**PŘÍLOHA č. 4 – TECHNICKÁ SPECIFIKACE**

**Popis současného stavu**:

Zadavatel provozuje současnou páteřní vrstvu LAN sítě na dvojici L3 přepínačů řady Cisco 6500, spojených do jednoho logického celku technologií VSS. Tyto prvky zabezpečují redundantní připojení pro zbytek LAN a ostatních technologických celků sítě ČRo. Zároveň je k těmto prvkům připojena serverová část. Servery a management prvky sítě jsou do páteřních prvků přímo redundantně připojeny.

## **Cílový stav**

Zadavatel požaduje obměnu stávajících přepínačů Cisco Catalyst 6509 novým hardwarem tak, aby byla oddělena část pro připojení serverových technologií (DC část) a část pro připojení přístupových přepínačů, připojení do WAN a internetu (LAN část).



## **Obměna páteřních přepínačů LAN**

Zadavatel požaduje provést výměnu dvou páteřních přepínačů Cisco 6509 formou obměny, s požadavky na funkcionalitu a vybavenost, uvedenými v tabulce níže. Zadavatel požaduje dodání celkem dvou nových L3 přepínačů, které budou sloučeny do jednoho logického přepínače tak, aby se chovaly jako jedna síťová entita z pohledu L2 i L3 protokolů. V rámci obměny je požadováno přepojení všech aktivních prvků a zařízení přímo připojených ke stávajícím páteřním přepínačům.

Zadavatel požaduje dodání nových transceiverů pro připojení některých přístupových přepínačů. Ke každému přepínači bude dodáno 21 transceiverů 10GBaseLRM, jeden transceiver 10GBaseLR a tři transceivery 1000BaseT. Zbylé aktivní prvky budou připojeny použitím stávajících optických transceiverů, které jsou již používány ve stávajících přepínačích.

