

SÍŤOVÁ INFRASTRUKTURA

Minimální parametry a rozsah

Požadavky zadavatele vymezují minimální technické parametry a rozsah plnění veřejné zakázky včetně požadovaných množství. U položek s předpokládaným dodáním více kusů je popis technických parametrů uveden pro jeden kus.

Případné názvy a popisy v zadávací dokumentaci odkazující na jednotlivá obchodní jména a označení výrobků či obchodních názvů materiálů popisují a specifikují podmínky požadovaného plnění s tím, že zadavatel připouští i jiná kvalitativně a technicky obdobná řešení za podmínky, že nesmí dojít ke zhoršení požadovaných parametrů technického řešení. Musí být zachována plná kompatibilita s již používanými zařízeními, která zůstanou v provozu paralelně s předmětem plnění zakázky. V případě požadavků na rozšíření stávajících systémů je přípustné, aby zájemce nabídl nový systém, který však bude stejných nebo lepších kvalitativních parametrů, jako rozšiřovaný systém.

Zadavatel nebude lépe hodnotit parametry lepší než minimální.

Zájemce prokáže, že všechny výrobky, které dodá zadavateli:

- a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
- b) mají plnou záruku od výrobce,
- c) budou podporovány výrobcem a budou součástí servisního a podpůrného programu výrobce pro ČR,
- d) obsahují licenci na používání příslušného softwaru,
- e) jsou/budou v databázi výrobce uvedeny jako nabízená/prodaná zadavateli,
- f) jsou určeny pro provoz v České republice.

Tyto skutečnosti zájemce doloží čestným prohlášením distributora nebo výrobce, popř. zájemcem samotným, nelze-li prohlášení distributora získat. Zadavatel si vyhrazuje právo na zjištění původu výrobku při jejich převzetí, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku u výrobce.

Veškeré požadované funkce musí být zároveň licencovány výrobcem.

Zadavatel si vyhrazuje právo vyžádat si od zájemce předvedení ukázky funkčního řešení vybrané části architektury v termínu max. 30 dnů od vyžádání.

2 x FIREWALL

Základní technické požadavky

- Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází, ...)
- Požadujeme dodání zařízení ve formátu HW appliance o velikosti 1RU
- Požadujeme veškeré příslušenství (montážní prvky) pro montáž do RACKu

Počet síťových rozhraní RJ45 10/100/1000	>= 18
Počet SFP	>= 4 GbE SFP
Propustnost 1518 / 512 / 64 byte UDP paketů	>= 18/18/8 Gbps
Latence firewallu (64B UDP paket)	<= 5 µs
Výkon firewall	>= 13 Mpps
Počet naráz otevřených spojení	>= 1,8 milionů
Počet nových spojení za sekundu	>= 130 000
Propustnost IPSEC VPN (512 B paket)	>= 8 Gbps
Propustnost SSL VPN	>= 780 Mbps
Propustnost IPS (HTTP / Traffic mix)	>= 5500/2000 Mbps
Podpora funkce bezdrátový kontrolér	>= 64 AP
Záruka a servis	60 měsíců HW a SW podpora

Funkce

Networking a High Availability

- Režim vysoké dostupnosti: Active/Active, Active/Passive, synchronizace stavové tabulky a SA mezi nody v clusteru
- Režim fungování L2 – transparentní režim, L3 – NAT/Router
- Podpora VLAN
- Podpora multicastu, vytváření politiky pro multicast routování
- Podpora 802.3ad link aggregation
- Funkce Load Balancing – možnost rozdělování zátěže směřující na virtuální IP na reálné servery, podpora health check funkcí, podpora SSL offload
- Podpora centrální NATovací tabulky, stavová inspekce SCTP komunikace
- Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP
- Policy based routing

VPN

- Podpora VXLAN
- Podpora VPN: SSL (portálový režim, tunelový režim)
- IPSEC (IKE, manual key, certifikát, gateway to gateway, hub and spoke, dial up konfigurace, internet browsing konfigurace, podpora více tunelů – redundantní VPN, možnost VPN v L2 – transparentním režimu, podpora IPv6
- Podpora L2TP, PPTP, GRE
- podpora dynamických routovacích protokolů OSPF, BGP ve VPN IPsec
- Podpora dynamicky navazovaných tunelů dle potřeby komunikace

