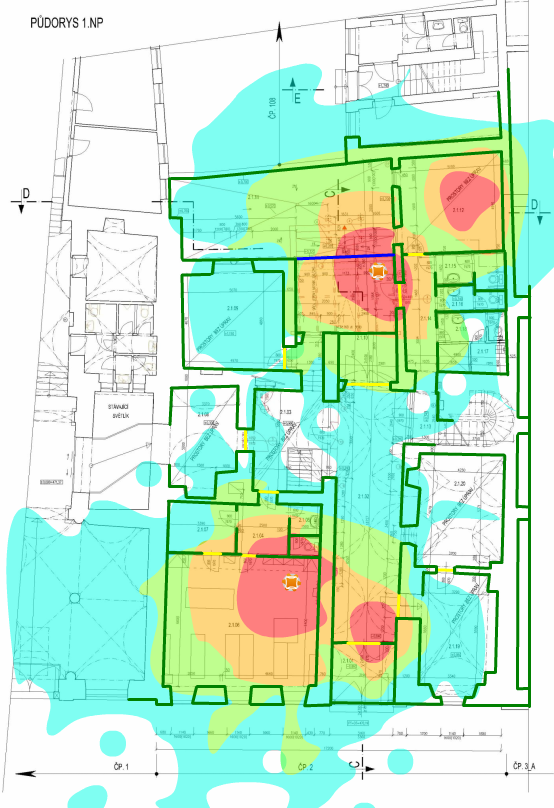
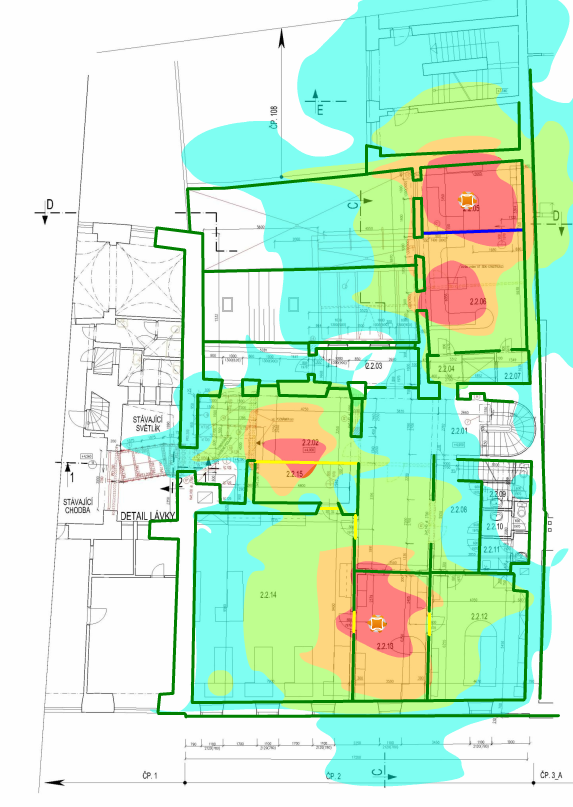
### Č.P. 1 + 151 2.NP