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Poznámka\*** |
| **HW specifikace** | |
| Typ hardwarového přepínače - L3 přepínač |  |
| Formát přepínače - modulární |  |
| Velikost přepínače maximálně (RU) - 5 |  |
| Minimální počet slotů v šasi - 4 |  |
| Celková minimální propustnost přepínacího subsystému – 2 Tb/s |  |
| Minimální kapacita interní sběrnice na 1 slot přepínače – 220 Gb/s |  |
| Minimální počet záznamů v MAC adresní tabulce – 128 000 |  |
| Minimální počet záznamů ve směrovací tabulce - IPv4 unicast – 256 000 |  |
| Minimální počet záznamů ve směrovací tabulce – IPv6 unicast – 128 000 |  |
| Minimální počet aktivních VLAN – 4 000 |  |
| Řídící modul s integrovanými rozhraními 10GE |  |
| Napájecí zdroj, max. dosažitelný výkon – alespoň 2 500W |  |
| Interní redundantní napájecí zdroj, max, dosažitelný výkon – alespoň 2 500W |  |
| Minimální počet 10GE portů s volitelným fyzickým rozhraním s lokálním přepínáním - 48 |  |
| Standard 802.1ae na 10Gbit/s portech s volitelným fyzickým rozhraním |  |
| Osazení 10GE transceivery – 21 x 10GBase-LRM, 1 x 10GBase-LR |  |
| Osazení 1GE transceivery – 3 x 1000BaseT |  |
| **Funkční specifikace** | |
| Virtualizace – možnost sloučit alespoň dvě fyzická šasi do jednoho logického celku – virtuálního šasi (jediná entita z pohledu L2 i L3 protokolů) |  |
| Ochranné mechanismy rozpadnutí virtuálního šasi bez nutnosti využití dodatečných zařízení |  |
| Stavové přepnutí mezi řídícími moduly v logickém šasi (ekvivalent funkce StatefullSwitchover/SSO mezi fyzickými šasi) |  |
| Směrování protokolů IPv4 a IPv6 v hardware (duální podpora IPv4 a IPv6, tedy možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, *dual‑stack*) |  |
| HW podpora MPLS a VPLS |  |
| Tunelovací protokoly (např. GRE) v hardware |  |
| Překlad adres/NAT v hardware |  |
| IEEE 802.3ad |  |
| IEEE 802.3ad přes více modulů |  |
| IEEE 802.3ad přes více šasi (funkční ekvivalent MultichassisEtherchannel) |  |
| IEEE 802.1Q |  |
| IEEE 802.1ak |  |
| tunelování 802.1Q v 802.1Q |  |
| IEEE 802.1s - Multiple Spanning Trees |  |
| IEEE 802.1w - Rapid SpanningTreeProtocol |  |
| IEEE 802.1p |  |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) |  |
| Hardwarová podpora dlouhých ethernetových rámců, tzv. „jumbo frames“ |  |
| Detekce jednosměrnosti optické linky (např. UDLD) |  |
| QoS classification – dle ACL, IP Prec, DSCP, CoS |  |
| QoS marking –dle IP Prec, DSCP, CoS |  |
| QoS olicing |  |
| Policing i na hodnotu agregovanou ze všech karet s lokálním přepínáním |  |
| Policing per-flow (např. microflowpolicing nebo funkčně ekvivalentní) |  |
| Konfigurovatelné HW prostředky ochrany CPU před útoky typu DoS |  |
| Hardwarová filtrace (access list) na fyzickém i logickém L2 i L3 rozhraní |  |
| Hardwarová filtrace (access list) dle L2, L3 i L4 informací |  |
| Provádění dílčích změn v access listu nemá vliv na filtraci datových toků nezměněnou částí access listu |  |
| Hardwarová filtrace (access list) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám síťových prostředků (např. SGACL, role-based ACL nebo funkčně ekvivalentní) |  |
| Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group TageXchangeProtocol dle RFC draft-smith-kandula-sxp-05 nebo funkčně ekvivalentní). |  |
| Propagace bezpečnostní role uživatele nebo koncového zařízení pro každý datový rámec (např. Security Group Tagging nebo funkčně ekvivalentní) |  |
| Zabezpečení a analýza DHCP protokolu (např. DHCP snoopingu nebo funkčně ekvivalentní) |  |
| Ochrana ARP protokolu (např. Dynamic ARP Inspection, DAI nebo funkčně ekvivalentní) |  |
| Ochrana podvrženého mapování IP/MAC adresy (např. IP Source Guard/IPSG nebo funkčně ekvivalentní) |  |
| MPLS směrování |  |
| VPLS směrování |  |
| BGPv4, MP-BGP |  |
| OSPFv2, OSPFv3 |  |
| OSPF s MD5 a NSSA |  |
| RIPv2, RIPng |  |
| IS-IS pro IPv4 a IPv6 |  |
| Router Redundancy protokol pro IPv4 (např. VRRP, HSRP) |  |
| Policy-based routing podle ACL |  |
| PIM-SM (Protocol Independent Multicast, sparse mód) |  |
| PIM SSM (PIM Source SpecificMulticast) |  |
| BidirectionalProtocol Independent Multicast (RFC 5015) |  |
| IGMPv2, IGMPv3 |  |
| Antispoofingová kontrola ekvivalentní funkci RPFC, *reverse pathforwardingcheck* dle RFC3704 a RFC3178 pro IPv4 i IPv6 |  |
| Směrování dle škálovatelné adresace (např. Locator/IdentifierSeparationProtocol (LISP) dle RFC 6830) |  |
| IPv6 services (HTTP, DNS, SSH, ACL, ICMP, DHCP) |  |
| Router Redundancy protokol pro IPv6 (např. VRRP, HSRP) |  |
| IPv6 First Hop Security (IPv6 Port ACL, RA guard, Secure Neighbor Discovery) |  |
| IPv6 Multicast (MLDv1 & v2, PIM SSM, PIM SM) |  |
| IPv6 over GRE v hardware |  |
| ISATAP v hardware |  |
| IPv6 QoS |  |
| Vytváření logicky oddělených instancí virtuálních směrovacích tabulek v rámci téhož L3 přepínače/směrovače pro tvorbu VPN (podpora virtualizace směrovacích tabulek - např. funkční ekvivalent Virtual Routing and Forwarding/Multi‑VRF) |  |
| Protokoly a služby per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING) |  |
| NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955) a Flexible NetFlow (nebo funkčně ekvivalentní) pro IPv4 i IPv6 |  |
| NetFlow (nebo funkčně ekvivalentní) na vstupu i výstupu |  |
| Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů |  |
| Statistiky určovány z každého paketu daného "flow" |  |
| Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb |  |
| Návaznost skriptů interpretovaných přepínačem po detekci daných parametrů "flow" |  |
| Zobrazení sbíraných infromací o "flow" přímo v přepínači. I včetně "TopN" pohledu. |  |
| Export statistik "flow" selektivně na více kolektorů |  |
| Interpretace uživatelských CLI a Tcl skriptů a jejich aktivace asynchronní událostí v systému zařízení |  |
| Konfigurovatelná autodiagnostika při startu i za provozu zařízení |  |
| Nástroj měření odezev sítě (např. IP SLA) pro IPv4 i IPv6 |  |
| Měření a ovládání spotřeby energie k LAN připojených koncových zařízení |  |
| Textové řádkově orientované/CLI konfigurační rozhraní |  |
| Konfigurace zařízení v člověku čitelné textové formě |  |
| Povyšování operačního software zařízení po síti pomocí protokolů TFTP, FTP a HTTP |  |
| Načtení/zálohování textové konfigurace zařízení po síti pomocí protokolů TFTP, FTP a HTTP |  |
| Přepínač může sloužit pro automatickou zálohu a obnovu firmware včetně konfigurace pro podřízený/é přepínač/e |  |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu |  |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů |  |
| Sériová konzolová linka |  |
| SSHv2 |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL |  |
| Synchronizace času protokolem NTPv3 (klient i server) |  |
| SNMPv2 |  |
| SNMPv3 |  |
| RADIUS klient pro AAA (autentizace, autorizace, accounting) |  |
| TACACS+ klient |  |
| Zrcadlení portů (funkční ekvivalent SPAN) |  |
| Vzdálené zrcadlení portů (funkční ekvivalent RSPAN) |  |
| Pokročilé interní nástroje pro ladění/debugging procházejícího provozu |  |
| Syslog |  |

