Specifikace požadavků zadávací dokumentace je po doplnění dodavatelem zároveň přílohou č. 2 smlouvy

VZ-IT-2018-1.3

Specifikace požadavků ZD k zakázce

Obnova síťové infrastruktury

Obsah:

[1 Cíl zakázky 3](#_Toc526508226)

[2 Popis stávajícího stavu 3](#_Toc526508227)

[3 Sizing nového řešení a základní požadavky 3](#_Toc526508228)

[4 Předmět veřejné zakázky 4](#_Toc526508229)

[4.1 Detailní specifikace poptávaného řešení 5](#_Toc526508230)

[4.1.1 2x nový centrální firewall pracující v HA režimu 6](#_Toc526508231)

[4.1.2 1x nový firewall vzdálené lokality 11](#_Toc526508232)

[4.1.3 2x Nový core switch 12](#_Toc526508233)

[4.1.4 Nové přístupové switche 16](#_Toc526508234)

[4.1.5 Společné parametry pro centrální správu switche TYP 1 / TYP2 / TYP4 17](#_Toc526508235)

[4.1.6 Specifikace TYP 1 19](#_Toc526508236)

[4.1.7 Specifikace TYP 2 19](#_Toc526508237)

[4.1.8 Specifikace TYP 4 20](#_Toc526508238)

[4.1.9 Parametry pro Switch TYP 3 20](#_Toc526508239)

[4.1.10 Parametry pro Switch TYP 5 22](#_Toc526508240)

[4.1.12 Systém pro ukládání a korelaci logů 25](#_Toc526508241)

[4.2 Instalace, konfigurace, zaškolení obsluhy, dokumentace skutečného provedení 26](#_Toc526508242)

[5 Požadavky na uchazeče – Kvalifikační požadavky 27](#_Toc526508243)

[5.1 Potvrzení dodavatele od výrobce 27](#_Toc526508244)

[5.2 Realizační tým dodavatele 27](#_Toc526508245)

[5.3 Čestné prohlášení dodavatele 27](#_Toc526508246)

# Cíl zakázky

Obnova a rozšíření stávajícího vybavení síťové infrastruktury, která zajišťuje běžný provoz IT technologií, potřebných k provozu administrativních a výzkumných informačních systémů. Stávajícímu vybavení končí podpora výrobce a již ji nelze prodloužit. Zároveň docházejí zdroje (především porty), výkon a zařízení nevyhovuje z pohledu aktuálních bezpečnostních hrozeb.

Kromě prosté obměny a rozšíření síťového vybavení je cílem i celková modernizace koncepce IT. Důraz je kladen na používání nových, moderních technologií, které mají být efektivní, spolehlivé a zároveň jednoduché pro správu.

Jedním z klíčových požadavků na navržené řešení, je využití stávajících prostředků i v novém prostředí. Cílem je využít tyto zdroje pro neprodukční (nekritické) systémy. Nové zařízení musí být se stávajícím síťovým zařízením plně kompatibilní.

Součástí nového řešení je i posílení stávajícího vybavení síťové infrastruktury a připojení do datové sítě 10Gb ethernetem.

# Popis stávajícího stavu

Stávající řešení využívá dva L3 core prvky umístěné v hlavní serverovně, které obsahují 12 SFP portů a 24 metalických gigabitových portů. Jsou centrem optické páteřní sítě topologie hvězda. FO kabely jsou typu singlemode 9/125, vzdálenost každého segmentu je do 10km. Jako přístupové prvky jsou použity L2 switche s 8/24 metalickými gigabitovými porty. L2 switche jsou do páteře připojeny SFP FO uplinky. Do core prvků jsou připojeny servery metalickými GBe porty.

Pro připojení do internetu a ochranu perimetru slouží firewall umístěný v centrální serverovně.

Výzkumný ústav má vzdálenou lokalitu, která má ochranu perimetru a připojení do internetu řešenou samostatným firewallem a mezi centrálou a vzdálenou lokalitou je propojení řešeno site to site VPN. Ve vzdálené lokalitě je umístěn navíc L2 switch pro připojení koncových zařízení.

Veškeré zařízení je již bez podpory výrobce a bezpečnostní parametry a výkon řešení neodpovídá současným standardům.

# Sizing nového řešení a základní požadavky

V Q3/2017 proběhlo měření zatížení aktuálního vybavení a na základě těchto vstupů vznikl Sizing nového prostředí. Přesná specifikace požadavků na nové vybavení je definována v dalších kapitolách tohoto dokumentu. Sizing nového řešení počítá s rezervou do budoucna s výhledem na minimálně 4 roky dopředu.

# Předmět veřejné zakázky

Předmětem veřejné zakázky je dodávka aktivních prvků LAN sítě, dodávka firewallů, dodávka centrálního managementu pro správu aktivních prvků a systému pro ukládání a korelaci logů.

Nové řešení se skládá z následujících komponent:

1. 2x nový Core switch
   * 24x GE/10 GE SFP+ ports
   * Funkční integrace s firewall platformou
   * 4letá podpora výrobce v režimu 24x7
2. 2x nový centrální firewall pracující v HA režimu
   * NGFW platforma ve formě HW appliance
   * Podpora virtualizace
   * Funkční integrace s core a access vrstvou sítě
   * 4letá podpora výrobce v režimu 24x7
3. 1x nový firewall pro vzdálenou lokalitu
   * 4letá podpora výrobce v režimu 24x7
4. 4x nový přístupový switch typ 1
   * Osazen minimálně 48x GE PoE + RJ45 a 4x10 GE SFP+ port
   * Note SFP+ porty jsou kompatibilní s 1 GE SFP
   * 4 letá podpora výrobce v režimu 24x7
5. 4x nový přístupový switch typ 2
   * Osazen minimálně 24 GE PoE+ a 2x10 GE SFP+ port
   * Note: SFP+ porty jsou kompatibilní s 1 GE SFP
   * 4 letá podpora výrobce v režimu 24x7
6. 4x nový přístupový switch typ 3
   * Osazen minimálně 8 GE PoE+ porty + 2 SFP port
   * 4 letá podpora výrobce v režimu 24x7
7. 3x nový přístupový switch typ 4
   * Osazen minimálně 48 GE porty + 4x10 GE SFP+ port
   * Note: SFP+ ports are compatlble with 1 GE SFP
   * 4 letá podpora výrobce v režimu 24x7
8. 1x nový přístupový switch typ 5
   * Osazen minimálně 24 GE PoE+ porty a 4x GE SFP port
   * 4 letá podpora výrobce v režimu 24x7
9. Dodávka systému pro ukládání a korelaci logů plně kompatibilní s dodávanými zařízeními (switch, firewall)
   * 4 letá podpora výrobce v režimu 24x7
10. Veškeré dodávané prvky a systémy (core switche, access switche, firewall, systém pro ukládání a korelaci logů) budou spravovány jednotným managementem, který bude součástí dodávky
11. 20 x nový Modul Transceiver LX
    * LX Transceiver Module
12. 44 x nový Modul Transceiver
    * 10 Gig SFP + Long Range
13. 8x nový Accessories
    * Misc Accessories, 10GE SFP+ Pasive Direct Attach Cable
14. 8x nový Modul Transceiver SFP Gig
    * copper Transceiver Module
15. 64 x nový LC/SC Singlemode 3 m
16. Instalace, konfigurace, zaškolení obsluhy, dokumentace skutečného provedení
    * Rozsah instalačních a konfiguračních prací a školení v rozsahu 18MD

## Detailní specifikace poptávaného řešení

V této kapitole je popsána detailní technická specifikace poptávaných komponent celého řešení.