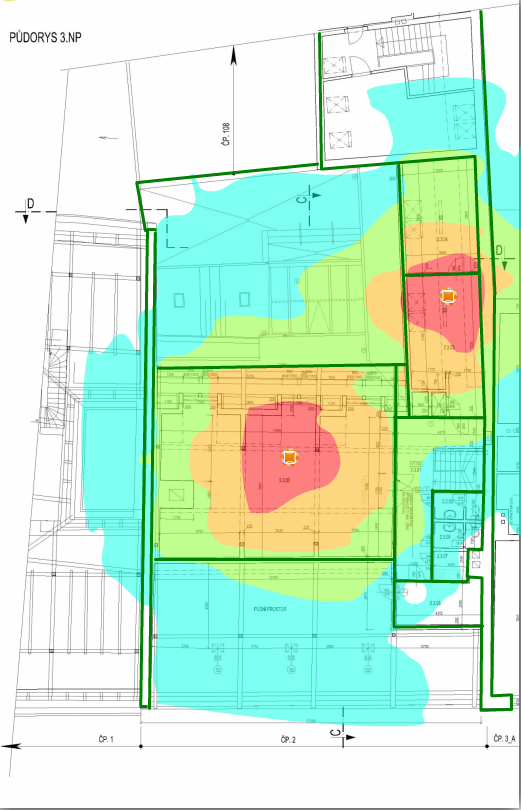
### Č.P. 1 + 151 3.NP

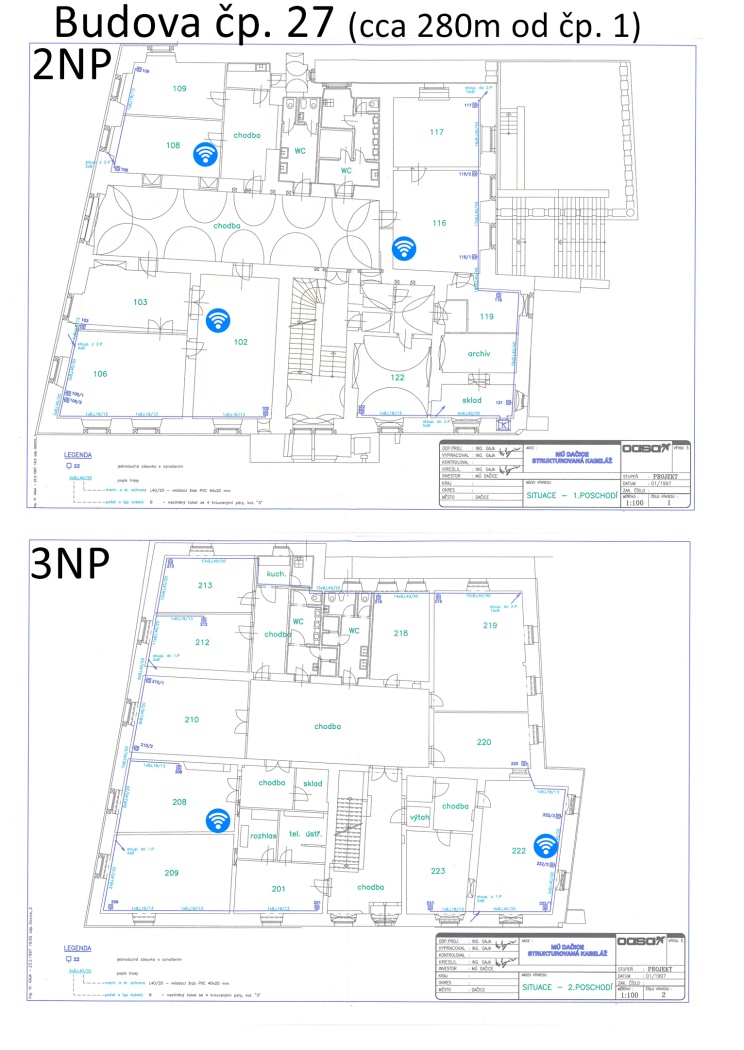


Č.P. 2 1.NP Č.P. 2 2.NP

Č.P. 2 3.NP





## **Požadované řešení – Přístupové body (AP) Wi-Fi sítě a řadič v režimu vysoké dostupnosti**

**Řadič bezdrátové sítě + 20ks AP pro vnitřní pokrytí s integrovanými anténami včetně montážního kitu**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parametr** | **Minimální požadavky** | **Splňuje ANO/NE** | **Popis řešení, názvy a popis produktů** |
| **Přístupové body bezdrátové sítě (AP)** | Podpora normy 802.11ac wave2 |  |  |
| Možnost provozu klientů s normou 802.11 a/g/n |  |
| Duální radiová část (2,4GHz a 5GHz), umožňující současný provoz na obou kmitočtech |  |
| Technologie MU-MIMO 2x2:2 (2x2 MIMO se 2 prostorovými streamy) |  |
| 8 BSSID na radio |  |
| 1x 10/100/1000BASE-T Ethernet (RJ-45); auto MDI/MDIX |  |
| Možnost definovat různé ESSID pro každé pásmo |  |
| Možnost označit provoz 802.1Q na základě ESSID i na základě přihlášeného uživatele |  |
| Napájení PoE+ dle specifikace 802.3af nebo 802.3at |  |
| Centrální správa přes řadič |  |
| Až 255 asociovaných klientských zařízení na rádio |  |
| Licence bez omezení počtu uživatelů |  |
| Podpora upgrade firmware |  |
| Manuálně konfigurovatelný vysílací výkon (prostřednictvím řadiče) |  |
| Změna vysílací frekvence nezpůsobí restart přístupového bodu |  |
| Zamezení změny frekvence, která by způsobila výpadek připojení klienta |  |
| Automatické omezení vysílacího výkonu dle platné legislativy |  |
| Podpora band steering |  |
| Podpora migrace zařízení mezi AP vyvolaná řadičem (sítí) |  |
| Podpora detekce a eliminace RogueAP (nemožnost připojení na detekovaný RogueAP) |  |
| Podpora QoS na 7. vrstvě OSI modelu, automatický QoS pro VoIP/video na L7 |  |
| Administrátorský přístup HTTPS, SSH na AP |  |
| DHCP server / klient, DNS klient, NTP klient |  |
| Terminace dat možná na ethernetu přístupového bodu (data neprochází řadičem) |  |
| Podpora tunelování veškerého uživatelského provozu skrze řadič |  |
| Oddělení provozu hostů od interních dat |  |
| Podpora 802.11h a WMM |  |
| Podpora WEP a WPA2-PSK/AES a WPA2-Enterprise/AES |  |
| Podpora ověřování uživatelů proti LDAP/ Radius / interní databázi řadiče |  |
| Automatická optimalizace sítě (přidělování kanálů, fast roaming, rozdělení klientů) |  |
| Automatická regulace vysílacího výkonu a frekvence v závislosti na okolním prostředí řízená řadičem |  |
| Podpora SNMPv2/SNMPv3 |  |
| Podpora logování na syslog server |  |
| Podpora DHCP snooping |  |
| Podpora IPv6 |  |
| V případě odcizení přístupového bodu nedojde k odcizení citlivých údajů (certifikáty atp.)  Integrované antény |  |