UTM

- UTM funkce, možnost výběru mezi file based režimem (buffer) nebo flow based (inspekce on-the-fly)
- Antivirus pro vybrané protokoly, možnost volby různých databází, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd)
- Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty
- Intrusion Protection System – detekce útoků založena na signaturové části a na anomálním filtru, možnost vytvářet vlastní signatury.
- Web Filter – založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorií na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne
- Web Filter – minimálně 50 filtračních kategorií
- Data Leak Prevention s funkcí document fingerprinting
- Reputační databáze obsahující známe IP adresy a domény C&C Botnet sítí
- Application Control – detekce, monitoring, povolení či zakázání více než 3000 síťových aplikací na základě signatury dané aplikace, nikoliv dle portu, možnost tvorby vlastních signatur
- Deep scanning – možnost kontroly komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,...)
- DoS Policy prevence proti základním útokům typu DoS

Firewall

- Možnost nastavovat firewall politiku na základě geografických údajů
- Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru
- Viditelnost do provozu na aplikační úrovni
- Možnost definice FW pravidel v tzv. NGFW režimu tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filtering (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo).
- Endpoint Control a monitoring – kontrola připojené pracovní stanice na patch level, instalovaný vhodný service pack, antivirový software, personální firewall či jiný software
- Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu
- Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
- Traffic Shaping, QoS s podporou DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii
- Podpora VoIP, SIP včetně zabezpečení, rate limiting, analýzy protokolu
- Reverzní proxy, WCCP
- Explicitní Proxy – plná podpora UTM profilů, podpora ověřování protokolem Kerberos
- Podpora silné autentizace uživatelů – integrovaná podpora generátoru jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů

Integrovaný kontroler bezdrátových (Wifi) sítí

- Wifi kontroler integrovaný do NGFW platformy
- Každá bezdrátová síť (SSID) bude reprezentována virtuálním síťovým rozhraním
- podpora bezpečnostních profilů (AV, AppControl, Webfilter, DLP) přímo na wifi kontroleru
- podpora SSL dekrypcie uživatelského provozu přímo na wifi kontroleru
- Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení

- On-wire rogue AP detekce a mitigace
- Podpora fast-roamingu (802.11 k,v,r)
- podpora více PSK u jednoho SSID
- podpora IPSEC tunelu pro šifrování data plane (uživatelských dat)

Management

- FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici
- Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě
- Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)

Požadujeme dodávku včetně implementace do stávající infrastruktury.

2 x SWITCH CORE

Typ parametru	Parametr	Minimální požadavek zadavatele
Základní vlastnosti	Typ zařízení	L3 switch
	Velikost zařízení 1U	ano
	Počet 10GE optických portů s volitelným fyzickým rozhraním	48x SFP+
	Počet 40GE optických portů s volitelným fyzickým rozhraním	6x QSFP+
	40GE port lze konvertovat na 4 nezávislé 10GE porty	ano
	Interní hot-swap AC napájecí zdroje	ano, 2x stejný model
	Možnost interního DC napájecího zdroje	ano
	Redundantní hot-swap ventilátory	ano
	Volitelný směr proudění vzduchu zařízením	ano, zezadu-dopředu
	Celková propustnost přepínače	1,44 Tbps
	Celkový paketový výkon přepínače	1050 Mpps
	Podpora Cut-Through přepínání	ano
	Podpora upgrade OS přepínačů ve stohu, bez narušení provozu (ISSU)	ano
	Počet přepínačů ve stohu	9
Stohování	Sestavení stohu přes standardizované síťové rozhraní	ano
	Stoh podporuje distribuované přepínání paketů	ano
	Kterýkoli prvek ve stohu může být řídicím prvkem (1:N redundance)	ano
	Stoh podporuje jednotnou konfiguraci (IP adresa, správa, konfigurační soubor)	ano
	Podpora seskupení portů (IEEE 802.3ad) mezi různými prvky stohu	ano
	Stoh vystupuje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF a OSPFv3	ano
	Podpora stohování mezi lokalitami vzdálenými až 10 km	ano
	Kapacita stohovacího propojení	80 Gbit/s
	Podpora jumbo rámců včetně velikosti 10k Byte	ano
Funkce a protokoly	IEEE 802.3ad	ano
	Počet LACP skupin/linek ve skupině	128/16
	Podpora VLAN podle IEEE 802.1Q	4000 aktivních VLAN
	Počet záznamů v tabulce MAC adres	288 000
	Protokol-based VLAN	ano
	MAC-based VLAN	ano
	Private VLAN včetně primary, secondary a community VLAN	ano
	Protokol pro definici šířených VLAN (MVRP nebo GVRP)	ano
	Tunelování 802.1Q v 802.1Q	ano
	IEEE 802.1s - multiple spanning trees	ano
	IEEE 802.1w - Rapid Tree Spanning Protocol	ano
	Podpora STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)	ano
	Detekce protilehlého zařízení pomocí LLDP	ano
	Implementace CFM a OAM na Ethernetu	802.3ah, 802.1ag
	Transparent Interconnection of Lots of Links (TRILL)	ano
	MPLS Layer-3 a Layer-2 VPN (VPLS)	ano
	FCoE v souladu s FC-BB-5, podpora režimů: FCF, NPV a transit	ano