Požadujeme možnost přihlášení se na technický portál výrobce pro vzdálenou podporu, možnost stažení aktuálního firmware apod..

Součástí dodávky centrálních FW jsou subskripce: UTM funkce, IPS, aplikační kontrola, WEB Filtrování na dobu 4roky

Na žádný HW ani SW nesmí být vyhlášen konec prodeje ani výroby.

### 2x nový centrální firewall pracující v HA režimu

Jedná se o dva totožné firewally v minimální konfiguraci:

V rámci tohoto projektu požadujeme dodání NGFW platformy ve formě HW appliance, která bude plnit zároveň roli perimetrového firewallu a roli interního segmentačního firewallu. Z toho důvodu klademe vysoké požadavky jak na výkonnost aplikačních kontrol, tak na výkonnost firewallu na úrovni L4. S ohledem na integraci těchto dvou rolí požadujeme také podporu virtualizace na daném HW tak, aby bylo možné jednotlivé logické prvky vyčlenit do samostatných virtuálních instancí. Požadavek na počet virtuálních instancí je volen tak, aby bylo možné dále využít samostatné virtuální FW instance v režimu L2 pro ochranu/monitoring dalších vybraných síťových segmentů.

Důležitým požadavkem je dále funkční integrace s přístupovou vrstvou sítě. Cílovým stavem je prostředí, ve kterém je plně funkčně integrována platforma NGFW s přístupovou vrstvou sítě (switche, následně i AP) tak, aby měl administrátor detailní přehled o dění v celé síti, a to v rámci jednoho management rozhraní. Takto zobrazované informace musí obsahovat minimálně data z bezpečnostních prvků (firewallů), wireless i wired sítě (switche, AP) a také detailní informace o koncových stanicích. Tato funkcionalita je detailněji popsána v kapitole s požadavky na switche.

|  |  |  |  |
| --- | --- | --- | --- |
| Požadovaná funkcionalita/vlastnost | | Požadované funkcionality  /vlastnosti | Způsob splnění požadované funkcionality  /vlastnosti |
| Výkon a funkcionalita firewallu | | |  |
| Formát zařízení | | Appliance, 1RU |  |
| Možnost doplnění o záložní napájecí zdroj | | Ano |  |
| Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených | | 1 |  |
| Minimální počet 1Gb 10/100/1000 BaseT Ethernet | | 12 |  |
| Minimální počet 1Gb SFP rozhraní portů pro data, standardně osazených | | 4 |  |
| Podporovaný počet současně otevřených spojení stavový FW | | Min.2M |  |
| Rychlost vytváření nových spojení přes stavový FW | | Min. 130K/s |  |
| Propustnost stavového firewallu (UDP 64B) | | Min. 18 Gbps |  |
| Propustnost aplikačního FW (next-gen FW) – (top parametry) | | Min. 3 Gbps |  |
| Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (top parametry) | | Min. 1,8 Gbps |  |
| Propustnost aplikačního FW (next-gen FW) | | Min. 800 Mbps |  |
| Propustnost aplikačního FW + IPS (next-gen FW, IPS) | | Min. 800 Mbps |  |
| VPN propustnost IPSec | | Min. 8 Gbps |  |
| Současný počet VPN spojení IPSec | | Min. 1 500 |  |
| Podpora L2 (transparentního) módu s podporou NAT a PAT | | Ano |  |
| Podpora L3 (routovaného) módu s podporou NAT a PAT | | Ano |  |
| Podporovaný počet VLAN v L3/L2 mode | | Min. 4000/250 |  |
| Podpora HA v režimu A-A i A-P, podpora stateful failover | | active/standby |  |
| Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podorou LACP | | Ano |  |
| Dynamické směrování - podpora alespoň RIP, OSPF, BGP | | Ano |  |
| Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP | | Ano |  |
| Podpora Policy based Routing (PBR musí být možné nakonfigurovat pomocí minimálně následujících metrik: protokol, interface, zdrojová adresa, cílová adresa, type of service) | | Ano |  |
| Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod. | | Ano |  |
| Podpora filtrace IPv4, IPv6 | | Ano |  |
| Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD | | Ano |  |
| Podpora inspekce IPv6 provozu | | Ano |  |
| Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu | | Ano |  |
| Podpora NAT64 a DNS64 | | Ano |  |
| Funkce QoS | | Ano |  |
| Možnost rozšíření o funkce NextGen FW | | Ano |  |
| Možnost rozšíření o funkce NextGen IPS | | Ano |  |
| Možnost rozšíření o funkce URL filtrace | | Ano |  |
| Možnost rozšíření o ochranu tzv. „Zero-day“ Anti-Malware | | Ano |  |
| Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele | | Ano |  |
| Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech | | Ano |  |
| Firewall musí podporovat aplikační kontrolu a kategorizaci webových stránek jako svou nativní funkcionalitu; identifikace aplikací musí být prováděna napříč všemi porty/protokoly. | | Ano |  |
| Konkrétní aplikace/kategorie aplikací a/nebo kategorie URL musí být nativní součástí vytváření standardního bezpečnostního pravidla. | | Ano |  |
| Možnost tvorby firewall pravidla na základě minimálně těchto parametrů: zdrojová adresa, cílová adresa, uživatel/skupina, aplikace, kategorie webových stránek. | | Ano |  |
| API rozhraní pro integraci s dalšími systémy | | Ano |  |
| Možnost začlenit do SDN řešení | | Ano |  |
| Požadované vlastnosti funkcionality IPS (licence musí být součástí nabídky) | | |  |
| Možnost definovat typ provozu předávaný k inspekci do IPS | | Ano |  |
| Podpora také IDS režimu – pasivního monitorování (TAP režim) | | Ano |  |
| Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close) | | Ano |  |
| Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti | | Ano |  |
| Podpora 802.1Q tagovaných rámců | | Ano |  |
| Podpora různých IPS politik pro různé typy provozu | | Ano |  |
| Inspekce pro IPv4 i IPv6 | | Ano |  |
| IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií | | Ano |  |
| Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací | | Ano |  |
| Možnost tvorby uživatelsky definovaných signatur IPS i Application bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele. | | Ano |  |
| IPS musí umět detekovat a blokovat útoky průzkumných aktivit | | Ano |  |
| IPS musí podporovat ochranu filtrů proti přetížení či DoS útoku na IPS | | Ano |  |
| IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C | | Ano |  |
| IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii | Ano | |  | |
| Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události | Ano | |  | |
| Funkce pro kontrolu DLP (např. s využitím techniky tzv. watermark, regulárních výrazů, dynamicky vytvářených signatur) | Ano | |  | |
| Různé senzory lze sdílet a aplikovat na různé politiky | Ano | |  | |
| IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků | Ano | |  | |
| Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“ | Ano | |  | |
| Podpora databází reputací adres v Internetu (Security Intelligence) | Ano | |  | |
| Funkce Next-Gen FW | | |  | |
| Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod. | Ano | |  | |
| Podpora pasivního monitorování (TAP režim) | Ano | |  | |
| Podpora 802.1Q tagovaných rámců | Ano | |  | |
| Podporovaných aplikací | Min. 3900 | |  | |
| Kategorie aplikací (nebezpečné, důležité, apod.) | Ano | |  | |
| URL kategorií | Min. 80 | |  | |
| Řízení přístupu k WWW - Web Usage Control (WCU) | Ano | |  | |
| Filtrace podle typů aplikací webových i ne-webových | Ano | |  | |
| SSL inspekce (dekrypce/enkrypce) | Ano | |  | |
| Security Inteligence database – známé uzly botnet sítí C&C | Ano | |  | |
| Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, apod. | Ano | |  | |
| Security Inteligence database – známé nebezpečné URL adresy a jmenné domény | Ano | |  | |
| Možnost integrovat vlastní reputační databáze | Ano | |  | |
| Filtry mohou zohlednit roli a identitu uživatele | Ano | |  | |
| Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow) | Ano | |  | |
| Řešení musí být schopné pasivního sběru informací o síťových zařízení a zobrazení: | Typ zařízení  Operační systém  Dodavatel OS  Použité síť. protokoly  Použité síť. služby  Otevřené porty síť. služeb  Potenciální zranitelnosti | |  |
| Přehled o síťových spojení má poskytovat minimálně tyto informace: | Čas startu a konce flow  Akce (allow, deny,..)  Důvod případného blokování  Zdroj. a cíl. adresa  Vstupní a výstupní zóna  Vstupní a výstupní rozhraní  Zdroj. a cíl. port  Aplikační protokol  IPS událost, pokud vznikne  Riziková úroveň IPS události  Použitá síťová aplikace  Rizikovost aplikace  „Business impact“ aplikace  Množství přenesených dat | |  |
| Správa | | |  |
| Vzdálená správa přes grafické rozhraní přístupné pomocí protokolu HTTPS, běžící přímo na firewallu, bez nutnosti instalace zvláštního SW | Ano | |  |
| Přístup ke GUI http/https protokolem | Ano | |  |
| Možnost vzdáleného přístupem protokolem ssh přímo do FW | Ano | |  |
| Možnost přístupu k textovým logům (syslog) přímo ve FW | Ano | |  |
| Možnost centrální správy při nasazení více firewallů | Ano | |  |
| Při centrální správě: možnost sdílených bezpečnostních politik | Ano | |  |
| Zobrazení logů a událostí v grafickém rozhraní správy | Ano | |  |
| Centrální dohledová konzole musí být schopna dohledovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod. | Ano | |  |
| Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole | Ano | |  |
| Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic | Ano | |  |
| Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu | Ano | |  |
| Pro reporty lze definovat template definující formát a obsah reportu | Ano | |  |
| Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu | Ano | |  |
| V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N | Ano | |  |
| Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů | Ano | |  |
| Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod. | Ano | |  |
| Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů. | Ano | |  |
| Podpora posílání událostí formou syslog, email, SNMP na externí platformy | Ano | |  |
| Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay | Ano | |  |
| Podpora řízeného přístupu podle rolí administrátorů | Ano | |  |
| Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora | Ano | |  |
| Možnost založit pro daný incident „ticket“ přímo v prostředí GUI managementu | Ano | |  |
| Workflow pro předávání „ticketů“ mezi administrátory | Ano | |  |
| Konkrétní bezpečnostní incident až na úrovni spojení lze přiložit k danému „tiketu“ pro další analýzu | Ano | |  |