\*Je nutné doplnit vysvětlení v případě náhrady komponentů.

## **INFRASTRUKTURA DATOVÉHO CENTRA**

Zadavatel požaduje vybudovat kompletní síťovou infrastrukturu datového centra a následně požaduje připojit k této infrastruktuře všechny servery a ostatní technologie, které jsou nyní zakončeny na páteřních přepínačích. Tato infrastruktura musí být vybudována v plně redundantním režimu.

Je požadováno, aby síť tvořila dvojice centrálních přepínačů, které budou v rámci jednotlivých rozváděčů datového centra rozšířeny o distribuované moduly s požadovanými fyzickými porty a jejich počtem. Na dvojici centrálních přepínačů datového centra je požadována rychlejší hardwarová podpora 24x7x4, kdy v případě poruchy dojde k výměně vadného hardware do 4 hodin od nahlášení závady.

Pro každý centrální přepínač požaduje zadavatel dodání jednoho rozšiřujícího modulu (celkem tedy 2 modulů), každý s klientskými porty 1/10GBASE-T. Propojení obou centrálních přepínačů a připojení každého vzdáleného modulu bude realizováno vždy dvěma 40GE spoji. Pro každý spoj budou k dispozici dvě vícevidová optická vlákna. Transceivery pro propojení budou součástí dodávky.

Zadavatel zároveň požaduje osazení každého centrálního přepínače čtyřmi transceivery 10GBaseLRM a třemi transceivery 1000BaseT. Celkové požadavky na každý systém jsou uvedeny v tabulce níže, včetně počtu distribuovaných modulů a jejich typu.

Dodaná infrastruktura musí obsahovat všechny potřebné transceivery. Připojení datového centra k jádru LAN sítě musí být realizováno přes páteřní přepínače sítě ČRo v režimu vysoké dostupnosti s celkovou šířkou pásma minimálně 4x10GE. Distribuované moduly musí být připojeny k centrálním přepínačům datového centra připojeny minimální konektivitou 2x40GE.

