

Požadované technické parametry dodávky

Předmětem dodávky je zařízení pro pokročilou správu a monitoring bezdrátové i drátové sítě.

Tabulka povinných požadavků

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Centralizovaný nástroj pro správu a monitoring drátové a bezdrátové sítě	ano
Formát zařízení	fyzická appliance, 1 RU
Redundantní napájecí zdroj, hotswap	2, ano
Počet a typ portů s rychlostí 10 Gb/s	2
Podpora stávajícího centrálního řadiče bezdrátové sítě	ano
Podpora stávající báze instalovaných AP	ano
Počet aktuálně provozovaných AP	1200
Výkonnostní parametry	
Počet současně spravovatelných zařízení (směrovač, přepínač, řadič bezdrátové sítě)	1000
Počet současně spravovatelných bezdrátových přístupových bodů	2000
Vlastnosti systému správy	
Jeden systém pro automatizaci, řízení, správu a monitoring drátové a bezdrátové sítě	ano
Zálohování systému / obnova systému ze zálohy	ano
Vzdálená správa systému	ano
Monitoring stavu a provozních parametrů systému	ano
Podpora pro modulární a inkrementální upgrade funkcí systému	ano
Automatická notifikace o dostupných aktualizacích systému	ano
Bezpečný přístup prostřednictvím grafického webového uživatelského rozhraní	ano
Přístupová práva založená na uživatelských rolích (RBAC)	ano
Podpora logování aktivity uživatelů a logování systémových událostí	ano
Otevřené API rozhraní pro integraci s externími systémy a podpora integrace do ITSM procesů	ano
Dokumentované API rozhraní pro volání funkcí systému	ano
Možnost integrace s nástroji pro správu IP adresního prostoru	ano
Vlastnosti správy síťových zařízení	
Automatické zjišťování stavu síťových zařízení	ano
Automatické rozpoznání role zařízení na základě jeho konfigurace/umístění v síti	ano
Inventarizace HW, SW a konfigurace spravovaných síťových zařízení	ano
Možnost přidat do inventury jednotlivé zařízení nebo skupinu zařízení	ano
Správa přístupových informací (credentials) pro konfiguraci a monitoring síťových	ano

zařízení	
Detailní přehled zařízení na základě typu zařízení nebo příslušnosti zařízení do lokality	ano
Umístění zařízení v mapách	
Hierarchické zobrazení topologické mapy včetně jejího členění na jednotlivé lokality (geo mapy)	ano
Umístění lokalit v mapách a základě adresy / GPS souřadnic	ano
Podpora pro import map z jiných nástrojů (Ekahau AI Pro, Prime Infrastructure apod.)	ano
Podpora pro import plánů budov pro jednotlivá patra	ano
Možnost návrh plánu patra pro pokrytí bezdrátovým signálem	ano
Vyhledávání zařízení v mapách	ano
Filtrování informací zobrazených v mapách	ano
Seskupování zařízení pro zajištění lepší přehlednosti	ano
Možnost výběru zařízení z mapy	ano
Grafická reprezentace stavu zařízení/lokality v mapě (zvýrazněné zařízení/lokality dotčené výpadkem apod.)	ano
Grafická reprezentace stavu pokrytí patra bezdrátovým signálem	ano
Hierarchické mapy zobrazující umístění bezdrátových přístupových bodů a jejich stav	ano
Správa software síťových zařízení	
Pokročilá správa operačních systémů (SW) síťových zařízení	ano
Podpora pro ověření integrity a originality obrazů operačních systémů pro síťová zařízení	ano
Podpora pro stažení posledních / doporučených verzí SW pro provozovaná síťová zařízení	ano
Podpora pro distribuci SW aktualizací na síťová zařízení	ano
Ověření úspěšné realizovatelnosti SW aktualizace - analýza stavu zařízení, identifikace případných rizik a jejich příčin	ano
Ověření úspěšného provedení SW aktualizace	ano
Možnost SW aktualizace více zařízení současně	ano
Možnost odložené aktivace SW aktualizace na základě volby uživatele	ano
Přehledné zobrazení zařízení, které vyžadují aktualizaci - jejichž SW není v souladu s definovanou politikou	ano
Správa konfigurace síťových zařízení	
Podpora pro Zero-Touch nasazení síťových zařízení	ano
Podpora pro automatizované zprovoznění síťového zařízení včetně standardního obrazu operačního systému a standardní konfigurace	ano
Automatická změna konfigurace sítě (síťových zařízení) po změně nastavení standardních síťových služeb	ano
Automatické nastavení standardních síťových služeb síťového zařízení po jeho instalaci do dané lokality	ano