Každý firewall bude obsahovat:

* + NGFW platforma ve formě HW appliance
  + Podpora virtualizace
  + Funkční integrace s core a access vrstvou sítě
  + 4 letá podpora výrobce v režimu 24x7

### 1x nový firewall vzdálené lokality

Jedná se o firewall v minimální konfiguraci:

|  |  |  |
| --- | --- | --- |
| Požadovaná funkcionalita/vlastnost | Požadované funkcionality /vlastnosti | Způsob splnění požadované funkcionality /vlastnosti |
| Formát zařízení | Appliance |  |
| Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených | 1 |  |
| Minimální počet 1Gb 10/100/1000 BaseT Ethernet | 8 |  |
| Podporovaný počet současně otevřených spojení stavový FW | Min.1 000 000 |  |
| Propustnost stavového firewallu | Min. 2,5 Gbps |  |
| VPN propustnost IPSec | Min. 1,8 Gbps |  |
| Současný počet VPN spojení IPSec | Min. 150 |  |
| Podpora L2 (transparentního) módu s podporou NAT a PAT | Ano |  |
| Podpora L3 (routovaného) módu s podporou NAT a PAT | Ano |  |
| Podporovaný počet VLAN | Min. 200 |  |
| Dynamické směrování - podpora alespoň RIP, OSPF, BGP | Ano |  |
| Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP | Ano |  |
| Podpora Policy based Routing | Ano |  |
| Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod. | Ano |  |
| Podpora filtrace IPv4, IPv6 | Ano |  |
| Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD | Ano |  |
| Podpora inspekce IPv6 provozu | Ano |  |
| Podpora NAT64 a DNS64 | Ano |  |
| Funkce QoS | Ano |  |
| Možnost rozšíření o funkce NextGen FW | Ano |  |
| Možnost rozšíření o funkce NextGen IPS | Ano |  |
| Možnost rozšíření o funkce URL filtrace | Ano |  |
| Možnost rozšíření o ochranu tzv. „Zero-day“ Anti-Malware | Ano |  |
| Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele | Ano |  |
| Firewall musí podporovat aplikační kontrolu a kategorizaci webových stránek jako svou nativní funkcionalitu; identifikace aplikací musí být prováděna napříč všemi porty/protokoly. | Ano |  |
| Konkrétní aplikace/kategorie aplikací a/nebo kategorie URL musí být nativní součástí vytváření standardního bezpečnostního pravidla. | Ano |  |
| Možnost tvorby firewall pravidla na základě minimálně těchto parametrů: zdrojová adresa, cílová adresa, uživatel/skupina, aplikace, kategorie webových stránek. | Ano |  |
| Podpora Policy based Routing (PBR musí být možné nakonfigurovat pomocí minimálně následujících metrik: protokol, interface, zdrojová adresa, cílová adresa, type of service) | Ano |  |
| Vzdálené správa přes grafické rozhraní přístupné pomocí protokolu HTTPS, běžící přímo na firewallu, bez nutnosti instalace zvláštního SW. | Ano |  |