| Součástí dodávky montážní kit pro montáž na strop |  |
| **Řadič bezdrátové sítě** | Přípustné řešení je dedikovaný HW řadič, řadič v dodávaném firewallu nebo řadič provozovaný na jednom z AP |  |
| Řadič musí být umístěn u zákazníka, tj. není přípustné cloudové řešení řadiče |  |
| Není přípustný softwarový řadič instalovaný na prostředcích zadavatele |  |
| Řadič bude provozován v režimu vysoké dostupnosti |  |
| Podpora minimálně 64 přístupových bodů |  |
| Licence bez omezení počtu uživatelů |  |
| Administrátorský přístup HTTPS a SSH |  |
| Administrátorské profily alespoň: plný přístup/pouze čtení/hostovké účty |  |
| Podpora virtuálních kontextů na řadiči |  |
| Podpora logování na syslog server |  |
| Captive portál součástí řadiče |  |
| Podpora až 64 AP bez nutnosti dokupovat licence |  |
| Firewall IPv4 integrovaný v řadiči včetně podpory NAT |  |
| Podpora tunelování veškerého uživatelského provozu skrze řadič |  |
| Možnost dešifrovaní uživatelského SSL provozu |  |

**Požadavky na záruku a podporu a další podmínky**

* Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství).
* Dodavatel se zavazuje poskytnout záruku na hardware s odesláním náhradního dílu či nového zařízení následující pracovní den v délce 60 měsíců.
* Dodavatel se zavazuje poskytovat aktualizace firmware a software (nové verze programového vybavení) po dobu minimálně 60 měsíců.
* Dodavatel zajistí technickou podporu výrobce zařízení po dobu min. 60 měsíců.

**1 ks Montáž AP a Implementace řešení centrálně řízené WiFi sítě**

Implementace řešení bude obsahovat nejméně:

* Montáž AP a jejich připojení k vyznačeným zásuvkám
* Základní nastavení celé sítě
* Konfigurace dvou SSID (jedno s Captive portálem)
* Integrace do sítě (VLAN, toky, routing)

Připojení AP k zásuvkám bude provedeno způsobem odpovídajícím potřebám zadavatele z pohledu technických možností daných prostor i potřebám vizuálním, tedy skrytého vedení kabelů apod. Montážní materiál a kabeláž bude součástí dodávky.

# **Zabezpečení – Zvýšení bezpečnosti perimetru sítě**

Pro zajištění bezpečnosti proti hrozbám z internetu a zároveň pro zajištění vysoké dostupnosti hraničního prvku internetového připojení bude nasazena dvojice bezpečnostních firewallů s funkcionalitami UTM.

Na firewallu bude řízen provoz mezi jednotlivými zónami s rozdílnou úrovní důvěryhodnosti (například Internet vs. DMZ, uživatelé vs. DMZ, WiFi uživatelé vs. interní servery apod.).

Řízení přístupu bude probíhat buď tradičním způsobem na základě IP adres, nebo díky vazbě se systémem řízení identit, na základě uživatelských rolí.

