

## Požadované technické parametry dodávky

Předmětem dodávky je aktivní síťový prvek dle technických podmínek uvedených níže.

### Tabulka povinných požadavků pro směrovač (požadován 1 ks)

Požadavek na funkcionalitu	Minimální požadavky
<b>Základní vlastnosti</b>	
Třída zařízení	směrovač, firewall
Formát zařízení	fixní konfigurace, desktop provedení
Montážní přípravek do racku s vyvedením portů dopředu a přichycením napájecího zdroje	ano
Počet 100/1000Base-T portů	5
Počet optických portů 1GE a jejich typ	1, SFP
Sériová konzolová linka	ano
<b>Podporované funkce</b>	
Provoz zařízení v režimu L3 (směrování)	ano
Podpora virtuálních instancí firewallu – plná funkcionalita jednotlivých virtuálních firewallů	ano
Podpora management protokolů SNMP, Syslog, NTP ve virtuální instanci firewallu	ano
Podpora překladu adres NAT/PAT	ano
Podpora protokolu IPv6 pro management, IPv6 tunnelling, firewalling, NAT46, NAT64, IPv6 IPsec VPN	ano
Podpora tunelování GRE a VXLAN	ano
Počet podporovaných VLAN	250
Podpora IEEE 802.1Q	ano
Podpora QoS pro IPv4 a IPv6	ano
Podpora prioritizace provozu na aplikační úrovni (7. vrstva)	ano
Podpora Link Aggregation IEEE 802.3ad/LACP	ano
Vytváření bezpečnostních zón (Zone-based firewall)	ano
<b>DoS/DDoS ochrana</b>	
Dekódování DNS, HTTP	ano
Identifikace útočících stanic – prahové hodnoty pro dotazy za časovou jednotku	ano
Akce blokace požadavků, akce snížení počtu požadavků za časovou jednotku	ano
Antispoofingová kontroly Reverse Path Forwarding Check pro IPv4 i IPv6	ano
Ochrana centrálního procesoru (Control Plane) pomocí rate limiterů	ano
<b>Správa a monitoring</b>	
Grafické rozhraní pro kompletní správu firewallu	ano
Textově orientované konfigurační rozhraní (CLI)	ano
Konfigurace zařízení v člověku čitelné textové formě	ano
Povýšení operačního software zařízení po síti pomocí protokolů TFTP, FTP a/nebo HTTP, HTTPS, SFTP/SCP	ano
Možnost nahrání/zálohování textové konfigurace zařízení po síti pomocí protokolů TFTP, FTP a/nebo HTTP, HTTPS, SFTP/SCP	ano
Přístup pomocí protokolu SSHv2	ano
Podpora protokolů SNMPv2, SNMPv3	ano
DNS klient	ano

Podpora synchronizace času protokolem NTPv3	ano
Podpora NetFlow v9, IPFIX nebo ekvivalentních protokolů exportů toků/flow	ano
Ověřování přístupu k zařízení pomocí RADIUS anebo TACACS+ protokolu	ano
Vzdálené logování na syslog server	ano
Systémový rollback konfigurace	ano
Správa revizí konfigurací	ano
<b>Směrovací protokoly</b>	
Směrování pro IPv4 a IPv6 s akcelerací v hardware	ano
Dynamické směrování pro IPv4 (OSPF, BGP)	ano
Dynamické směrování pro IPv6 (OSPFv3, MP-BGP)	ano
OSPF s MD5 a NSSA	ano
Policy-based routing	ano
Statické směrování pro IPv4 a IPv6	ano
<b>Směrování multicastu</b>	
PIM (dense i sparse mód)	ano
PIM pro IPv6	ano
IGMPv2	ano
IGMPv3	ano
IGMPv3 snooping	ano
<b>Bezpečnost</b>	
Statefull firewall	ano
Transparentní (L2) stavový firewall	ano
Možnost rozšíření o rozpoznávání aplikací	ano
Možnost rozšíření o kategorizaci a kontrolu web obsahu	ano
ACL na rozhraní IN/OUT včetně virtuálních – VLAN, loopback, 802.3ad	ano
ACL pro IP	ano
ACL pro ethernetové rámce	ano
ACL podle regulárních výrazů ze záhlaví paketu i vlastních dat	ano
<b>Management</b>	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
Možnost omezení přístupu k CLI definováním uživatelských rolí	ano
Podpora managementu stávajícího firewallu	ano
DNS klient	ano
NTP klient s MD5 autentizací	ano
Nástroje pro měření odezev v síti (například IP SLA nebo ekvivalentní)	ano
<b>Výkonnostní parametry</b>	
Minimální agregovaná propustnost firewallu při plném zatížení	4 Gb/s
Maximální zpoždění při plném zatížení	4 μs
Minimální počet současných TCP spojení	700 tisíc
Minimální počet nových spojení	70 tisíc/s
Minimální propustnost IPSec VPN (AES256 + SHA256)	4 Gb/s
Minimální počet IPSec tunelů	200
Počet virtuálních instancí firewallu	5

## Další technické požadavky

- Všechny poptávané aktivní síťové prvky musí být z důvodů ochrany stávajících investic a minimalizace celkových nákladů na vlastnictví a provoz počítačové sítě zadavatele kompatibilní se všemi již používanými zařízeními, komunikačními protokoly a systémy správy sítě specifikovanými níže.