Firewall bude obsahovat:

* + Možnost vytvoření site to site VPN do centrály
  + 4 letá podpora výrobce v režimu 24x7

### 2x Nový core switch

* Core prvky musí být plně integrované s firewall platformou poptávanou v tomto výběrovém řízení jak na funkční, tak na management úrovni
* touto integrací je myšleno zejména:
  + automatická nebo manuální autorizace switchů
  + předautorizace switchů na základě sériového čísla
  + jednotné management rozhraní, ze kterého lze spravovat switche i firewally
  + vizualizace logické i fyzické topologie celé infrastruktury až do úrovně koncové stanice/uživatele (firewally, switche, koncové stanice/uživatelé)
  + koncová zařízení musí být v jednotném management rozhraní graficky zobrazena včetně minimálně následujících informací: název zařízení, verze OS, MAC adresy síťových rozhraní, IP adresy, datum posledního připojení k síti, počet otevřených spojení, množství přenesených dat, počet paketů, aktuálně využitá šířka pásma, uživatelské jméno a detekované zranitelnosti pracovní stanice
  + možnost vyhledávání konkrétních zařízení nebo uživatel na základě minimálně následujících parametrů: IP adresa, MAC adres, uživatelské jméno
  + vyhledané zařízení musí být znázorněno v rámci vizualizace síťové topologie včetně všech výše uvedených informací
  + možnost manuálního nebo automatického vložení zařízení do karantény (samostatná VLAN) na základě bezpečnostního incidentu detekovaného na firewall platformě
  + vizualizace množství přenesených dat na jednotlivých portech (access i uplink porty). Možnost konfigurace časového intervalu tohoto zobrazení.
* Technické parametry:
  + 24x GE/10 GE SFP+ port
  + Servisní port 10/100/1000
  + Velikost 1 RU
  + podpora VLAN (802.1Q)
  + podpora QoS (802.1p)
  + podpora protokolů z rodiny spanning tree (STP, RSTP, 802.1D + 802.1w)
  + podpora LLDP (802.1ab)
  + podpora LACP (802.3ad)
  + IGMP snooping for multicast filtering
  + IEEE 802.1X
  + MAC Radius autentifikace
  + BDPU guard, Root guard
  + možnost karantény klientského zařízení na základě pokynu z nového firewallu
  + plná integrace s firewall řešením
  + neblokující architektura přepínacího subsystému

|  |  |  |
| --- | --- | --- |
| **Management and Configuration** |  |  |
| Auto Discovery of Multiple Switches | Ano |  |
| Software Upgrade of Switches | Ano |  |
| Centralized VLAN Configuration | Ano |  |
| Switch POE Control | Ano |  |
| Link Aggregation Configuration | Ano |  |
| Spanning Tree | Ano |  |
| **Security and Visibility** |  |  |
| 802.1x Authentication (Port-based, MAC-Based, MAB) | Ano |  |
| Syslog Collection | Ano |  |
| DHCP Snooping | Ano |  |
| Device Detection | Ano |  |
| **High Availability** |  |  |
| LAG support | Ano |  |
| Active-Active Split LAG | Ano |  |
| Multi-Chassis Link Aggregation (MCLAG) | Ano |  |
| **Layer 2** |  |  |
| Jumbo Frames | Ano |  |
| Auto-negotiation for port speed and duplex | Ano |  |
| IEEE 802.1D MAC Bridging/STP | Ano |  |
| IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) | Ano |  |
| IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) | Ano |  |
| STP Root Guard | Ano |  |
| Edge Port / Port Fast | Ano |  |
| IEEE 802.1Q VLAN Tagging | Ano |  |
| Private VLAN | Ano |  |
| IEEE 802.3ad Link Aggregation with LACP | Ano |  |
| Unicast/Multicast traffic balance over trunking port (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac) | Ano |  |
| IEEE 802.1AX Link Aggregation | Ano |  |
| Spanning Tree Instances (MSTP/CST) | 15/1 |  |
| IEEE 802.3x Flow Control and Back-pressure | Ano |  |
| IEEE 802.1Qbb Priority-based Flow Control | Ano |  |
| IEEE 802.3u 100Base-TX | Ne |  |
| IEEE 802.3z 1000Base-SX/LX | Ano |  |
| IEEE 802.3ab 1000Base-T | Ano |  |
| IEEE 802.3ae 10 Gigabit Ethernet | Ano |  |
| IEEE 802.3 CSMA/CD Access Method and Physical Layer Specifications | Ano |  |
| Storm Control | Ano |  |
| MAC, IP, Ethertype-based VLANs | Ano |  |
| Virtual-Wire | Ano |  |
| Split Port (QSFP+ breakout to 4xSFP+) | Ano |  |

|  |  |  |
| --- | --- | --- |
| **Security and Visibility** |  |  |
| Port Mirroring | Ano |  |
| Admin Authentication Via RFC 2865 RADIUS | Ano |  |
| IEEE 802.1x authentication Port-based | Ano |  |
| IEEE 802.1x Authentication MAC-based | Ano |  |
| IEEE 802.1x Guest and Fallback VLAN | Ano |  |
| IEEE 802.1x MAC Access Bypass (MAB) | Ano |  |
| IEEE 802.1x Dynamic VLAN Assignment | Ano |  |
| MAC-IP Binding | Ano |  |
| sFlow | Ano |  |
| ACL | Ano, 2K entries |  |
| IEEE 802.1ab Link Layer Discovery Protocol (LLDP) | Ano |  |
| IEEE 802.1ab LLDP-MED | Ano |  |
| DHCP-Snooping | Ano |  |
| Dynamic ARP Inspection | Ano |  |
| Sticky MAC | Ano |  |
| **Quality of Service** |  |  |
| IEEE 802.1p Based Priority Queuing | Ano |  |
| IP TOS/DSCP Based Priority Queuing | Ano |  |
| **Management** |  |  |
| IPv4 and IPv6 Management | Ano |  |
| Telnet / SSH | Ano |  |
| HTTP / HTTPS | Ano |  |
| SNMP v1/v2c/v3 | Ano |  |
| SNTP | Ano |  |
| Standard CLI and web GUI interface | Ano |  |
| Software download/upload: TFTP/FTP/GUI | Ano |  |
| Support for HTTP REST APIs for Configuration and Monitoring | Ano |  |
| **Additional RFC and MIB Support** |  |  |
| RFC 2571 Architecture for Describing SNMP Framework | Ano |  |
| DHCP Client | Ano |  |
| RFC 854 Telnet Server | Ano |  |
| RFC 2865 RADIUS | Ano |  |
| RFC 1643 Ethernet-like Interface MIB | Ano |  |
| RFC 1213 MIB-II | Ano |  |
| RFC 1354 IP Forwarding Table MIB | Ano |  |
| RFC 2572 SNMP Message Processing and Dispatching | Ano |  |
| RFC 1573 SNMP MIB II | Ano |  |
| RFC 1157 SNMPv1/v2c | Ano |  |
| RFC 2030 SNTP | Ano |  |