Snadné vytváření politik (intent-based – podle potřeb chodu organizace, nikoli použitých síťových technologií)	ano
Automatická transformace síťových politik na specifickou konfiguraci konkrétních a politikou dotčených síťových zařízení podle role, HW, SW a stávající konfigurace těchto zařízení pro vybrané politiky	ano
Konfigurace sítě a síťových politik prostřednictvím předdefinovaných workflows	ano
Připravené postupy (workflows) pro automatizované nasazení QoS a jeho monitoring	ano
Integrace s identity management systémem pro segmentaci, mikrosegmentaci a řízení přístupu do sítě	ano
Podpora pro definici standardních konfigurací síťových zařízení a jejich implementaci	ano
Automatizovaný postup (workflow) pro provedení výměny vadného zařízení za nové s instalací standardního obrazu operačního systému a přenosem původní konfigurace včetně případného převodu licence pro aktivní prvky	ano
Podpora tvorby konfiguračních šablon v jazyce Jinja2 nebo podobném	ano
Podpora simulace nasazení konfiguračních šablon	ano
Přiřazení konfiguračních šablon k zařízení na základě lokality, modelu nebo značky	ano
Monitorování síťových zařízení	
Monitoring provozních parametrů (využití CPU, DRAM paměti, provozní teploty, stav HW apod.) všech řízených síťových zařízení	ano
Monitoring stavu a provozních parametrů (vytížení, chybovost apod.) rozhraní síťových zařízení	ano
Monitoring připojovaných koncových zařízení	ano
Monitoring událostí v síti	ano
Sběr analytických dat pro každé zařízení v síti	ano
Udržování přehledu o výkonnosti a stavu celé komunikační infrastruktury včetně monitorování stavu směrovacích protokolů	ano
Kompletní přehled o stavu celé síťové infrastruktury v jednom pohledu	ano
Zobrazení nejvýznamnějších zaznamenaných problémů na úrovni celé sítě	ano
Kompletní přehled stavu všech síťových zařízení v jednom pohledu	ano
Kompletní přehled stavu síťových zařízení konkrétní lokality v jednom pohledu	ano
Kompletní přehled stavu pro zařízení daného typu v jednom pohledu	ano
Kompletní přehled o provozovaných aplikacích	ano
Systém musí zobrazit přehledně detailní informace o stavu vybrané aplikace, vývoji jejího chování v čase, diagnostikovaných problémech a zdrojích informací o aplikačním provozu této aplikace v jednom pohledu	ano
Uchování minimálně 24 hodin provozní historie sítě umožňující analýzu stavu sítě stejnými postupy jako u právě probíhajících výpadků	ano
Monitorování klientů	
Kompletní přehled o množství, stavu a typu připojených klientů v jednom pohledu	ano
Snadná identifikace příčiny problémů připojení jednotlivých typů klientů	ano
Analýza příčiny síťových problémů a její upřesnění na základě provozních a	ano

organizačních souvislostí (context based)	
Diagnostika problémů klientů (stav a kvalita připojení apod.) a aplikací s využitím okamžitých a historických dat	ano
Retrospektivní analýza problémových situací klientů a infrastruktury	ano
Zobrazení detailů k vybranému problému včetně dotčené lokality, případně zařízení, klientů apod.	ano
Proaktivní monitoring a identifikace potenciálních problémů v síti na základě dlouhodobého sledování stavu sítě a zaznamenaných trendů	ano

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.