Kromě funkce stavového firewallu zadavatel požaduje, aby dvojice firewallů disponovala pokročilými bezpečnostními funkcionalitami:

* **Antivirovou ochranu**, která kontroluje procházející datové toky v reálném čase a odhaluje a odstraňuje viry, červy, spyware a prohlíží a kontroluje přílohy příchozích a odchozích e-mailových zpráv.
* **IDS/IPS systém**, který chrání na základě databáze signatur síť jak před známými útoky z internetu, tak obsahuje i metody ochrany proti dosud neznámým útokům.
* **Web filtering s podporou kategorií,** který umožňuje omezit či zakázat přístup k nežádoucím kategoriím webů a blokuje potencionálně nebezpečné Java aplety, cookies a Active X skripty.
* **VPN** umožňuje vytvářet zabezpečené přístupy z internetu do vnitřní sítě pomocí SSL nebo IPSec technologií.
* **Aplikační kontrolu**  pro rozpoznávání komunikace konkrétních aplikací a možnost vytvářet pravidla pro dané aplikace, například omezit nebo úplně zakázat provozování z pohledu bezpečnosti nežádoucích aplikací, jako jsou například P2P a sociální sítě.
* **Antispam** umožňuje vytvářet zakázané a povolené seznamy domén, IP adres a e-mailových adres, a takto vydefinovaná pravidla aplikovat na jednotlivé uživatele nebo skupiny uživatelů.
* **Možnost integrace se systémem Sandbox,** který pomocí virtualizace prostředí, ve kterém testuje podezřelé soubory, dokáže výrazně zvýšit zabezpečení a také reagovat na hrozby v raném stádiu rozšíření**.**
* **Ochrana proti tzv. zpětnému volání Botnet sítí**

Pro pokročilou bezpečnostní analýzu zadavatel požaduje, aby nabídka nového zabezpečení perimetru obsahovala analytický nástroj formou samostatného softwarového/hardwarového zařízení, které umožní na jednom místě shromažďovat, analyzovat a porovnávat data z navržených firewallů, zobrazovat na jednom terminálu podrobná data o provozu na firewallech a generovat reporty.

Reporty musí být snadno přizpůsobitelné, musí umožnovat filtrovat a prozkoumávat z firewallů získaná data, například kompletní datové přenosy, události, výskyty virů, útoky, obsah webové komunikace. Také musí obsahovat pokročilé́ funkce pro správu zařízení, například souborové́ karantény, korelaci událostí, analýzu síťového provozu, hodnocení zranitelnosti sítě.

Tento analytický nástroj musí plně podporovat navržené firewallové řešení a být s ním integrované.

## **Požadované řešení – 2 ks UTM firewall včetně analytického nástroje:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parametr** | **Minimální požadavky** | **Splňuje ANO/NE** | **Popis řešení, názvy a popis produktů** |
| **Propustnost L3 Firewall** | 4 Gbps (64 byte UDP) |  |  |
| **Propustnost NGFW (IPS + aplikační kontrola)** | 350 Mbps (tzv. Enterprise Traffic mix nebo IMIX) |  |
| **Propustnost UTM (IPS + aplikační kontrola + Antivirus)** | 250 Mbps (tzv. Enterprise Traffic mix nebo IMIX) |  |
| **Současných spojení** | 2 000 000 |  |
| **Propustnost SSL VPN** | 250 Mbps |  |
| **Základní parametry** | Režim fungování L2 – transparentní režim, L3 – NAT/Router |  |
| Podpora multicast, vytváření politiky pro multicast routování |  |
| konfigurace, internet browsing konfigurace, podpora více tunelů – redundantní VPN, možnost VPN v L2 – transparentním režimu |  |
| Podpora PPTP, L2TP, GRE |  |
| Podpora IPv6 |  |
| Podpora dynamických routovací protokolů - (RIP, OSPF, BGP) |  |
| Virtuální domény/kontexty/firewally – minimálně 5 |  |
| **Vysoká dostupnost** | Podpora režimu vysoké dostupnosti (Active Active, Active Passive, full mesh HA) |  |
| Synchronizace stavové tabulky mezi nódy v clusteru |  |
| Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora healt check funkcí |  |
| **Bezpečnostní parametry** | Podpora VPN: SSL (portálový režim, tunelový režim), IPSEC (IKE, manual key, certifikát, gateway to gateway, hub and spoke, dial up |  |
| SSL offloading pro možnost inspekce příchozího SSL provozu |  |
| UTM funkce – možnost výběru mezi file based režimem (buffer) nebo flow based (inspekce on-the-fly) |  |
| Web Filter – založený na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne |  |
| Web Cache |  |
| Explicitní Proxy |  |
| Reverzní proxy |  |
| WCCP |  |
| Propojení se Sandbox |  |
| Podpora silné autentizace uživatelů – integrovaná podpora generátoru jednorázových hesel (OTP) |  |
| Podpora dvoufaktorové autentizace |  |
| Podpora certifikátů pro ověření uživatelů |  |
| Podpora blokování volání C&C center Botnet sítí již na interface |  |
| **Analytický nástroj** | Minimální velikost diskového prostoru pro logy a reporty 1 GB |  |
| Může být HW zařízení nebo virtuální appliance (podpora nejméně Hyper-V, Vmware, KVM) |  |
| Možnost dostat se proklikem z vizuálního zobrazení na konkrétní logy |  |
| Realtime a historický náhled do logů |  |
| Před-vytvořený dashboard pro NOC |  |
| Podpora prohlížení statistických údajů nad logy |  |
| Korelace logů |  |
| Samostatné sekce týkající se hrozeb v síti |  |
| Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF |  |
| Generování reportů v pravidelných intervalech |  |
| Předdefinované vzory reportů pro nejčastější použití |  |
| Možnost vytváření vlastních reportů na základě SQL dotazů |  |
| Event management, upozorňování na informace z logů, Email, SNMP trapy |  |