|  |  |  |
| --- | --- | --- |
| **Hardware Specifications** |  |  |
| Total Network Interfaces (Proposed) | min 24x GE/10 GE SFP+ ports |  |
| 10/100/1000 Service Ports | 1 |  |
| RJ-45 Serial Console Port | 1 |  |
| Form Factor | 1 RU Rack-Mount Appliance |  |
| **System Specifications** |  |  |
| Switching Capacity (Duplex) | 480 Gbps |  |
| Packets Per Second (Duplex) | 714 Mpps |  |
| Mac Address Storage | 128 K |  |
| Network Latency | < 800ns |  |
| VLANs Supported | 4 K |  |
| IPv4/IPv6 Dual Stack Routing Ready Hardware | Yes |  |
| Link Aggregation Group Size | Up to 24 |  |
| Queues/Port | 8 |  |
| Packet Buffers | 9 MB |  |

* + 4 letá podpora výrobce v režimu 24x7

### Nové přístupové switche

* Specifikace všech přístupových switchů (Typ 1, Typ 2, Typ 3, Typ 4, Typ 5)
* Přístupové switche musí být plně integrované s firewall platformou poptávanou v tomto výběrovém řízení jak na funkční, tak na management úrovni
* touto integrací je myšleno zejména:
  + automatická nebo manuální autorizace switchů
  + předautorizace switchů na základě sériového čísla
  + jednotné management rozhraní, ze kterého lze spravovat switche i firewally
  + vizualizace logické i fyzické topologie celé infrastruktury až do úrovně koncové stanice/uživatele (firewally, switche, koncové stanice/uživatelé)
  + koncová zařízení musí být v jednotném management rozhraní graficky zobrazena včetně minimálně následujících informací: název zařízení, verze OS, MAC adresy síťových rozhraní, IP adresy, datum posledního připojení k síti, počet otevřených spojení, množství přenesených dat, počet paketů, aktuálně využitá šířka pásma, uživatelské jméno a detekované zranitelnosti pracovní stanice
  + možnost vyhledávání konkrétních zařízení nebo uživatel na základě minimálně následujících parametrů: IP adresa, MAC adres, uživatelské jméno
  + vyhledané zařízení musí být znázorněno v rámci vizualizace síťové topologie včetně všech výše uvedených informací
  + možnost manuálního nebo automatického vložení zařízení do karantény (samostatná VLAN) na základě bezpečnostního incidentu detekovaného na firewall platformě
  + vizualizace množství přenesených dat na jednotlivých portech (access i uplink porty). Možnost konfigurace časového intervalu tohoto zobrazení.
* Technické parametry:
  + Počty a typy portů jsou specifikovány v kapitole Předmět zakázky
  + Servisní port
  + Velikost 1 RU
  + podpora VLAN (802.1Q)
  + podpora QoS (802.1p)
  + podpora protokolů z rodiny spanning tree (STP, RSTP, 802.1D + 802.1w)
  + podpora LLDP (802.1ab)
  + podpora LACP (802.3ad)
  + IGMP snooping for multicast filtering
  + IEEE 802.1X
  + MAC Radius autentifikace
  + BDPU guard, Root guard
  + možnost karantény klientského zařízení na základě pokynu z firewallu
  + Plná integrace s firewall řešením
  + Neblokující architektura přepínacího subsystému

### Společné parametry pro centrální správu switche TYP 1 / TYP2 / TYP4

|  |  |  |
| --- | --- | --- |
| **Management and Configuration** |  |  |
| Auto Discovery of Multiple Switches | Ano |  |
| Software Upgrade of Switches | Ano |  |
| Centralized VLAN Configuration | Ano |  |
| Switch POE Control | Ano |  |
| Link Aggregation Configuration | Ano |  |
| Spanning Tree | Ano |  |
| **Security and Visibility** |  |  |
| 802.1x Authentication (Port-based, MAC-based, MAB) | Ano |  |
| Syslog Collection | Ano |  |
| DHCP Snooping | Ano |  |
| Device Detection | Ano |  |
| **High Availability** |  |  |
| LAG support | Ano |  |
| Active-Active Split LAG | Ano |  |
| Multi-Chassis Link Aggregation (MCLAG) | Ano |  |
| **Layer 2** |  |  |
| Jumbo Frames | Ano |  |
| Auto-negotiation for Port Speed and Duplex | Ano |  |
| IEEE 802.1D MAC Bridging/STP | Ano |  |
| IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) | Ano |  |
| IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) | Ano |  |
| STP Root Guard | Ano |  |
| STP BPDU Guard | Ano |  |
| Edge Port / Port Fast | Ano |  |
| IEEE 802.1Q VLAN Tagging | Ano |  |
| Private VLAN | Ano |  |
| IEEE 802.3ad Link Aggregation with LACP | Ano |  |
| Unicast/Multicast traffic balance over trunking port (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac) | Ano |  |
| IEEE 802.1AX Link Aggregation | Ano |  |
| Spanning Tree Instances (MSTP/CST) | 15/1 |  |
| IEEE 802.3x Flow Control and Back-pressure | Ano |  |
| IEEE 802.3 10Base-T | Ano |  |
| IEEE 802.3u 100Base-TX | Ano |  |
| IEEE 802.3z 1000Base-SX/LX | Ano |  |
| IEEE 802.3ab 1000Base-T | Ano |  |
| IEEE 802.3ae 10 Gigabit Ethernet | Ano |  |
| IEEE 802.3 CSMA/CD Access Method and Physical Layer Specifications | Ano |  |
| Storm Control | Ano |  |
| MAC, IP, Ethertype-based VLANs | Ano |  |
| Virtual-Wire | Ano |  |
| Time-Domain Reflectcometry (TDR) Support | Ano |  |
| **Security and Visibility** |  |  |
| Port Mirroring | Ano |  |
| Admin Authentication Via RFC 2865 RADIUS | Ano |  |
| IEEE 802.1x authentication Port-based | Ano |  |
| IEEE 802.1x Authentication MAC-based | Ano |  |
| IEEE 802.1x Guest and Fallback VLAN | Ano |  |
| IEEE 802.1x MAC Access Bypass (MAB) | Ano |  |
| IEEE 802.1x Dynamic VLAN Assignment | Ano |  |
| Radius CoA (Change of Authority) | Ano |  |
| Radius Accounting | Ano |  |
| sFlow | Ano |  |
| IEEE 802.1ab Link Layer Discovery Protocol (LLDP) | Ano |  |
| IEEE 802.1ab LLDP-MED | Ano |  |
| DHCP-Snooping | Ano |  |
| Dynamic ARP Inspection | Ano |  |
| Sticky MAC and MAC Limit | Ano |  |
| **Quality of Service** |  |  |
| IEEE 802.1p Based Priority Queuing | Ano |  |
| IP TOS/DSCP Based Priority Queuing | Ano |  |
| **Management** |  |  |
| IPv4 and IPv6 Management | Ano |  |
| Telnet / SSH | Ano |  |
| HTTP / HTTPS | Ano |  |
| SNMP v1/v2c/v3 | Ano |  |
| SNTP | Ano |  |
| Standard CLI and Web GUI Interface | Ano |  |
| Software download/upload: TFTP/FTP/GUI | Ano |  |
| Support for HTTP REST APIs for Configuration and Monitoring | Ano |  |
| **Additional RFC and MIB Support** |  |  |
| RFC 2571 Architecture for Describing SNMP | Ano |  |
| DHCP Client | Ano |  |
| RFC 854 Telnet Server | Ano |  |
| RFC 2865 RADIUS | Ano |  |
| RFC 1643 Ethernet-like Interface MIB | Ano |  |
| RFC 1213 MIB-II | Ano |  |
| RFC 1354 IP Forwarding Table MIB | Ano |  |
| RFC 2572 SNMP Message Processing and Dispatching | Ano |  |
| RFC 1573 SNMP MIB II | Ano |  |
| RFC 1157 SNMPv1/v2c | Ano |  |
| RFC 2030 SNTP | Ano |  |

