

Příloha č. 1
Technická specifikace

Specifikace předmětu veřejné zakázky

1. 110 ks WAN směrovačů - typ A = Cisco směrovač ISR4331-SEC/K9

Pro splnění požadavků zadavatele, definovaných v technické specifikaci (Příloha č.1) je navržen směrovač Cisco ISR4331 se Security bundle licencí. Směrovač plně splňuje definované požadavky:

- Směrovač má modulární architekturu s možností přidávat moduly rozhraní dle budoucí potřeby.
- Směrovač podporuje šifrování aplikačního provozu s využitím technologie IPSec a s podporou Suite-B šifrovacích algoritmů definovaných v RFC 6379. Směrovač má integrovanou hardwarovou podporu šifrování.
- Směrovač má plnou podporu IP adresace a směrovacích protokolů pro IPv4 a IPv6 s minimálními požadavky na směrovací protokoly OSPFv2/v3, BGPv4 a Multiprotocol BGP.
- Směrovač plně podporuje pokročilé mechanismy pro řízení kvality služeb (QoS) včetně Hierarchical QoS, klasifikace provozu, markování provozu (DSCP, COS) a vyčlenění šířky pásma provozu v jednotlivých aplikačních kategoriích a definici prioritní fronty pro provoz IP telefonie.
- Směrovač má plnou podporu IPv6 služeb jako jsou DNS, Telnet/SSH, DHCP, Multicast a QoS. Směrovač podporuje technologii DualStack (IPv4 a IPv6).
- Směrovač plně podporuje monitorování aplikačních toků (všech paketů) s využitím technologie NetFlow a obsahuje nástroje pro on-line měření kvality přenosové infrastruktury.

Přesná funkční specifikace WAN směrovače typu A = Cisco směrovač ISR4331-SEC/K9 je uvedena v následující tabulce.

Tabulka 1 Funkční specifikace WAN směrovače- typ A

Požadovaná funkcionality/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplň Uchazeč dle nabízeného zařízení
110 ks WAN směrovačů typ A		
Výrobce zařízení	Uvedení výrobce	Cisco Systems, Inc.
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uveďte Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	ISR4331-SEC/K9
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	http://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-732542.html
Typ zařízení	Směrovač	Směrovač
Formát zařízení	Modulární	Modulární

Požadovaná funkcionálnita/vlastnost	Způsob splnění požadované funkcionálnity/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
Požadovaný počet portů GigabitEthernet	2x10/100/1000Base-TX, 1x1000BASE-X s volitelným fyzickým rozhraním	1x 10/100/1000Base-TX / SFP (1000BASE-X) 1x 10/100/1000Base-TX 1x SFP (1000BASE-X)
Interní AC napájecí zdroj	ANO	ANO
Min. 3 volné sloty pro rozšiřující moduly	ANO	ANO
Možnost instalovat LAN modul s min. 24x 10/100/1000Base-TX porty s podporou PoE+ napájení	ANO	ANO
Směrování IPv4	ANO	ANO
Směrování IPv6	ANO	ANO
OSPFv2	ANO	ANO
BGPv4	ANO	ANO
Podpora 4 byte AS numbers in BGP	ANO	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
GRE (Generic Routing Encapsulation)	ANO	ANO
Policy-based routing podle ACL	ANO	ANO
IP Multicast (PIM SSM, PIM SM)	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
uRPF	ANO	ANO
First Hop Redundancy Protokol pro IPv6	ANO	ANO
OSPFv3	ANO	ANO
MP BGP	ANO	ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO	ANO
Minimální počet oddělených (nezávislých) směrovacích tabulek	30	ANO, 30 a více
IPv6 Multicast (MLDv1 & v2)	ANO	ANO
IPv6 Multicast (PIM SM, PIM SSM)	ANO	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking - DSCP, CoS	ANO	ANO
QoS Shaping and Policing	ANO	ANO
Class Based and Priority queuing	ANO	ANO
Rate Limiting	ANO	ANO
Hierarchical QoS	ANO, min. 3 úrovně	ANO, 3 úrovně
RSVP	ANO	ANO
Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)	ANO	ANO
ACL na rozhraní IN/OUT	ANO	ANO
Zone-based firewall	ANO	ANO
IPSec AES-GCM-256	ANO	ANO
Hardwarová akcelerace šifrování pro IPSec AES-GCM-256	ANO	ANO
Minimální propustnost směrovače (IMIX provoz) při aktivovaných službách IPSec šifrování a QoS	90Mb/s	ANO, 92Mb/s
Možnost zvýšit propustnost směrovače (IMIX provoz) při aktivovaných službách IPSec šifrování a QoS, např. formou licence	ANO, min. na 270Mb/s	ANO, 279Mb/s
IKEv2	ANO	ANO
SHA-2 (SHA-256, SHA-512)	ANO	ANO
Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami	ANO	ANO

Požadovaná funkcionálnita/vlastnost	Způsob splnění požadované funkcionálnity/vlastnosti	Doplňí Uchazeč dle nabízeného zařízení
Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů	ANO	ANO
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	ANO	ANO
Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	ANO	ANO
Interní nástroje pro debugging procházejícího provozu	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
SNMPv2/v3	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
NTPv3 server	ANO	ANO