## Požadavky na záruku a servis

- Požadujeme originální a nová zařízení, licencovaná ve jménu ZČU tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce.
- Po dobu trvání záruky budou dostupné nové originální náhradní díly od výrobce pro dodané řešení v režimu 24h x 7d x NBD (počet hodin dostupnosti servisu uchazeče x počet dní v týdnu dostupnosti servisu x doba pro odeslání náhradního dílu do místa plnění).
- Výše specifikovaná záruka, servis a dostupnost náhradních dílů je požadována po dobu **minimálně 36 měsíců (3 roky)**.

## Struktura technické části nabídky

Technická část nabídky musí obsahovat:

- **Podrobný popis technických a funkčních parametrů** nabízeného řešení, z něhož bude jasné patrné splnění jednotlivých položek technických a funkčních požadavků technického zadání.
- **Podrobný popis servisních a záručních podmínek**, z něhož bude jasné patrné splnění jednotlivých položek servisních a záručních požadavků zadání.
- **Podrobnou položkovou specifikaci** nabízených zařízení (např. typů šasi, jednotlivých modulů, operačního software, napájecích zdrojů apod.).

## Popis prostředí počítačové sítě ZČU

### Používané komunikační protokoly a podpůrné vlastnosti aktivních prvků sítě ZČU

V akademické síti ZČU WEBnet jsou v současné době používány následující komunikační protokoly a další podpůrné vlastnosti aktivních prvků, s nimiž musí být poptávaná zařízení kompatibilní:

- Podpora IEEE 802.1Q/p (minimálně 1000 VLAN, konfigurační možnosti statického omezování šíření VLAN), IEEE 802.1s/w (RSTP/MSTP), IEEE 802.3ad, IGMPv2/v3, MLDv1/v2 a vlastnické L2 protokoly VTPv3, PVRSTP+, CDPv2, UDLD.
- Možnosti ochrany spanning tree protokolu vůči zneužití (filtrace BPDU rámců na jednotlivých rozhraních, kontrola přípustnosti BPDU apod.).
- Podpora agregace linek (LACP nebo PAgP).
- Podpora privátních VLAN (logická izolace jednotlivých rozhraní nebo skupin rozhraní v rámci téže VLAN).
- Podpora omezení (procentuálního poměru) broadcastového a multicastového provozu na rozhraní.
- Duální podpora IPv4 a IPv6 unicast i multicast (možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, dual-stack).
- Podpora směrovacích protokolů BGPv4, OSPFv2, OSPFv3, PIM-SMv2, RIP, statického směrování a možnosti redistribuce směrovacích informací mezi jednotlivými protokoly, rozkládání zatížení na L3 paralelních cestách, možnosti vytváření logicky oddělených instancí virtuálních směrovacích tabulek v rámci téhož L3 přepínače (podpora virtuálních směrovacích instancí).
- Podpora HSRP nebo VRRP pro zajištění redundance výchozí brány koncovým stanicím/serverům.
- Podpora GRE tunelů.

- Podpora IGMPv2, IGMPv3 a hardwarová podpora omezování zbytečného šíření multicastových rámců/paketů na rozhraní bez explicitních příjemců (IGMPv2/v3 a MLDv1/v2 snooping).
- Možnost definovat povolené MAC adresy na portu, jejich maximální počet na portu a definování různého chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy).
- Hardwarová podpora bezstavové bezpečnostní filtrace provozu podle L2/L3/L4 atributů na úrovni linkové/síťové/transportní vrstvy aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní (VLAN).
- Vzdálený management aktivních prvků (typicky pomocí protokolů Telnet, SSH, HTTP/HTTPS nebo SNMPv2/v3).
- Implementace čítačů přenesených bytů/paketů pro jednotlivé relevantní entity síťových informací (typicky rozhraní, filtry apod.) přístupné přes příkazovou řádku a SNMP.
- Možnost nastavení omezení distribuce IP multicastu ve VLAN.
- Možnost ochrany proti útokům na úrovni síťové a linkové vrstvy (IP DHCP Snooping, Dynamic ARP Inspection, IP Source Guard).
- Hardwarová podpora zajištění kvality služby (QoS) podle L2/L3/L4 atributů umožňující implementaci QoS podle modelu rozlišovaných služeb (DiffServ).

## **Nástroje používané pro správu sítě ZČU**

Pro správu sítě ZČU jsou používány následující nástroje síťového managementu, s nimiž musí být poptávaná zařízení kompatibilní.

## **Připojení vzdálených lokalit pomocí VPN**

Pro připojení vzdálených lokalit ZČU je využíván firewall<sup>1</sup>, pro jehož management je používán specializovaný software<sup>2</sup>. Pro sledování a reportování provozních anomálií je používán specializovaný analyzátor<sup>3</sup>. Na firewallu jsou ukončeny VPN spojení vzdálených lokalit využívající technologii IPsec a GRE. Pro sledování provozu na úrovni L3/L4 datových toků se využívá technologie NetFlow v9. NetFlow informace exportované z firewallu se zpracovávají pomocí software FTAS<sup>4</sup>. Přístup na firewall je centrálně řízen pomocí protokolu TACACS+.

---

<sup>1</sup>Dva NGFW Fortinet Fortigate 1800F zapojené v clusteru.

<sup>2</sup>Virtuální appliance Fortinet FortiManager.

<sup>3</sup>Fortinet FortiAnalyzer 3000E.

<sup>4</sup><http://www.cesnet.cz/doc/techzpravy/2004/ftas-arch/>,  
<http://www.cesnet.cz/doc/techzpravy/2006/ftas-interface/>,  
<http://www.cesnet.cz/akce/2009/zazemi-pro-cert-csirt/p/sledovani-provozu.pdf>