### Specifikace TYP 1

|  |  |  |
| --- | --- | --- |
| **Hardware Specifications** |  |  |
| Total Network Interfaces | min 48x GE POE RJ45 and 4x10 GE SFP+ ports / SFP+ ports are compatlble with 1 GE SFP |  |
| Dedicated Management 10/100 Port | 1 |  |
| RJ-45 Serial Console Port | 1 |  |
| Form Factor | 1 RU Rack Mount |  |
| Power over Ethernet (PoE) Ports | 48 (802.3af/at) |  |
| PoE Power Budget | 370 W |  |
| Mean Time Between Failures | > 10 years |  |
| **System Specifications** |  |  |
| Switching Capacity (Duplex) | 176 Gbps |  |
| Packets Per Second (Duplex) | 262 Mpps |  |
| MAC Address Storage | 16 K |  |
| Network Latency | < 1µs |  |
| VLANs Supported | 4 K |  |
| Link Aggregation Group Size | 8 |  |
| Packet Buffers | 1.5 MB |  |

* + 4 letá podpora výrobce v režimu 24x7

### Specifikace TYP 2

|  |  |  |
| --- | --- | --- |
| **Hardware Specifications** |  |  |
| Total Network Interfaces | 24x GE POE RJ45 and 2x10 GE SFP+ ports / SFP+ ports are compatlble with 1 GE SFP |  |
| Dedicated Management 10/100 Port | 1 |  |
| RJ-45 Serial Console Port | 1 |  |
| Form Factor | 1 RU Rack Mount |  |
| Power over Ethernet (PoE) Ports | 24 (802.3af/at) |  |
| PoE Power Budget | 185 W |  |
| Mean Time Between Failures | > 10 years |  |
| **System Specifications** |  |  |
| Switching Capacity (Duplex) | 88 Gbps |  |
| Packets Per Second (Duplex) | 131 Mpps |  |
| MAC Address Storage | 16 K |  |
| Network Latency | < 1µs |  |
| VLANs Supported | 4 K |  |
| Link Aggregation Group Size | 8 |  |
| Packet Buffers | 1.5 MB |  |

* + 4 letá podpora výrobce v režimu 24x7

### Specifikace TYP 4

|  |  |  |
| --- | --- | --- |
| **Hardware Specifications** |  |  |
| Total Network Interfaces | 48x GE RJ45 and 4x10 GE SFP+ ports / SFP+ ports are compatlble with 1 GE SFP |  |
| Dedicated Management 10/100 Port | 1 |  |
| RJ-45 Serial Console Port | 1 |  |
| Form Factor | 1 RU Rack Mount |  |
| Power over Ethernet (PoE) Ports | — |  |
| PoE Power Budget | N/A |  |
| Mean Time Between Failures | > 10 years |  |
| **System Specifications** |  |  |
| Switching Capacity (Duplex) | 176 Gbps |  |
| Packets Per Second (Duplex) | 262 Mpps |  |
| MAC Address Storage | 16 K |  |
| Network Latency | < 1µs |  |
| VLANs Supported | 4 K |  |
| Link Aggregation Group Size | 8 |  |
| Packet Buffers | 1.5 MB |  |