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Poznámka\*** |
| **HW specifikace** | |
| Formát zařízení - Fixní |  |
| Typ hardwarového přepínače – L3 přepínač |  |
| Redundantní zdroj |  |
| Celková propustnost přepínače – 3,6 Tbps |  |
| Minimální počet neblokovaných portů typu 40/50GE s volitelným fyzickým rozhraním typu QSFP – 28 |  |
| Z toho počet portů, které podporují rozhraní 10GE ve formátu SFP+ (možno formou redukce) – 9 |  |
| Minimální počet neblokovaných portů 100GE s volitelným fyzickým rozhraním typu QSFP28 - 4 |  |
| Podpora 40GE rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4 |  |
| Podpora distribuovaných rozšiřujících modulů (virtuální vzdálené rozšiřujících moduly umístěné v jiném fyzickém šasi) |  |
| Minimální počet 1/10GBASE-T portů dostupných na vzdáleném modulu - 2x48 |  |
| Osazení 10GE transceivery - 4x10GBase-LRM |  |
| Osazení 1GE transceivery – 3x1000 BaseT |  |
| CLI rozhraní |  |
| **Funkční specifikace** |  |
| VXLAN bridging | |  |
| VXLAN gateway |  |
| VXLAN routing |  |
| VXLAN with MP-BGP EVPN control plane |  |
| IEEE 802.3ad |  |
| IEEE 802.3ad přes více šasi (Multichassis Link Aggregation) |  |
| Minimálně 32 linek jako součást Link Aggregation Group |  |
| Minimální počet konfigurovatelných Link AggregationGroups - 256 |  |
| Podpora "jumbo rámců" – min. 9216 bytes |  |
| IEEE 802.1Q |  |
| Minimální počet aktivních VLAN - 4000 |  |
| Podpora instance spanning-tree protokolu per VLAN – min. 256 |  |
| IEEE 802.1w - Rapid SpanningTreeProtocol |  |
| Detekce protilehlého zařízení (např. LLDP) |  |
| Minimální počet MAC záznamů - 96000 |  |
| QoS classification – ACL, DSCP, CoSbased |  |
| QoS marking - DSCP, CoS |  |
| QoS – Priority BasedFlowControl (IEEE 802.1Qbb) |  |
| Approximate Fair Droping |  |
| Možnost zobrazit využití bufferů per port a per queue v reálném čase |  |
| Min. velikost sdíleného systémového bufferu – 40MB |  |
| Možnost rozšířit funkcionalitu přepínače o FCoE NPV |  |
| GRE (Generic Routing Encapsulation) |  |
| Minimální počet host IPv4 routes - 200000 |  |
| First Hop Redundancy Protokol (např. VRRP, HSRP) |  |
| OSPFv2 |  |
| BGP |  |
| ECMP – min. 64 cest |  |
| IGMPv2, IGMPv3, MLDv2 |  |
| IGMP snooping |  |
| IP Multicast (PIM SMPIM SSM) pro IPv4 i IPv6 |  |
| Virtualizace směrovacích tabulek - např. VirtualRouting and Forwarding (VRF) |  |
| First Hop Redundancy Protokol pro IPv6 |  |
| OSPFv3 |  |
| MP BGP |  |
| VLAN ACL |  |
| HW podpora realtime line rate telemetrie (schopnost monitorovat každý paket, každý datový tok procházející přepínačem) |  |
| Integrovaná Flow table – min. 32000 záznamů |  |
| Control Plane Policing |  |
| Podpora NETCONF/YANG |  |
| Streaming telemetrie - gRPC/GPB transport |  |
| Streaming telemetrie – time-based a event-basedtriggers |  |
| Python scripting |  |
| Puppet, Chef programming |  |
| Power-on autoprovisioning |  |
| SSHv2 |  |
| SNMPv3 |  |
| NTP server |  |
| RADIUS klient pro AAA (autentizace, autorizace, accounting) |  |
| TACACS+ klient |  |
| Port mirroring (SPAN) |  |
| Vzdálený port mirroring |  |
| Počet SPAN spojení – 4 |  |
| Syslog |  |
| Role Based Access Control |  |
|  |  |

\*Je nutné doplnit vysvětlení v případě náhrady komponentů.