**Požadavky na záruku a podporu a další podmínky**

* Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství a potřebné kabeláže).
* Dodavatel se zavazuje poskytnout záruku na hardware s odesláním náhradního dílu nejpozději následující pracovní den v délce 60 měsíců.
* Dodavatel se zavazuje poskytovat aktualizace software (nové verze programového vybavení) po dobu minimálně 60 měsíců.
* Dodavatel zajistí technickou podporu výrobce po dobu min. 60 měsíců.
* Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných parametrů na dobu alespoň 5 let provozu.
* Licence UTM v délce 60 měsíců.

**1 ks Implementace UTM firewall včetně analytického nástroje**

Implementace řešení bude obsahovat nejméně:

* Montáž obou firewallů do rozvaděčů
* Základní nastavení firewallů a analytického nástroje
* Zajištění HA firewallů
* Integraci firewallů MS Active Directory zadavatele
* Převzetí základních firewallových politik ze stávajícího řešení
* Integraci firewallů a analytického nástroje
* Základní nastavení SSL VPN pro 2 skupiny uživatelů
* Nasazení celého řešení – migrace a napojení na infrastrukturu

Zadavatel poskytne součinnost v podobě konfigurace stávajících řešení (propojení s Active Directory pro autentizaci uživatelů apod.) a přípravy podkladů pro vytvoření/migraci bezpečnostních politik firewallu.

# **Zálohování dat – NAS úložiště**

Důležitým aspektem konceptu je důraz na datovou bezpečnost a zálohování, proto je součástí řešení dedikované diskové pole – NAS úložiště a SW pro správu zálohování.

## **Požadované řešení**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parametr** | **Minimální požadavky** | **Splňuje ANO/NE** | **Popis řešení, názvy a popis produktů** |
| **Formát zařízení a velikost** | do racku 19“, maximálně 2U |  |  |
| **Pamět RAM** | 16 GB |  |
| **Pozice na disky** | 12 x 3.5” nebo 2.5” SATA 6Gb/s, SATA 3Gb/s HDD nebo SSD, včetně disků 12 TB |  |
| Pevný disk vyměnitelný za chodu |  |
| **Metalické porty** | 2x RJ-45 1GbE LAN port  2x RJ-45 10GbE LAN port |  |
| **USB porty** | 1x USB 3.0 pro externí pevný disk |  |
| **Certifikováno pro použití virtualizačního software** | Podpora minimálně HyperV Windows Server 2012 R2, Windows Server 2012 |  |
| **Podpora RAID** | RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |  |
| **Cache pro SSD** | Pro čtení i zápis |  |
| Podpora iSCSI pro připojení k serverům |  |
| iSCSI LUN Clone/Snapshot |  |
| Podpora Link Aggregation včetně LACP |  |
| **Instalované disky** | 4 ks 3TB 3.5” SATA 6Gb/s s optimalizací pro NAS a plně kompatibilní |  |

**Požadavky na záruku a další podmínky**

* Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství).
* Dodavatel se zavazuje poskytnout záruku po dobu min. 60 měsíců.
* Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů na dobu alespoň 5 let provozu.