* + 4 letá podpora výrobce v režimu 24x7

### Parametry pro Switch TYP 3

|  |  |  |
| --- | --- | --- |
| **Management and Configuration** |  |  |
| Auto Discovery of Multiple Switches | Ano |  |
| Software Upgrade of Switches | Ano |  |
| Centralized VLAN Configuration | Ano |  |
| Switch POE Control | Ano |  |
| Link Aggregation Configuration | Ano |  |
| Spanning Tree | Ano |  |
| **Security and Visibility** |  |  |
| 802.1x Authentication (Port-based, MAC-based, MAB) | Ano |  |
| Syslog Collection | Ano |  |
| DHCP Snooping | Ano |  |
| Device Detection | Ano |  |
| **High Availability** |  |  |
| LAG support | Ano |  |
| Active-Active Split LAG | NE |  |
| **Layer 2** |  |  |
| Jumbo Frames | Ano |  |
| Auto-negotiation for Port Speed and Duplex | Ano |  |
| IEEE 802.1D MAC Bridging/STP | Ano |  |
| IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) | Ano |  |
| IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) | Ano |  |
| STP Root Guard | Ano |  |
| STP BPDU Guard | Ano |  |
| Edge Port / Port Fast | Ano |  |
| IEEE 802.1Q VLAN Tagging | Ano |  |
| Private VLAN | NE |  |
| IEEE 802.3ad Link Aggregation with LACP | Ano |  |
| Unicast/Multicast traffic balance over trunking port (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac) | Ano |  |
| IEEE 802.1AX Link Aggregation | Ano |  |
| Spanning Tree Instances (MSTP/CST) | 15/1 |  |
| IEEE 802.3x Flow Control and Back-pressure | Ano |  |
| IEEE 802.3 10Base-T | Ano |  |
| IEEE 802.3u 100Base-TX | Ano |  |
| IEEE 802.3z 1000Base-SX/LX | Ano |  |
| IEEE 802.3ab 1000Base-T | Ano |  |
| IEEE 802.3 CSMA/CD Access Method and Physical Layer Specifications | Ano |  |
| Storm Control | Ano |  |
| MAC, IP, Ethertype-based VLANs | Ano |  |
| Virtual-Wire | NE |  |
| Time-Domain Reflectcometry (TDR) Support | NE |  |
| **Security and Visibility** |  |  |
| Port Mirroring | Ano |  |
| Admin Authentication Via RFC 2865 RADIUS | Ano |  |
| IEEE 802.1x authentication Port-based | Ano |  |
| IEEE 802.1x Authentication MAC-based | Ano |  |
| IEEE 802.1x Guest and Fallback VLAN | Ano |  |
| IEEE 802.1x MAC Access Bypass (MAB) | Ano |  |
| IEEE 802.1x Dynamic VLAN Assignment | Ano |  |
| Radius CoA (Change of Authority) | NE |  |
| Radius Accounting | NE |  |
| sFlow | NE |  |
| IEEE 802.1ab Link Layer Discovery Protocol (LLDP) | Ano |  |
| IEEE 802.1ab LLDP-MED | Ano |  |
| DHCP-Snooping | Ano |  |
| Dynamic ARP Inspection | NE |  |
| **Management** |  |  |
| IPv4 and IPv6 Management | Ano |  |
| Telnet / SSH | Ano |  |
| HTTP / HTTPS | Ano |  |
| SNMP v1/v2c/v3 | Ano |  |
| SNTP | Ano |  |
| Standard CLI and Web GUI Interface | Ano |  |
| Software download/upload: TFTP/FTP/GUI | Ano |  |
| Support for HTTP REST APIs for Configuration and Monitoring | Ano |  |
| **Additional RFC and MIB Support** |  |  |
| RFC 2571 Architecture for Describing SNMP | Ano |  |
| DHCP Client | Ano |  |
| RFC 854 Telnet Server | Ano |  |
| RFC 2865 RADIUS | Ano |  |
| RFC 1643 Ethernet-like Interface MIB | Ano |  |
| RFC 1213 MIB-II | Ano |  |
| RFC 1354 IP Forwarding Table MIB | Ano |  |
| RFC 2572 SNMP Message Processing and Dispatching | Ano |  |
| RFC 1573 SNMP MIB II | Ano |  |
| RFC 1157 SNMPv1/v2c | Ano |  |
| RFC 2030 SNTP | Ano |  |
| Hardware Specifications |  |  |
| Total Network Interfaces | Min 8x GE POE RJ45 and 2x GE SFP |  |
| Dedicated Management 10/100 Port | 0 |  |
| RJ-45 Serial Console Port | 1 |  |
| Form Factor | 1 RU Rack Mount |  |
| Power over Ethernet (PoE) Ports | 4 (802.3af/at) |  |
| PoE Power Budget | 65 W |  |
| Mean Time Between Failures | > 10 years |  |
| System Specifications |  |  |
| Switching Capacity (Duplex) | 20 Gbps |  |
| Packets Per Second (Duplex) | 30 Mpps |  |
| MAC Address Storage | 8 K |  |
| Network Latency | 4µs |  |
| VLANs Supported | 4 K |  |
| Link Aggregation Group Size | 8 |  |
| Total Link Aggregation Groups | 8 |  |
| Packet Buffers | 512 KB |  |

* + 4 letá podpora výrobce v režimu 24x7

### Parametry pro Switch TYP 5

|  |  |  |
| --- | --- | --- |
| **Management and Configuration** |  |  |
| Auto Discovery of Multiple Switches | Ano |  |
| Software Upgrade of Switches | Ano |  |
| Centralized VLAN Configuration | Ano |  |
| Switch POE Control | Ano |  |
| Link Aggregation Configuration | Ano |  |
| Spanning Tree | Ano |  |
| **Security and Visibility** |  |  |
| 802.1x Authentication (Port-based, MAC-based, MAB) | Ano |  |
| Syslog Collection | Ano |  |
| DHCP Snooping | Ano |  |
| Device Detection | Ano |  |
| **High Availability** |  |  |
| LAG support | Ano |  |
| Active-Active Split LAG | Ano |  |
| Multi-Chassis Link Aggregation (MCLAG) | Ne |  |
| **Layer 2** |  |  |
| Jumbo Frames | Ano |  |
| Auto-negotiation for Port Speed and Duplex | Ano |  |
| IEEE 802.1D MAC Bridging/STP | Ano |  |
| IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) | Ano |  |
| IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) | Ano |  |
| STP Root Guard | Ano |  |
| STP BPDU Guard | Ano |  |
| Edge Port / Port Fast | Ano |  |
| IEEE 802.1Q VLAN Tagging | Ano |  |
| Private VLAN | Ano |  |
| IEEE 802.3ad Link Aggregation with LACP | Ano |  |
| Unicast/Multicast traffic balance over trunking port (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac) | Ano |  |
| IEEE 802.1AX Link Aggregation | Ano |  |
| Spanning Tree Instances (MSTP/CST) | 15/1 |  |
| IEEE 802.3x Flow Control and Back-pressure | Ano |  |
| IEEE 802.3 10Base-T | Ano |  |
| IEEE 802.3u 100Base-TX | Ano |  |
| IEEE 802.3z 1000Base-SX/LX | Ano |  |
| IEEE 802.3ab 1000Base-T | Ano |  |
| IEEE 802.3 CSMA/CD Access Method and Physical Layer Specifications | Ano |  |
| Storm Control | Ano |  |
| MAC, IP, Ethertype-based VLANs | Ano |  |
| Virtual-Wire | Ano |  |
| Time-Domain Reflectcometry (TDR) Support | Ano |  |
| **Security and Visibility** |  |  |
| Port Mirroring | Ano |  |
| Admin Authentication Via RFC 2865 RADIUS | Ano |  |
| IEEE 802.1x authentication Port-based | Ano |  |
| IEEE 802.1x Authentication MAC-based | Ano |  |
| IEEE 802.1x Guest and Fallback VLAN | Ano |  |
| IEEE 802.1x MAC Access Bypass (MAB) | Ano |  |
| IEEE 802.1x Dynamic VLAN Assignment | Ano |  |
| Radius CoA (Change of Authority) | Ano |  |
| Radius Accounting | Ano |  |
| sFlow | Ano |  |
| IEEE 802.1ab Link Layer Discovery Protocol (LLDP) | Ano |  |
| IEEE 802.1ab LLDP-MED | Ano |  |
| DHCP-Snooping | Ano |  |
| Dynamic ARP Inspection | Ano |  |
| **Management** |  |  |
| IPv4 and IPv6 Management | Ano |  |
| Telnet / SSH | Ano |  |
| HTTP / HTTPS | Ano |  |
| SNMP v1/v2c/v3 | Ano |  |
| SNTP | Ano |  |
| Standard CLI and Web GUI Interface | Ano |  |
| Software download/upload: TFTP/FTP/GUI | Ano |  |
| Support for HTTP REST APIs for Configuration and Monitoring | Ano |  |
| **Additional RFC and MIB Support** |  |  |
| RFC 2571 Architecture for Describing SNMP | Ano |  |
| DHCP Client | Ano |  |
| RFC 854 Telnet Server | Ano |  |
| RFC 2865 RADIUS | Ano |  |
| RFC 1643 Ethernet-like Interface MIB | Ano |  |
| RFC 1213 MIB-II | Ano |  |
| RFC 1354 IP Forwarding Table MIB | Ano |  |
| RFC 2572 SNMP Message Processing and Dispatching | Ano |  |
| RFC 1573 SNMP MIB II | Ano |  |
| RFC 1157 SNMPv1/v2c | Ano |  |
| RFC 2030 SNTP | Ano |  |
| Hardware Specifications |  |  |
| Total Network Interfaces | Min 24x GE RJ45 ports and 4x GE SFP ports |  |
| Dedicated Management 10/100 Port | 1 |  |
| RJ-45 Serial Console Port | 1 |  |
| Form Factor | 1 RU Rack Mount |  |
| Power over Ethernet (PoE) Ports | 12 (802.3af/802.3at) |  |
| PoE Power Budget | 180 W |  |
| Mean Time Between Failures | > 10 years |  |
| System Specifications |  |  |
| Switching Capacity (Duplex) | 56 Gbps |  |
| Packets Per Second (Duplex) | 83 Mpps |  |
| MAC Address Storage | 16 K |  |
| Network Latency | < 1µs |  |
| VLANs Supported | 4 K |  |
| Link Aggregation Group Size | 8 |  |
| Total Link Aggregation Groups | Do počtu portů |  |
| Packet Buffers | 1,5 MB |  |