**Terminálové servery**

Zadavatel požaduje dodání dvojice terminálových serverů, které budou sloužit primárně pro terminálový přístup přes sériové rozhraní k vybraným zařízením, umístěným v sálech s datovými technologiemi. Umístění terminálových serverů je požadováno v datovém centru. Minimální požadované vlastnosti jsou uvedeny v tabulce níže

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Poznámka\*** |
| **Typ zařízení – směrovač** |  |
| Formát zařízení – modulární |  |
| Požadovaný počet portů Gig0abitEthernet (WAN) – 1x10/100/1000Base-TX kombo s SFP, 1x10/100/1000Base-TX |  |
| Požadovaný počet portů sériové rozhraní – asynchronní – min. 16 |  |
| Sloty pro rozšiřující moduly – min. 2 |  |
| Možnost rozšíření formou modulů na celkový počet sériových portů – min. 48 |  |
| Autentizace přístupu ke každému sériovému portu uživatelským jménem/heslem prostřednictvím centrálního AAA serveru (TACACS+ a Radius) |  |
| Evidence a autorizace přístupu k sériovým portům prostřednictvím centrálního AAA serveru (TACACS+ a Radius) |  |
| Dostupnost funkcionality akcelerace aplikací i v samotném firmware směrovače |  |
| Směrování IPv4 |  |
| Směrování IPv6 |  |
| OSPFv2 |  |
| BGPv4 |  |
| 4 byte AS numbers in BGP |  |
| First Hop Redundancy Protokol (např. VRRP, HSRP) |  |
| GRE (GenericRoutingEncapsulation) |  |
| Policy-basedrouting podle ACL |  |
| IP Multicast (PIM SSM, PIM SM) |  |
| IGMPv2, IGMPv3 |  |
| uRPF |  |
| First Hop Redundancy Protokol pro IPv6 |  |
| OSPFv3 |  |
| Minimální počet oddělených (nezávislých) směrovacích tabulek – 15 |  |
| Možnost rozšíření o IPv6 MPLS VPN (6VPE) |  |
| QoS classification – ACL, DSCP, CoS, MPLS based |  |
| QoS marking - DSCP, CoS, MPLS |  |
| QoS Shaping |  |
| ClassBased and Priority queuing |  |
| RateLimiting |  |
| Hierarchical QoS – mi. 3 úrovně |  |
| Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, PING, traceroute) |  |
| ACL na rozhraní IN/OUT |  |
| Možnost rozšíření o zonebased firewall |  |
| Možnost rozšíření o stavovou filtrace (firewall) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám síťových prostředků (např. Security Group Firewall nebo funkčně ekvivalentní) |  |
| Možnost rozšíření o klasifikaci bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Security Group Exchange Protocol dle RFC draft-smith-kandula-sxp-01 nebo funkčně ekvivalentní). |  |
| Možnost rozšíření o monitorování aplikačních toků (za účelem detekce bezpečnostních incidentů) prostřednictvím technologie NetFlow nebo ekvivalentní |  |
| Možnost rozšíření o definici klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód |  |
| Možnost rozšíření o podporu minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat) |  |
| Možnost rozšíření o export NetFlow dat dle formátu NetFlow v9 nebo IPFIX |  |
| Možnost rozšíření o Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní |  |
| Možnost rozšíření o směrování dle dynamicky měřených metrik, typu aplikace, zejména pro realtimové a multimediální aplikace (např. Performance Routing nebo ekvivalentní) |  |
| SSHv2 |  |
| CLI rozhraní |  |
| SNMPv2/v3 |  |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) |  |
| NTPv3 server |  |

\*Je nutné doplnit vysvětlení v případě náhrady komponentů.

Před zahájením implementace požaduje zadavatel zpracování realizačního projektu, který bude obsahovat analýzu stávajícího stavu, návrh cílového řešení a postup implementace. Implementační práce budou podmíněny akceptací projektové dokumentace zadavatelem. Projektová dokumentace bude vypracována v písemné i elektronické podobě, ve formátu MS Word/Excel, MS Visio a PDF.

V rámci implementace požaduje zadavatel provedení akceptačních testů. Strukturu akceptačních testů vypracuje dodavatel. Testován bude provoz sítě se simulací výpadků jednotlivých aktivních prvků a jejich komponentů (simulace výpadku zdroje, modulárního větráku, jednoho uplinku) konfigurovaných v HA módu.

Po dokončení implementace požaduje zadavatel dodání dokumentace konečného provedení. Dokumentace bude vypracována v písemné i elektronické podobě, ve formátu MS Word/Excel, MS Visio a PDF.

Jako součást dodávky požaduje zadavatel školení administrace HW v nezbytně nutném rozsahu pro základní administraci systémů.