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 totéž fyzické nebo logické 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.

Správa konfigurací

Zálohování konfigurací všech aktivních komunikačních prvků Cisco je prováděno centrálně automaticky pomocí systému Oxidized¹ periodicky alespoň jednou denně. Archivace (změn) historie konfigurací je udržována minimálně po dobu jednoho roku.

Pro hromadné konfigurace skupin zařízení se využívají systémy Netmanager², umožňující paralelní vykonávání příkazů.

Správa bezdrátové sítě

Na ZČU je provozována bezdrátová síť eduroam³, která podporuje IP mobilitu a roaming uživatelů v rámci české sítě národního výzkumu a vzdělávání. Kromě toho je provozována síť zcu-mobile, která mobilitu a roaming nepodporuje. Pro její provoz byl vyvinut vlastní systém založený na open-source řešení. Obě řešení jsou navázána na AAA infrastrukturu založenou na ověřovacím serveru freeRADIUS⁴. Třetí bezdrátovou síť je zcu-hub, která je používána pro připojování IoT zařízení. Tato síť je navázána na ověřovací systém Cisco Identity Service Engine provozovaný v redundantním zapojení se dvěma PAN uzly. Pro správu a konfiguraci bezdrátových přístupových bodů je využíváno centralizované řešení⁵. Jako centrální prvky jsou použity dva bezdrátové řadiče⁶ pracující v režimu active/standby, které jsou schopny současně spravovat až 2000 AP. Pro konzistentní konfiguraci obou bezdrátových řadičů a monitoring klientů je používán specializovaný software⁵.

Inventarizace síťových zařízení

Pro inventarizaci veškerých síťových zařízení (typicky aktivních komunikačních prvků a koncových zařízení jako jsou uživatelská PC, notebooky, servery a síťové tiskárny) se využívají dva druhy nástrojů:

¹<https://github.com/ytti/oxidized>

²Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

³<http://www.eduroam.cz>

⁴<http://freeradius.org>

⁵Cisco Prime Infrastructure verze 3.10 pro 4000 uzlů provozovaný ve virtualizovaném prostředí.

⁶Dva bezdrátové řadiče Cisco Wireless Controller Cisco Catalyst 9800-40.

- registrační systém Sauron⁷ v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet⁸ v prostředí kolejní sítě (včetně funkce řízení přístupu oprávněných uživatelů do sítě na základě konfigurace kolejních DHCP/DNS serverů a pravidel na centrálním kolejním firewallu)
- on-line systémy NAV⁹, který na základě periodicky získávaných informací z aktivních komunikačních prvků pomocí protokolů SNMP a CDP poskytuje informace o zařízeních připojených do sítě (např. počty, typy a verze OS aktivních prvků, informace o topologii sítě, VLAN, IP podsítích, bezdrátových SSID, mapování MAC adres na IP adresy, připojení MAC/IP adres za konkrétními fyzickými porty jednotlivých přepínačů, informace o SMB atd.¹⁰) s možností pokročilého vyhledávání (např. nalezení fyzického připojení zařízení s danou IP/MAC adresou, nalezení duplicitních MAC/IP adres apod.), včetně uchovávání stavové historie.

Monitorování provozu

Provozní trendy

Pro sledování non-stop dostupnosti na úrovni služeb se používá systém Nagios¹¹, který je současně také využíván pro monitorování dostupnosti všech aktivních komunikačních prvků a služebních/management serverů, včetně konfigurace automatického upozorňování/eskalace e-mailem při detekci problémové/chybové situace.

