Příloha č. 2 Kupní smlouvy - technická specifikace
Výpočetní technika (III.) 020 - 2023

Vyplní se automaticky
Vyplní dodavatel

					[DOPLNÍ DODAVATEL]									[DOPLNÍ DODAVATEL]				
Položka	**Název**	**Množství**	**Měrná jednotka [MJ]**	**Popis**	**Obchodní název + typ + délka záruky**	**Odkaz na splnění požadavku Energy star nebo TCO Certified, ***	**Fakturace**	**Financováno z projektových finančních prostředků**	**Pokud financováno z projektových prostředků, pak DODAVATEL uvede NA FAKTURU: NÁZEV A ČÍSLO DOTAČNÍHO PROJEKTU**	**Obchodní podmínky NAD RÁMEC STANDARDNÍCH obchodních podmínek**	**Kontaktní osoba k převzetí zboží**	**Místo dodání**	**Termín dodání** (uveden v kalend. dnech od dojití výzvy Objednatele k plnění Smlouvy)	**MAXIMÁLNÍ CENA za měrnou jednotku (MJ) v Kč bez DPH**	**NABÍDKOVÁ CENA za měrnou jednotku (MJ) v Kč bez DPH**	**NABÍDKOVÁ CENA CELKEM v Kč bez DPH**	**VYHOVUJE / NEVYHOVUJE**	**CPV - výběr VÝPOČETNÍ TECHNIKA**
1	Přepínač	5	ks	Specifikace viz **Příloha č. 3 Kupní smlouvy - technická specifikace_Přepínače_VT (III.)-020-2023.pdf**	Cisco C9200L-48PXG-4X-E, C9200L-DNA-E-48-3Y, PWR-C5-1KWAC/2, rozšířená záruka 36 měsíců	NE	Společná faktura	ANO	Národní plán obnovy pro oblast vysokých škol pro roky 2022–2024 Registrační číslo projektu: NPO_ZČU_MSMT-16584/2022 Specifický cíl A: Transformace formy a obsahu VŠ vzdělávání Specifický cíl A1: Digitalizace vzdělávací činnosti a studijních agend	Viz **Příloha č. 6 Kupní smlouvy - požadavky na záruku za jakost_Přepínače_VT (III.)-020-2023.pdf**	Ing. Martin Šimek, Ph.D., Tel.: 37763 2834, 606 098 303	Univerzitní 20, 301 00 Plzeň, Centrum informatizace a výpočetní techniky - Servrovna, místnost UI 420	**310**	204 000,00 Kč	203 894,00 Kč	1 019 470,00 Kč	VYHOVUJE	32423000-4 - Síťové rozbočovače
2	VPN koncentrátor	2	ks	Specifikace viz **Příloha č. 4 Kupní smlouvy - technická specifikace_VPN koncentrátor_VT (III.)-020-2023.pdf**	Cisco FPR3130-NGFW-K9, rozšíření podpora (BxSxNBD) 36 měsíců	NE				Viz **Příloha č. 7 Kupní smlouvy - požadavky na záruku za jakost_VPN koncentrátor_VT (III.)-020-2023.pdf**			**90**	1 000 000,00 Kč	997 824,00 Kč	1 995 648,00 Kč	VYHOVUJE	32420000-3 - Síťová zařízení
3	Povýšení funkčních vlastností VPN koncentrátoru	2	ks		Povýšení funkčních vlastností VPN koncentrátoru	NE							**90**	300 000,00 Kč	298 666,00 Kč	597 332,00 Kč	VYHOVUJE	
4	Řídicí prvek bezdrátové sítě	2	ks	Specifikace viz **Příloha č. 5 Kupní smlouvy - technická specifikace_Přístupové prvky WiFi_VT (III.)-020-2023.pdf**	Cisco C9800-40-K9, C9800-AC-750W-R, rozšířená podpora (BxSxNBD) 36	NE				Viz **Příloha č. 8 Kupní smlouvy - požadavky na záruku za jakost_Přístupové prvky WiFi_VT (III.)-020-2023.pdf**			**200**	600 000,00 Kč	598 776,00 Kč	1 197 552,00 Kč	VYHOVUJE	
5	Povýšení funkčních vlastností řídicího prvku bezdrátové sítě	2	ks		Povýšení funkčních vlastností řídicího prvku bezdrátové sítě	NE							**200**	200 000,00 Kč	197 862,00 Kč	395 724,00 Kč	VYHOVUJE	
6	Bezdrátový přístupový bod typ A	110	ks		Cisco CW9164I-E, AIR-DNA-E-3Y, rozšířená záruka 36 měsíců	NE							**150**	21 450,00 Kč	21 365,00 Kč	2 350 150,00 Kč	VYHOVUJE	
7	Bezdrátový přístupový bod typ B	340	ks		Cisco C9115AXI-E, AIR-DNA-E-3Y, rozšířená záruka 36 měsíců	NE							**150**	17 100,00 Kč	16 988,00 Kč	5 775 920,00 Kč	VYHOVUJE	

Informace pro dodavatele: Pokud se dodavateli při zadávání jednotkových cen objeví text - "NEVYHOVUJE", znamená to překročení stanovené maximální nepřekročitelné nabídkové ceny, a to znamená nesplnění podmínek stanovených Zadavatelem. Pokud bude nabídka v této podobě podána Zadavateli, bude při posouzení vyřazena.