	IEEE 802.1Qbb – PFC	ano
	IEEE 802.1Qaz – ETS	ano
	DHCP server pro IPv4 a IPv6	ano
	DHCP relay pro IPv4 a IPv6	ano
	Podpora zapouzdření: GRE over IPv4, GRE over IPv6, IPv6 over IPv6	ano
	DNS klient pro IPv4 a IPv6	ano
	Podpora Layer3 routed port	ano
	Statické směrování IPv4 a IPv6	ano
	Směrování OSPF a OSPFv3 včetně podpory BFD	ano
	Směrování BGP a MP BGP včetně podpory BFD	ano
	Policy based směrování na základě ACL pro IPv4 a IPv6	ano
	IGMP a MLD Snooping	ano
	Směrování multicast IPv4: PIM-DM, PIM-SM, PIM-SSM, BIDIR-PIM	ano
	Směrování multicast IPv6: PIM-DM, PIM-SM, PIM-SSM, BIDIR-PIM	ano
	Podpora MSDP	ano
	Hardware podpora IPv4 a IPv6 ACL	ano
	IEEE 802.1p - Minimální počet front	8
	ACL klasifikace na úrovni zdrojová/cílová MAC adresa, zdrojová/cílová IPv4/IPv6 adresa, číslo zdrojového/cílového portu, protokol, číslo VLAN	ano
	HW ochrana proti zahlcení (broadcast/multicast/ unicast) nastavitelná na procentuální rychlost portu a množství paketů za vteřinu	ano
	BPDU guard a Root guard	ano
	DHCP snooping pro IPv4 a IPv6	ano
	QoS ochrana před zahlcením WRED	ano
	Kontrola dostupnosti zdroje routovaného unicast packetu	ano
	Lze aktivovat podporu SDN VMware NSX	ano
Management	CLI formou RJ45 serial konsole port	ano
	Konfigurace zařízení v člověku čitelné textové formě	ano
	OoB management formou portu RJ45 s podporou ethernetu	ano
	USB port pro přenos konfigurace a firmware	ano
	SSHv2 a SCP pro IPv4 a IPv6	ano
	Podpora PKI včetně možnosti importu certifikátu CA	ano
	Podpora SNMPv2c a SNMPv3	ano
	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
	Podpora Role Based Access Control (RBAC)	ano
	Podpora Radius	ano
	Podpora TACACS včetně command authorization	ano
	Port mirroring, alespoň 4 různé obousměrné session	SPAN, RSPAN
	Zrcadlení provozu na základě ACL (traffic mirroring)	ano
	Podpora skriptování v jazyce Python	ano
	Podpora Netconf over SSH	ano
	Automatická archivace konfigurací na vzdálené FTP / SCP	ano, např. skriptem
	Analýza síťového provozu sFlow podle RFC 3176	ano
	Podpora OpenFlow v1.3	ano

Záruka a servis

60 měsíců HW a SW podpora poskytovaná přímo výrobcem zařízení s odezvou a opravou zařízení následující pracovní den

Součástí dodávky musí být (dohromady pro oba switche):

- 2 ks propojovací kabely DAC 40Gb QSFP+ 1m
- 34 ks SFP+ transceiver 10GBASE-LR/LW SM 10km LC duplex
- implementace do stávající infrastruktury.