* + 4 letá podpora výrobce v režimu 24x7

### Systém pro ukládání a korelaci logů

Je poptáván systém pro ukládání a korelaci logů v síti zadavatele. Systém musí být plně kompatibilní s dodávanými zařízeními, musí podporovat analýzu logů nad provozem. Dále musí být schopné poskytovat reporty nad logy a informovat správce systému o hrozbách, které byly v síti odhaleny.

Hlavní parametry appliance:

* požadujeme virtuální appliance s podporou VMware, KVM a Hyper-V
* Kapacita úložiště logů minimálně 3TB a minimální limit pro množství přijatých logů za jeden den 6GB
* Podpora minimálně 4 virtuálních síťových rozhraní
* Možnost škálovatelného navýšení kapacity úložiště na základě licence

Logovací a reportovací funkce

* Musí se jednat o centrální logovací prvek pro všechny UTM firewally
* Možnost dostat se z vizuálního zobrazení proklikem na konkrétní logy
* Realtime a historický náhled do logů
* Korelace logů
* Samostatná sekce týkající se hrozeb v síti
* Podpora prohlížení statistických údajů nad logy
* Podpora tvorby reportů ve formátu HTML/CSV/XML/PDF
* Generování reportů v pravidelných intervalech
* Předdefinované vzory pro reporty na nejčastější použití
* Možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze
* Možnost úpravy reportů do vlastního designu – vlastní loga, texty, úprava hlavičky

Možnosti správy a komunikace

* Správa přes webové rozhraní HTTPS
* Podpora SNMPv2, SNMPv3
* Podpora REST API
* Administrátorské účty musí být možné konfigurovat lokálně nebo na vzdáleném serveru (LDAP, RADIUS, Tacacs+)
* Podpora šifrované komunikace mezi zdroji logů a log serverem

Dodávka systému pro ukládání a korelaci logů plně kompatibilní s dodávanými zařízeními (switche, firewall)

* + 4 letá podpora výrobce v režimu 24x7

## Instalace, konfigurace, zaškolení obsluhy, dokumentace skutečného provedení

Součástí dodávky jsou implementační práce spojené s implementací a nasazením poptávaného řešení

Dodávka obsahuje:

* + Instalace do racku v sídle zadavatele,
  + základní nastavení systémů a jejich konfigurace tak, aby mohl pracovat v prostředí zadavatele,
  + poskytnutí součinnosti při konfiguraci systémů zadavatele,
  + ověření funkčních a výkonových parametrů nabízeného řešení,
  + zaškolení obsluhy,
  + dokumentace skutečného provedení v českém jazyce.

Celkový objem instalační prací v rozsahu 18 MD.

**Zadavatel si vyhrazuje možnost vyzvat účastníka k ověření vybraných technických parametrů formou bezplatné prezentace nabízeného řešení v prostředí zadavatele před uzavřením smlouvy.**

Účastník je povinen zajistit prezentaci nabízeného řešení na minimálně 14 kalendářních dnů a nejdéle do 10 kalendářních dnů od doručení výzvy zadavatelem. Testování bude provádět dodavatel za účasti zástupců zadavatele, který mu poskytne potřebnou součinnost. Testy budou provedeny v prostředí zadavatele. Po ukončení testování bude zápůjčka účastníkovi vrácena (účastník si vyzvedne zápůjčku na vlastní náklady v místě plnění).

V případě, že nabízené řešení neprojde úspěšným otestováním, může být nabídka vyloučena z výběrového řízení z důvodu nesplnění povinných požadavků pro účast ve výběrovém řízení.

# Požadavky na uchazeče – Kvalifikační požadavky

## Potvrzení dodavatele od výrobce

Zadavatel dále vyžaduje, aby dodavatel prokázal doložením kopie potvrzení přímo od výrobce navrhovaného řešení, že pro tuto konkrétní veřejnou zakázku a daného dodavatele:

* je dodavatel oprávněn dodat navrhované řešení a je certifikovaným partnerem výrobce
* je dodavatel oprávněn provádět instalační, implementační a konzultační služby na dodané zařízení
* se jedná o zcela nové zařízení, které je určené pro užívání a provoz v ČR.

Součástí nabídky bude Čestné prohlášení předkladatele nabídky, že navržené HW řešení, tj. switche, firewally, management jsou od jednoho výrobce a jsou kompatibilní, případně požadujeme prohlášení všech výrobců, o vzájemné kompatibilitě jednotlivých prvků uchazečem nabízené konfigurace.

## Realizační tým dodavatele

Dodavatel doloží platnými certifikáty nebo čestným prohlášením pro toto výběrové řízení, že v posledních 3 letech prováděl alespoň jednu obdobnou zakázku v celkové hodnotě minimálně 500.000 Kč bez DPH, a to včetně krátkého popisu řešení. Popis bude mít formu čestného prohlášení a bude zde uveden objednatel, předmět zakázky, cena uchazečem realizované dodávky, doba plnění a kontaktní osoba objednatele včetně telefonického, e-mailového nebo korespondenčního spojení na osobu, u které lze tuto referenci ověřit. Obdobnou zakázkou se rozumí zakázka na dodávku řešení a služeb odpovídající předmětu VZ, jakou uchazeč předkládá ve své nabídce.

## Pojištění dodavatele

Uchazeč předloží v prosté kopii pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou zákazníkovi a čestné prohlášení, že pojištění bude platné po celou dobu realizace zakázky. Pojistné plnění musí být minimálně 5 000 000,- Kč.

Veškerá čestná prohlášení uchazeče musí být podepsána osobou oprávněnou jednat jménem či za uchazeče.

Těmito požadavky se snažíme maximálně eliminovat možnost nevhodně provedené konfigurace, popřípadě poškození, či ztráty dat.