CELKOVÁ MAXIMÁLNÍ CENA za celou VZ v Kč BEZ DPH	**CELKOVÁ NABÍDKOVÁ CENA v Kč bez DPH**
13 393 500,00 Kč	**13 331 796,00 Kč**

V případě, že se dodavatel při předání zboží na některá uvedená tel. čísla nedovolá, bude v takovém případě volat tel. 377 631 320, 377 631 325.

Požadované technické parametry dodávky

Předmětem dodávky jsou aktivní síťové prvky dle technických podmínek uvedených níže.

- 5 ks 48 portový PoE+ přepínač s 10 Gb uplink porty s podporou mGig.

Tabulka povinných požadavků pro 48 portový PoE+ přepínač s 10 Gb uplink porty s podporou mGig (požadováno 5 ks)

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Třída zařízení	L2 přepínač
Formát zařízení	fixní konfigurace, rozšiřitelný na stohování, 1RU
Stohovatelný	ano, modulem
Stohování požadováno	ano
Minimální délka stohovacího kabelu	100 cm
Interní redundantní ventilátory	ano
Možnost instalovat interní redundantní napájecí zdroj	ano
Redundantní napájecí zdroj požadován	ne
Počet RJ-45 portů 10/100/1000	36
Počet RJ-45 portů mGig 10/5/2,5 Gb/s IEEE 802.3bz a 802.3an	12
Podpora PoE (IEEE 802.3af, 15,4 W/port)	ano
Podpora PoE+ (IEEE 802.3at, 30 W/port)	ano
Dostupný výkon pro napájení PoE portů	1000 W
Počet uplink portů a jejich typ	4x 10GE SFP+
Schopnost poskytovat PoE napájení připojeným zařízením i během restartu	ano
Vlastnosti stohování	
Vzájemné stohování všech modelů stejné řady s 1GE/10GE uplinky	ano
Počet přepínačů ve stohu	8
Automatická kontrola a sjednocení verze software přepínačů ve stohu	ano
Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením	ano
Seskupování portů (IEEE 802.3ad) mezi různými prvky stohu	ano
Kterýkoli prvek ve stohu může být řídícím prvkem stohu (1:N redundance)	ano
Protokoly fyzické vrstvy	
IEEE 802.3-2005	ano
IEEE 802.3ad	ano
Podpora "jumbo rámců"	ano
Protokoly spojové vrstvy	
IEEE 802.1D	ano
IEEE 802.1Q	ano
Počet aktivních VLAN	4000
IEEE 802.1X – Port Based Network Access Control	ano
IEEE 802.1s – multiple spanning trees	ano
IEEE 802.1w – Rapid Tree Spanning Protocol	ano
Per VLAN Rapid Spanning Tree (PVRST+) nebo ekvivalentní	ano
Detekce protilehlého zařízení	ano
Detekce parametrů protilehlého zařízení	ano

Protokol pro definici šířených VLAN	ano
Detekce jednosměrnosti optické linky	ano
STP root guard	ano
STP loop guard	ano
Možnost autorecovery po chybovém stavu	ano
Multicast/broadcast storm control – hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ano
Protokol IP	
IP alias (více IP sítí na jednom rozhraní)	ano
QoS	ano
Minimální počet HW QoS front	8
QoS classification – ACL, DSCP, CoS based	ano
QoS marking – DSCP, CoS	ano
QoS – Strict Priority Queue	ano
QoS Policing	ano
QoS i na stohovacím spoji	ano
DHCP relay	ano
Protokol IPv6	
Podpora IPv6 ACL	ano
Podpora IPv6 services (DNS, Telnet, SSH, Syslog, ICMP)	ano
Podpora IPv6 MLDv2 snooping	ano
Podpora IPv6 Port ACL	ano
Podpora IPv6 First Hop Security RA guard	ano
Podpora IPv6 First Hop Security DHCPv6 guard	ano
Podpora IPv6 First Hop Security IPv6 Binding Integrity Guard	ano
Směrování multicastu	
IGMPv2 snooping	ano
IGMPv3 snooping	ano
IPv6 MLDv1 & v2 snooping	ano
Bezpečnost	
ACL na rozhraní in/out	ano
ACL pro IP	ano
ACL pro ethernetové rámce	ano
IPv6 ACL	ano
Možnost definovat povolené MAC adresy na portu	ano
Možnost definovat maximální počet MAC adres na portu	ano
Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	ano
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ano
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ano
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ano
IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu	ano
IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači, sdílení ověření koncových stanic	ano
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ano

Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)	ano
Management	
CLI rozhraní	ano
SSHv2	ano
SSHv2 over IPv6	ano
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
SNMPv2	ano
SNMPv3	ano
Konzolová linka	ano
DNS klient	ano
NTP klient s MD5 autentizací	ano
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano
TACACS+ klient	ano
Port mirroring	ano
Vzdálený port mirroring	ano
Syslog	ano
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ano
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ano
Streaming telemetrie prostřednictvím NETCONF/XML	ano
Zařízení musí být možno spravovat používaným management nástrojem v celém možném rozsahu jeho funkcí bez omezení	ano
Měření zakončení a délky metalického kabelu (TDR)	ano
Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute)	ano
Přepínač si může automaticky zazálohovat a obnovit firmware včetně konfigurace z nadřazeného směrovače	ano
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	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.

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 síření 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/HTPS 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 Oxidized[1] periodicky alespoň jednou denně. Archivace (změn) historie konfigurací je udržována minimálně po dobu jednoho roku.

Pro hromadné konfigurace skupin zařízení se využívají systémy Netmanager[2], umožňující paralelní vykonávání příkazů.

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:

- registrační systém Sauron[3] v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet[4] 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 NAV[5], který na základě periodicky získávaných informací z aktivních komunikačních prvků pomocí protokolů SNMP a CDP poskytují 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.[6]) 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 Nagios[7], 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 SNMP[8] (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.

---

[1] https://github.com/ytti/oxidized

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

[3] http://sauron.jyu.fi/

[4] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

[5] https://nav.uninett.no/

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

[7] http://www.nagios.org/

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

Pro sledování provozu na úrovni L3/L4 datových toků se využívá technologie NetFlow v9. NetFlow informace exportované ze směrovačů, linuxových firewallů (kolejní extranet) se zpracovávají pomocí software FTAS[9].

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 Core[10] 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 OSSEC[11] a pro SNMP trapy systémem Zenoss Core.

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 nejblíže místu svého vzniku podle typu komunikačního prvku) je řízeno pomocí nástroje NetSpy[12]. 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 pouze[13] 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.

[9] 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

[10] http://www.zenoss.com/solution/network-monitoring

[11] http://www.ossec.net/

[12] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

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

Požadované technické parametry dodávky

Předmětem dodávky jsou **VPN koncentrátory (požadovány 2 ks)** dle technických podmínek uvedených níže.

Tabulka povinných požadavků pro VPN koncentrátor (požadovány 2 ks)

Požadovaná funkcionalita	**Minimální požadavky**
Základní vlastnosti	
Typ zařízení	Stavový firewall / VPN koncentrátor
Vysoká dostupnost/High Availability	V režimech active/passive i active/active
Formát zařízení	samostatné zařízení
Počet a typ rozhraní 1/10G dedikovaných pro management	1, SFP+
Počet a typ rozhraní 1/10/25G	8, SFP+/SFP28
Možnost rozšíření o moduly rozhraní s rychlostí 40 Gb/s	ano
Požadovaný počet a typ transceiverů	4 ks, 25GBase AOC, 7 m
Redundantní napájecí AC zdroj	ano
Napájecí zdroje vyměnitelné za chodu	ano
Výkonnostní parametry	
Počet současně otevřených spojení	5 miliónů
Počet nových spojení za vteřinu	600 tisíc
Agregovaná propustnost firewallu	35 Gb/s
Agregovaná propustnost VPN koncentrátoru (šifrování AES256)	9 Gb/s
Agregovaná propustnost IPSec VPN	12 Gb/s
Podporované funkce	
Stateful failover	V režimech active/active i active/passive
Počet VLAN	700
Provoz zařízení v režimu L3 (směrování)	ano
Provoz zařízení v režimu L2 (přepínání nebo transparentní)	ano
Seskupování portů IEEE 802.3ad	ano
Statické i dynamické směrování pro IPv4 (OSPF, BGP)	ano
Statické i dynamické směrování pro IPv6 (OSPFv3, MP-BGP)	ano
NAT64 a DNS64	ano
Policy based Routing	ano
Kontrola paketů TCP provozu s ochranou před útoky, jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	ano
Filtrace IPv4 a IPv6 provozu	ano
Inspekce IPv4 a IPv6 provozu	ano
Filtrace podle identity uživatele nebo jeho skupiny definované v AD	ano
Filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	ano
Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	ano
Bezpečnostní pravidla se zohledněním i identity uživatele	ano
Bezpečnostní pravidla se zohledněním informací o koncovém zařízení (typ, stav, apod.)	ano
API rozhraní pro sdílení kontextových informací s dalšími systémy	ano

RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano
DHCP relay	ano
Správa	
CLI rozhraní	ano
Přístup pomocí protokolu SSHv2	ano
Omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
Protokoly SNMPv2, SNMPv3	ano
Ověřování přístupu k zařízení pomocí RADIUS anebo TACACS+ protokolu	ano
Řízení přístupu na zařízení podle rolí administrátorů	ano
Vzdálené logování na syslog server	ano
Export statistik datových toků pomocí netflow, sflow nebo ekvivalentních	ano
Vzdálené správa konfigurace přes grafické rozhraní bez nutnosti instalace zvláštního SW	ano
Přehledy a statistiky na dohledové konzoli s filtrací podle času, typů incidentů, aplikací, koncových stanic	ano
Centrální dohledová konzole s vytvářením reportů manuálně a podle časového harmonogramu	ano
Centrální dohledová konzole s korelací událostí s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu apod.	ano
Funkcionalita VPN	
Počet souběžných šifrovaných spojení	10000
Definice specifických přístupových oprávnění (bezpečnostní politiky, ACL, atd.) podle identity nebo skupiny uživatele (např. v AD)	ano
Autentizace uživatelů pomocí lokální databáze	ano
Autentizace uživatelů pomocí RADIUS serveru	ano
Autentizace uživatelů pomocí Kerberos serveru	ano
Autentizace uživatelů pomocí digitálních certifikátů X. 509	ano
Autentizace uživatelů pomocí SmartCard	ano
Autentizace uživatelů pomocí RSA softID a RSA securID	ano
Podpora veřejných CA včetně možnosti zprovoznit CA přímo na firewallu	ano
Současná autentizace AAA a certifikátem	ano
CRL a OCSP pro kontrolu revokace certifikátu	ano
Přiřazení IPv6 adres klientům	ano

Další požadavky

- Součástí nabídky musí být samostatná položka **povýšení základních funkčních vlastností VPN koncentrátoru**, které bude zahrnovat plnou podporu provozu v režimu vysoké dostupnosti (HA režim active/active i active/standby včetně statefull switchover) a podpora šifrování AES.
- Zadavatel požaduje převod konfigurace a licencí klientského VPN software používaného VPN koncentrátoru na dodané zařízení bez ztráty funkcionality.
- 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.

..

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 síření 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/HTPS 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).

Popis současného stavu

ZČU v současné době používá jako VPN koncentrátor dvojici zařízení Cisco ASA 2130 v režimu active/standby. Aktivní i záložní VPN koncentrátor je připojen do dvojice zařízení Cisco Nexus 93180YC-EX využívající technologii vPC (Virtual Port Channel). Použitým typem optického rozhraní je v obou případech SFP+/SFP28. Jako klientský VPN software je použit Cisco Secure VPN Client

licencovaný pro 800 klientů. Pro autentizaci uživatelů je použit Kerberos anebo klientský certifikát vydaný certifikační autoritou ZČU a GEANT, dostupný buď ve formě souboru, nebo USB tokenu. Pro autorizaci uživatelů je použita dvojice RADIUS serverů, která slouží pro přidělování pevné IPv4 a IPv6 adresy, masky sítě a přístupových práv formou access-listu vybraným uživatelům.

Pro sledování provozu na úrovni L3/L4 datových toků se využívá technologie NetFlow v9. NetFlow informace exportované ze směrovačů, linuxových firewallů (kolejní extranet) a specializované FlowMon[1] sondy (kolejní intranet) se zpracovávají pomocí IPv4/IPv6 software FTAS[2].
AAA auditní informace o administrátorských přístupech ke konfigurovaným zařízením je k dispozici na TACACS+ serverech CIV ZČU.

[1] http://www.invea.cz/produkty-sluzby/flowmon/flowmon-sondy

[2] 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

Požadované technické parametry dodávky

Předmětem dodávky jsou aktivní síťové prvky dle technických podmínek uvedených níže.

- 2 ks centrálních řadičů bezdrátové sítě.
- 110 ks bezdrátových přístupových bodů typu A.
- 340 ks bezdrátových přístupových bodů typu B.