10 x SWITCH KONCOVÝ

Typ parametru	Parametr	Minimální požadavek zadavatele
Základní vlastnosti	Třída zařízení	L3 switch
	Velikost zařízení: 1U	ano
	Počet 1Gbit/s metalických portů	48x10/100/1000Mbit RJ45
	Počet 10Gbit/s optických portů s volitelným fyzickým rozhraním	4x10Gbit SFP+ nezávislé
	10GE interface zpětně kompatibilní s 1Gbit/s a 100Mbit/s transceivery	ano
	Všechny ethernet porty jsou dostupné zepředu	ano
	Primární napájecí zdroj	1x interní AC
	Podpora Energy Efficient Ethernet (802.3az)	ano
	Celková propustnost přepínače	176 Gbps
	Celkový paketový výkon přepínače	112 Mpps
	Paměťový buffer	12MB
	Maximální hloubka přepínače	max. 27 cm
Funkce a protokoly	Podpora "jumbo rámců" včetně velikosti 9220 Byte	ano
	Podpora linkové agregace IEEE 802.1AX	ano
	Konfigurovatelné rozkládání LACP zátěže podle L3 a L4	ano
	Počet LACP skupin/linek ve skupině	26/8
	Počet záznamů v tabulce MAC adres	16 000
	Počet záznamů v tabulce ARP	1 000
	Protokol pro definici šířených VLAN	MVRP
	Podpora VLAN podle IEEE 802.1Q	512 aktivních VLAN
	Zařazování do VLAN podle protokolu 802.1v	ano
	Zařazování do VLAN podle MAC adresy bez nutnosti externího řízení (Radius)	ano
	IEEE 802.1s - Multiple Spanning Tree	ano
	STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)	ano
	Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED	ano
	Detekce jednosměrnosti optické linky (např. UDLD)	ano
	DHCP server	ano
	DHCP relay pro IPv4 a IPv6 včetně option 82 a 79	ano
	NTP pro IPv4 a IPv6 včetně MD5 autentizace	ano
	Statické směrování IPv4 a IPv6	ano
	Dynamické směrování RIPv2 a RIPv6	ano
	Počet záznamů ve směrovací tabulce	2 000
	IGMP v3 a MLD v2	ano
	Hardware podpora IPv4 a IPv6 ACL	ano
	ACL definice na základě skupiny fyzických portů	ano
	ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN	ano
	BPDU Guard a Root Guard	ano
	DHCP snooping pro IPv4 a IPv6	ano
	HW ochrana proti zahlcení (broadcast/multicast storm) nastavitelná na % rychlosti portu a množství paketů za vteřinu	ano

	ICMPv4 a ICMPv6 rate-limiting per port	ano
	Podpora ověřování 802.1X včetně více uživatelů per-port	32 uživatelů na port
	RADIUS MAC autentizace, probíhající před 802.1x pro případy, že koncové zařízení není softwarově vybaveno pro 802.1x autentizaci	ano
	Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675	ano
	Podpora 802.1X Guest VLAN	ano
	Podpora IPv6 RA Guard	ano
	IP source guard / dynamic IP lockdown pro IPv4 a IPv6	ano
	Podpora Dynamic ARP protection	ano
	Port security - omezení počtu MAC adres na port, statické MAC, možnost definování akcí při překročení	ano
	Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení	ano
	Ochrana control plane (CPU) před útoky typu DoS	ano
	Podpora IPv4 a IPv6 QoS	ano
	IEEE 802.1p - minimální počet front	8
Management	CLI formou RJ45 serial konsole port	ano
	USB konzolový port	ano
	Konfigurace zařízení v člověku čitelné textové formě	ano
	Podpora managementu přes IPv4 i IPv6	ano
	SSHv2 a SFTP	ano
	Podpora SNMPv2c a SNMPv3	ano
	RMON	ano
	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
	Lokálně vynucené RBAC na úrovni přepínače	ano
	Dualní flash image	ano
	TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logování do více syslog serverů	ano
	Podpora oddělených čítačů paketů pro IPv4 a IPv6 provoz	ano
	Podpora RADIUS včetně RADIUS CoA (RFC3576)	ano
	Aktivní monitoring dostupnosti RADIUSu přednastaveným jménem a heslem	ano
	Podpora TACACS+	ano
	Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)	ano
	Analýza síťového provozu sFlow podle RFC 3176	ano
	Podpora zrcadlení portů (SPAN) v režimu N:1	ano
	Podpora IP SLA pro měření zpoždění provozu VoIP	ano
	Podpora Zero Touch Provisioning (ZTP)	ano
	REST API pro automatizaci nastavení, včetně popory CLI a batch CLI příkazů	ano
	Podpora Chromecast Gateway	ano
	Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty. (Apple Bonjour Gateway)	ano
	Automatická konfigurace portu dle připojeného zařízení	ano
	Podpora Cloud based management	ano
Záruka a servis	60 měsíců HW a SW podpora poskytovaná přímo výrobcem zařízení s odezvou a opravou zařízení následující pracovní den	