Pro sledování non-stop dostupnosti na úrovni služeb pro systém VoIP ZČU se používá systém Nagios, který je využíván pro monitorování dostupnosti všech aktivních komunikačních prvků a služebních/management serverů systému VoIP ZČU, včetně konfigurace automatického upozorňování/eskalace e-mailem při detekci problémové/chybové situace.

Pro non-stop historii sledování základních L2 provozních charakteristik aktivních komunikačních prvků všech prostředí pomocí SNMP¹² (typicky zatížení CPU, obsazení operační paměti, stav napájecích zdrojů, teplota, počet BGP prefixů a stavové informace jednotlivých portů/rozhraní jako počet přenesených bytů/rámců/paketů, chybovost portů/rozhraní atd.) se používá systém NAV.

Pro sledování provozu na úrovni L3/L4 datových toků se využívá technologie NetFlow v9. NetFlow informace exportované ze směrovačů, linuxových firewallů (kolejný extranet) se zpracovávají pomocí software FTAS¹³.

Pro monitorování problémových provozních stavů se používá standardní mechanismus zpracování nevyžádaných deníkových zpráv generovaných aktivními prvky na bázi protokolu Syslog a SNMP trap, přičemž se navíc využívá i nadstavba Zenoss Core¹⁴ pro inteligentní korelaci trapů.

Bezpečnostní monitorování

Pro monitorování síťové bezpečnosti se jednak využívají standardní nástroje Syslog a SNMP trapy, které mohou být ještě dále inteligentně předzpracovány/filtrovány, korelovány a reportovány SIEM systémem zpracování Syslog hlášení z aktivních prvků OSSEC¹⁵ a pro SNMP trapy systémem Zenoss Core.

⁷<http://sauron.jyu.fi/>

⁸Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

⁹<https://nav.uninett.no/>

¹⁰Z bezpečnostních důvodů se však záměrně nevyužívají integrované služby manipulace se stavy portů přepínačů vyžadující SNMP přístup pro zápis.

¹¹<http://www.nagios.org/>

¹²Konfigurace aktivních prvků pouze v režimu pro čtení s povolenými IP adresami management stanic dle ACL.

¹³<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>

¹⁴<http://www.zenoss.com/solution/network-monitoring>

¹⁵<http://www.ossec.net/>

Přehled o anomáliích na úrovni automatické detekce podezřelých IPv4 datových toků podle analýzy NetFlow dat poskytuje software FTAS.

Vynucování bezpečnostní síťové přístupové politiky umožňující centralizované systémové zablokování přístupu problémových uživatelů do sítě či síťových služeb (blacklist) zejména na úrovni L2 VACL nebo L3 ACL případně ještě s kombinací vypnutí daného portu na přístupovém prvku (typicky nejbližší místu svého vzniku podle typu komunikačního prvku) je řízeno pomocí nástroje NetSpy¹⁶. Tento vlastní nástroj také poskytuje další potřebné podpůrné administrátorské funkce jako např. automatickou detekci neregistrovaných zařízení, vyhledání různých konfliktních síťových stavů, management VLAN/IP podsítí atd.

Vzdálený administrátorský přístup ke všem aktivním síťovým prvkům je zajištěn pouze¹⁷ pomocí SSH protokolu s autentizací/autorizací protokolem TACACS+ z předdefinovaných povolených bezpečných podsítí/IP adres. Management rozhraní L2 přepínačů je umístěno ve vyhrazené IP podsíti chráněné firewallem. Pro L3 přepínače/směrovače je konfigurována ochrana Control Plane Policing/CoPP, pokud tuto vlastnost podporují. AAA auditní informace o administrátorských přístupech ke konfigurovaným zařízením je k dispozici na TACACS+ serverech CIV ZČU.

¹⁶Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

¹⁷S výjimkou menšího počtu zastaralých přepínačů, které SSH nepodporují a jsou postupně podle finančních možností nahrazovány.