Tabulka povinných požadavků pro centrální řadič bezdrátové sítě (požadovány 2 ks)

Požadavek na funkcionalitu	**Minimální požadavky**
Základní vlastnosti	
Třída zařízení	centrální řadič bezdrátové sítě
Formát zařízení	samostatné zařízení
Počet a typ portů s rychlostí 10Gb/s	4, SFP+
Požadovaný počet a typ transceiverů	4 ks, 10GBase AOC, 3 m
Redundantní napájecí zdroj	ano
Podpora stávající báze instalovaných AP	ano
Podpora AP požadovaných v této ZD	ano
Výkonnostní parametry	
Počet současně připojitelných klientů	30000
Propustnost datového systému	40 Gb/s
Počet současně obsluhovaných AP	2000
Počet bezdrátových sítí WLAN	4000
Počet sítí VLAN	4000
Vysoká dostupnost řadiče	
Možnost redundance na úrovni řadičů a jejich portů	ano
Redundantní provoz v režimu active/standby	ano
Upgrade operačního systému bezvýpadkově za provozu	ano
Schopnost samostatného provozu (dočasné zrušení redundantního provozu)	ano
Vlastnosti správy bezdrátové sítě	
Integrovaný radio-resource management, spolupráce RRM mezi řadiči v clusteru	ano
Mobility management, L2/L3	ano
Automatizované řešení roamingu uživatelů v rámci AP na jednom řadiči i mezi 2 a více řadiči, L2/L3	ano
Optimalizace multicast provozu v bezdrátové síti (IGMP snooping)	ano
Podpora auto-provisioningu AP	ano
Automatizovaná správa frekvenčního pásma AP	ano
Integrované řešení návštěvnického přístupu	ano
Bezpečné oddělení návštěvnického provozu od zaměstnaneckého provozu	ano
Integrovaná správa návštěvnických účtů s možností definice jejich platnosti	ano
Webová autentizace návštěvníků	ano
Podpora možnosti tunelování uživatelských dat z AP až na řadič, možnost šifrování těchto uživatelských dat	ano
Podpora možnosti lokálního bridgování uživatelských dat přímo na příslušném AP	ano
Podpora 802.11e/WMM	ano
Diferenciace úrovní QoS	ano

Mechanismy řízení přístupu (Call Admission Control) pro hlasový a video provoz	ano
Podpora Video-streamingu se spolehlivým multicastem	ano
Podpora indoor a outdoor mesh sítí, současné připojení normálních a mesh AP k jednomu řadiči	ano
Podpora designu s centrálními řadiči a vzdálenými AP na pobočkách připojených přes WAN	ano
Existence programu/mechanismu výrobce pro validaci interoperability bezdrátových klientů třetích stran s infrastrukturou. Zahrnující inovativní funkce bezpečnosti, mobility, QoS, management. Alespoň pro klienty DELL, HP, Lenovo, Fujitsu, Nokia, BlackBerry apod.	ano
Bezpečnost	
Podpora 802.11i, respektive jeho implementací WPA2 včetně enterprise variant autentizace/šifrování	ano
Podpora Wi-Fi Protected Access 3 (WPA3)	ano
802.1X/EAP autentizace: PEAP, EAP-FAST, EAP-TLS, …	ano
Šifrování AES	ano
Integrovaný IDS systém pro detekci útoků na bezdrátovou síť (wireless IDS)	ano
Detekce cizích AP (Rogue AP) a klientů v AdHoc režimu	ano
Možnost vynuceného odpojení klientů od cizích AP	ano
Ochrana řídících rámců na AP a klientovi podle standardu IEEE 802.11w	ano
Centrální administrace správců s granularitou přístupových práv	ano
Spolupráce s cizími sítěmi podle standardu IEEE 802.11u	ano
Rychlý roaming klientů mezi AP podle standardu IEEE 802.11r	ano
Vysoká dostupnost AP	
Automatické zvýšení vysílacího výkonu okolních AP při výpadku AP	ano
Automatické přizpůsobení se bezdrátové sítě na základě indexu kvality radiového signálu	ano
Rychlá detekce selhání komunikace AP-řadič (pod 4 sekundy)	ano
Monitoring a měření kvality radiového signálu	
Vyhodnocování kvality signálu bezdrátové sítě v reálném čase a grafické vyobrazení	ano
Možnost detekce rušivých signálů (interference) a identifikace zdrojů interference na základě signatur	ano
Současná funkčnost AP pro přenos dat, detekci bezpečnostních incidentů a analýzu radiového spektra	ano
Troubleshooting radiového signálu a automatické řešení problému rušivého signálu	ano
Možnost nastavovat prahové hodnoty pro úroveň kvality signálu bezdrátové sítě	ano
Automatické spouštění alarmů na základě překročení prahových hodnot kvality signálu	ano
Management	
CLI rozhraní	ano
Web rozhraní	ano
Přístup přes SSHv2	ano
Omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
SNMPv2 a SNMPv3	ano
Podpora NETCONF/YANG	
Export datových toků pomocí Netflow nebo Sflow	ano
Sériová konzolová linka	ano
RADIUS klient pro AAA (autentizace, autorizace, accounting) bezdrátových klientů	ano
TACACS+ klient pro přístup	ano
Syslog	ano