Součástí dodávky musí být (dohromady pro všechny switche):

- 20 ks SFP+ transceiver 10GBASE-LR/LW SM 10km LC duplex

7 x SWITCH KONCOVÝ

Typ parametru	Parametr	Minimální požadavek zadavatele
Základní vlastnosti	Třída zařízení	L3 switch
	Možnost splnění požadovaných parametrů dvěma switchi	ano
	Minimální propustnost stohovacího spojení v případě řešení se dvěma switchi (bez snížení počtu požadovaných portů)	1x10 Gbps
	Počet 1Gbit/s metalických portů	48x10/100/1000Mbit RJ45
	Počet 10Gbit/s optických portů s volitelným fyzickým rozhraním	2x10Gbit SFP+ nezávislé
	10GE interface zpětně kompatibilní s 1Gbit/s a 100Mbit/s transceivery	ano
	Všechny ethernet porty jsou dostupné zepředu	ano
	Primární napájecí zdroj	1x interní AC
	Podpora Energy Efficient Ethernet (802.3az)	ano
	Celková propustnost přepínače (platí pro jeden každý switch)	176 Gbps
	Celkový paketový výkon přepínače (platí pro jeden každý switch)	51 Mpps
	Paměťový buffer	3MB
	Maximální hloubka přepínače	max. 27 cm
	Hlučnost	Provedení bez ventilátorů
Stohování	Podporovaný počet přepínačů ve stohu	4
	Sestavení stohu přes standardizované síťové rozhraní	ano
	Stoh se chová jako jedno L2 zařízení z pohledu spanning tree	ano
	Podpora stohování mezi geograficky odlišnými lokalitami, vzdálenost mezi lokalitami 10km	ano
	Kapacita stohovacího propojení	20 Gbit/s
Funkce a protokoly	Podpora "jumbo rámců" včetně velikosti 9220 Byte	ano
	Podpora linkové agregace IEEE 802.1AX	ano
	Konfigurovatelné rozkládání LACP zátěže podle L3 a L4	ano
	Počet záznamů v tabulce MAC adres	16 000
	Podpora VLAN podle IEEE 802.1Q	1024 VLAN
	IEEE 802.1s - Multiple Spanning Tree	ano
	Detekce protilehlého zařízení pomocí LLDP	ano
	DHCP relay pro IPv4 a IPv6 včetně option 82 a 79	ano
	NTP pro IPv4 a IPv6 včetně MD5 autentizace	ano
	Statické směrování IPv4 a IPv6	ano
	Počet záznamů ve směrovací tabulce	32
	IGMP v3 a MLD	ano
	Hardware podpora IPv4 a IPv6 ACL	ano
	ACL definice na základě skupiny fyzických portů	ano
	BPDU Guard a Root Guard	ano
	DHCP snooping pro IPv4 a IPv6	ano
	Port security - omezení počtu MAC adres na port, statické MAC, možnost definování akcí při překročení	ano
Management	CLI formou RJ45 serial konsole port	ano
	Konfigurace zařízení v člověku čitelné textové formě	ano

	Podpora managementu přes IPv4 i IPv6	ano
	SSHv2 a SFTP	ano
	Podpora SNMPv2c a SNMPv3	ano
	RMON	ano
	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
	Podpora RADIUS včetně RADIUS CoA (RFC3576)	ano
	Podpora TACACS+	ano
Záruka a servis	60 měsíců HW a SW podpora poskytovaná přímo výrobcem zařízení s odezvou a opravou zařízení následující pracovní den	

Součástí dodávky musí být (dohromady pro všechny switche):

- 14 ks SFP+ transceiver 10GBASE-LR/LW SM 10km LC duplex

V případě nabídky dvou samostatných switchů požadujeme dodávku včetně 7 ks stohovacích kabelů.