Tabulka povinných požadavků pro bezdrátový přístupový bod typu A (požadováno 110 ks)

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Typ zařízení	bezdrátový přístupový bod
Montáž	na strop
Montážní konzole součástí dodávky	ne
Rádiové rozhraní pro pásmo 2,4 GHz	ano
Rádiové rozhraní pro pásmo 5 GHz	ano
Rádiové rozhraní pro pásmo 6 GHz	ano
Samostatné rádio pro monitorování 2,4, 5 a 6 GHz RF spektra – detailní spektrální analýza, detekce útoků na bezdrátovou síť, lokalizace klientů	ano
Rozhraní 100/1000/2500 Mb/s kompatibilní s 802.3bz	ano
Podpora IEEE 802.3bt/at napájení z přepínače nebo injektoru	ano
Typ antén	integrované pro všechna pásma
Podpora centralizovaných řadičů bezdrátové sítě poptávaných v této ZD	ano
Podpora systému centralizované správy bezdrátových řadičů	ano
Výkonnostní parametry	
Fyzická přenosová rychlost celé bezdrátové části	7 Gb/s
Protokoly fyzické vrstvy	
IEEE 802.11a/b/g/n/ac/ax a Wi-Fi 6E	ano
MIMO (Multiple Input Multiple Output) v pásmu 2,4/5/6 GHz	2x2:2/4x4:4/4x4:4
Podpora Multiuser Multiple-Input Multiple-Output (MU MIMO)	ano
Maximal ratio combining (MRC)	ano
Agregace rámců A-MPDU a A-MSDU	ano
Dynamický výběr volné frekvence DFS	ano
Podpora 20 MHz a 40 MHz kanálův pásmu 2,4 GHz	ano
Podpora 80 MHz kanálů v pásmu 5 GHz	ano
Podpora 160 MHz kanálů v pásmu 6 GHz	ano
Podpora BSS Coloring	ano
Optimalizace fáze vysílaného bezdrátového signálu směrem ke klientům	ano
Podpora mechanismu pro nucené přepojení klientů mezi pásmy	ano
Podpora současného vysílání a příjmu více klientů najednou (OFDMA)	ano
Hardwarová podpora spektrální analýzy (detekce zdroje rušivého signálu)	ano
Hardwarová podpora rozpoznání zdroje rušivého signálu podle otisku	ano
Výpočet závažnosti dopadu interference na kvalitu radiového signálu	ano
Minimální počet inzerovaných SSID (BSSID)	8/rádiové rozhraní
Rádio podporující BLE 5.1 a Target Wake Time (TWT)	ano
Bezpečnost	
Podpora WPA3	ano
Certifikát s lokální platností pro nasazení PKI	ano
Fyzické zabezpečení/zamknutí k okolním pevným částem	ano
Management	
CLI rozhraní	ano
SSHv2	ano
Konzolová linka	ano
Detekce a monitorování problémů bezdrátové sítě odchytáváním provozu	ano

Tabulka povinných požadavků pro bezdrátový přístupový bod typu B (požadováno 340 ks)

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Typ zařízení	bezdrátový přístupový bod
Montáž	na strop
Montážní konzole součástí dodávky	ne
Rádiové rozhraní pro pásmo 2,4 GHz	ano
Rádiové rozhraní pro pásmo 5 GHz	ano
Rozhraní 100/1000/2500 Mb/s kompatibilní s 802.3bz	ano
Podpora IEEE 802.3bt/at napájení z přepínače nebo injektoru	ano
Typ antén	integrované pro všechna pásma
Podpora stávajících centralizovaných řadičů bezdrátové sítě	ano
Podpora centralizovaných řadičů bezdrátové sítě poptávaných v této ZD	ano
Podpora systému centralizované správy bezdrátových řadičů	ano
Výkonnostní parametry	
Fyzická přenosová rychlost celé bezdrátové části	5 Gb/s
Protokoly fyzické vrstvy	
IEEE 802.11a/b/g/n/ac/ax	ano
MIMO (Multiple Input Multiple Output)	4x4:4
Podpora Multiuser Multiple-Input Multiple-Output (MU-MIMO)	ano
Maximal ratio combining (MRC)	ano
Agregace rámců A-MPDU a A-MSDU	ano
Dynamický výběr volné frekvence DFS	ano
Podpora 20 MHz a 40 MHz kanálův pásmu 2,4 GHz	ano
Podpora 80 MHz a 160 MHz kanálů v pásmu 5 GHz	ano
Optimalizace fáze vysílaného bezdrátového signálu směrem ke klientům (Beam Forming)	ano
Podpora mechanismu pro nucené přepojení klientů mezi pásmy	ano
Podpora současného vysílání a příjmu více klientů najednou (OFDMA)	ano
Minimální počet inzerovaných SSID (BSSID)	8/rádiové rozhraní
Rádio podporující BLE 5.0 a Target Wake Time (TWT)	ano
Bezpečnost	
Podpora WPA3	ano
Certifikát s lokální platností pro nasazení PKI	ano
Fyzické zabezpečení/zamknutí k okolním pevným částem	ano
Management	
CLI rozhraní	ano
SSHv2	ano
Konzolová linka	ano
Detekce a monitorování problémů bezdrátové sítě odchytáváním provozu a jeho zasíláním do analyzátoru (například Wireshark)	ano

Další technické požadavky

- Součástí nabídky musí být samostatná položka **povýšení základních funkčních vlastností centrálního řadiče bezdrátové sítě**, které bude zahrnovat plnou podporu provozu v režimu vysoké dostupnosti (HA režim active/standby včetně statefull switchover) a podporu šifrování uživatelských dat z AP až na řadič.

- 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.

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 síření 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/HTPS 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 Oxidized[1] periodicky alespoň jednou denně. Archivace (změn) historie konfigurací je udržována minimálně po dobu jednoho roku.

Pro hromadné konfigurace skupin zařízení se využívají systémy Netmanager[2], umožňující paralelní vykonávání příkazů.

Správa bezdrátové sítě

Na ZČU je provozována bezdrátová síť eduroam[3], 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 freeRADIUS[4]. Pro správu a konfiguraci bezdrátových přístupových bodů je využíváno centralizované řešení. Jako centrální prvky jsou použity čtyři bezdrátové řadiče[5] pracující v režimu active/standby, které jsou schopny současně spravovat až 1500 AP. K udržení konzistentní konfigurace obou bezdrátových řadičů je používán specializovaný software[6].

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:

- registrační systém Sauron[7] v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet[8] 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 NAV[9], který na základě periodicky získávaných informací z aktivních komunikačních prvků pomocí protokolů SNMP a CDP poskytují 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

[1] https://github.com/ytti/oxidized
[2] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.
[3] http://www.eduroam.cz
[4] http://freeradius.org
[5] Dva bezdrátové řadiče Cisco Wireless LAN Controller (WLC) 5520 pro 1500 AP.
[6] Cisco Prime Infrastructure verze 3.10 pro 4000 uzlů provozovaný ve virtualizovaném prostředí.
[7] http://sauron.jyu.fi/
[8] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.
[9] https://nav.uninett.no/
[10] Z bezpečnostních důvodů se však záměrně nevyužívají integrované služby manipulace se stavy portů přepínačů vyžadující SNMP přístup pro zápis.

Pro sledování non-stop dostupnosti na úrovni služeb se používá systém Nagios[11], 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 SNMP[12] (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 (kolejní extranet) se zpracovávají pomocí software FTAS[13].

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 Core[14] 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 OSSEC[15] a pro SNMP trapy systémem Zenoss Core.

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 nejblíže místu svého vzniku podle typu komunikačního prvku) je řízeno pomocí nástroje NetSpy[16]. 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 pouze[17] 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.

---

[11] http://www.nagios.org/

[12] Konfigurace 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/

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

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

Požadavky na záruku za jakost

- Zadavatel požaduje originální a nová zařízení určená pro evropský trh, licencovaná ve jménu Zadavatele tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce.
- Dodavatel je povinen s dodávkou doložit oficiální potvrzení zastoupení výrobce o určení dodávaných dílů a zařízení (seznamu výrobních čísel). Výrobní čísla svázaná s identitou koncového zákazníka (ZČU) doloží Dodavatel na požádání.
- Všechna dodaná síťová zřízení musí být 100% kompatibilní se zařízeními používanými v současné době, spolupracovat s jejich konfigurací a nastavením a musí zajistit kontinuální provoz stávající počítačové sítě bez vynaložení dodatečných nákladů.
- Dodavatel poskytne zadavateli po dobu trvání servisní podpory (36 měsíců) autorizovaný přístup pro stahování nových verzí programového vybavení (SW releases) a autorizovaný přístup do servisního a asistenčního centra výrobce pro řešení vzniklých problémů.
- Dodavatel se dále zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení.
- V databázi výrobce musí být Zadavatel veden jako první uživatel zboží.
- Nabídka bude zahrnovat záruku za jakost po dobu 36 měsíců od podpisu dodacích listů oběma smluvními stranami.
- Záruka za jakost bude zahrnovat nárok na bezplatnou instalaci všech nových verzí firmware.

Požadavky na záruku za jakost

- Zadavatel požaduje originální a nová zařízení, licencovaná ve jménu zákazníka tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce.
- Dodavatel je povinen s dodávkou doložit oficiální potvrzení zastoupení výrobce o určení dodávaných dílů a zařízení (seznamu výrobních čísel) pro koncového zákazníka ZČU, pokud o to zadavatel požádá.
- Všechna dodaná síťová zřízení musí být 100% kompatibilní se zařízeními používanými v současné době, spolupracovat s jejich konfigurací a nastavením a musí zajistit kontinuální provoz stávající počítačové sítě bez vynaložení dodatečných nákladů.
- Dodavatel poskytne zadavateli po dobu trvání servisní podpory autorizovaný přístup pro stahování nových verzí programového vybavení (SW releases) a autorizovaný přístup do servisního a asistenčního centra výrobce pro řešení vzniklých problémů.
- Dodavatel se dále zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení.
- Nabídka bude zahrnovat záruku za jakost po dobu 36 měsíců od podpisu dodacích listů oběma smluvními stranami a rozšířenou podporu po dobu záruky.
- Rozšířená podpora bude zahrnovat alespoň:
  - povýšení základních funkčních vlastností požadovaných v zadávací dokumentaci,
  - výměnu vadného dílu nebo zařízení do následujícího pracovního dne po ohlášení závady (8x5xNBD),
  - nárok na bezplatnou instalaci všech nových verzí firmware v rozsahu dodané licence,
  - nárok na přímou podporu výrobce v případě softwarových nebo hardwarových závad, jejichž řešení nebude v silách dodavatele.
- Veškeré podmínky a kritéria poptávky musí být splněny.

Požadavky na záruku za jakost

- Zadavatel požaduje originální a nová zařízení určená pro evropský trh, licencovaná ve jménu Zadavatele tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce.
- Dodavatel je povinen s dodávkou doložit oficiální potvrzení zastoupení výrobce o určení dodávaných dílů a zařízení (seznamu výrobních čísel). Výrobní čísla svázaná s identitou koncového zákazníka (ZČU) doloží Dodavatel na požádání.
- Všechna dodaná síťová zřízení musí být 100% kompatibilní se zařízeními používanými v současné době, spolupracovat s jejich konfigurací a nastavením a musí zajistit kontinuální provoz stávající počítačové sítě bez vynaložení dodatečných nákladů.
- Dodavatel se dále zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení.
- V databázi výrobce musí být Zadavatel veden jako první uživatel zboží.
- Součástí nabídky musí být doživotní záruka na bezdrátové přístupové body, která zahrnuje:
  - výměnu vadného dílu nebo zařízení do 10 pracovních dnů od nahlášení závady zástupcem Zadavatele,
  - nárok na bezplatnou instalaci všech nových verzí firmware.
- Nabídka bude zahrnovat záruku za jakost po dobu 36 měsíců od podpisu dodacích listů oběma smluvními stranami a rozšířenou podporu po dobu záruky na centrální řadič bezdrátové sítě, která obsahuje:
  - povýšení základních funkčních vlastností požadovaných v zadávací dokumentaci,
  - výměnu vadného dílu nebo zařízení do následujícího pracovního dne po ohlášení závady (8x5xNBD),
  - nárok na bezplatnou instalaci všech nových verzí firmware v rozsahu dodané licence,
  - nárok na přímou podporu výrobce v případě softwarových nebo hardwarových závad, jejichž řešení nebude v silách dodavatele.
- Veškeré podmínky a kritéria poptávky musí být splněny.

SEZNAM PODDODAVATELŮ

Název veřejné zakázky	Výpočetní technika (III.) 020 - 2023

Poddodavatel[1] - Název/Obchodní firma	IČO	Sídlo
Dodavatel nehodlá využít pro plnění Předmětu plnění žádné poddodavatele.		

Využití poddodavatele je podmíněno předchozím souhlasem Objednatele.

[1] Za poddodavatele se považuje osoba odlišná od Dodavatele, prostřednictvím níž bude Dodavatel poskytovat Předmět plnění nebo jeho část (poddodavatelem tedy je třetí osoba, která se aktivně zapojí do plnění (poskytne nějakou činnost), tj. např. zajišťuje služby přepravy Předmětu plnění od Dodavatele k Objednateli, služby instalace Předmětu plnění v místě plnění, montáž, stavební práce, školení, servisní či revizní služby apod.).