2. 185 ks přístupový LAN přepínač 48 portů a 108 ks přístupový LAN přepínač 24 portů = Cisco přepínač WS-C3650-48PS-S a Cisco přepínač WS-C3650-24PS-S

Pro splnění požadavků zadavatele, definovaných v technické specifikaci (Příloha č.1) jsou navrženy LAN přepínače Cisco Catalyst 3650 s IP Base licencí v provedení 48-portovém a 24-portovém. Přepínače plně splňují definované požadavky:

- Přístupový LAN přepínač má stohovatelnou architekturu.
- Přístupový LAN přepínač podporuje standardy pro napájení po Ethernetu (PoE) dle norem 802.3af a 802.3at.
- Přístupový LAN přepínač podporuje zabezpečení portů dle standardu 802.1x.
- Přístupový LAN přepínač podporuje optimalizaci IP multicast provozu (IGMP a MLD snooping).
- Přístupový LAN přepínač umožňuje zabezpečení na L2 portech proti podvržení zdrojové MAC a IP adresy a ochranu proti neautorizovaným službám DHCP.
- Přístupový LAN přepínač plně podporuje řízení kvality služeb (QoS) s možností definice frontování, klasifikace provozu, markování provozu (DSCP, COS) s možností omezení a vyčlenění šířky pásma provozu v jednotlivých kategoriích a definici prioritní fronty.
- Přístupový LAN přepínač plně podporuje IPv6 protokoly a služby jako jsou DNS, Telnet/SSH, DHCP, ACL a QoS. Přepínač podporuje funkcionalitu IPv6 First Hop Security (minimálně IPv6 RA guard a DHCPv6 snooping).
- Přístupový LAN přepínač plně podporuje monitorování aplikačních toků (všech paketů) s využitím technologie NetFlow pro účely detekce anomálních datových toků a bezpečnostních útoků.

Přesná funkční specifikace přístupových LAN přepínačů = Cisco přepínačů WS-C3650-48PS-S a Cisco přepínač WS-C3650-24PS-S je uvedena v následujících tabulkách.

Tabulka 2 Funkční specifikace přístupového LAN přepínače – 48 portů

Požadovaná funkcionální/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplň Uchazeč dle nabízeného zařízení
185 ks LAN přepínačů - 48 portů		
Výrobce zařízení	Uvedení výrobce	Cisco Systems, Inc.
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	WS-C3650-48PS-S
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3650-series-switches/datasheet-c78-729449.html
Typ přepínače	L3 přepínač	L3 přepínač
Formát přepínače	Stohovatelný nebo modulární	Stohovatelný
V případě stohovatelného přepínače možnost rozšířit přepínač o dedikovaný stohovací modul	ANO	ANO

Požadovaná funkcionální/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplň Uchazeč dle nabízeného zařízení
Minimální počet zařízení ve stohu/min. počet slotů v šasi	8	9
Minimální kapacita sběrnice stohu/min. kapacita per slot modulárního šasi	160Gb/s	160Gb/s
Stateful Switch Over v rámci stohu nebo šasi	ANO	ANO
Počet portů 10/100/1000 Base-TX s PoE napájením	48	48
Minimální počet 1GE uplink portů s volitelným fyzickým rozhraním	4	4
Velikost MAC address tabulky	30000	ANO – až 32000
IEEE 802.3ad (Link Aggregation)	ANO	ANO
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	64	ANO - až 128
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	1000	ANO - až 1024
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	ANO
RADIUS CoA	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora jumbo rámců (min. 9198 bytes)	ANO	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2	ANO	ANO
OSPFv3	ANO	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
Reverse path check (uRPF)	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
DHCP relay	ANO	ANO
Minimální počet HW QoS front	8	8
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking - DSCP, CoS	ANO	ANO
QoS - Strict Priority Queue	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS Policing	ANO	ANO
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO	ANO
IPv6 services (Telnet, SSH, Syslog, DHCP)	ANO	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping)	ANO	ANO
IPv6 ACL	ANO	ANO
Možnost definovat povolené MAC adresy na portu	ANO	ANO
PACL, VAACL	ANO	ANO
IEEE 802.1ae na 1GE uplink portech	ANO	ANO

Požadovaná funkcionálnita/vlastnost	Způsob splnění požadované funkcionálnity/vlastnosti	Doplň Uchazeč dle nabízeného zařízení
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	ANO
IEEE 802.3af	ANO	ANO
IEEE 802.3at	ANO	ANO
Minimální PoE budget	390W	390W
IEEE 802.3az	ANO	ANO
Možnost automatické aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO
Integrovaný WLAN kontrolér	ANO	ANO
Vyhodnocování kvality signálu bezdrátové sítě v reálném čase, zpracování a reakce na informace o rušivých signálech (interference) z AP	ANO	ANO
Podpora 802.11i, respektive jeho implementací WPA a WPA2 včetně enterprise variant autentizace/šifrování	ANO	ANO
Aplikace QoS per WLAN AP, WLAN SSID, WLAN klient	ANO	ANO
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	ANO	ANO
Zrcadlení provozu na úrovni jednotlivých fyzických rozhraní i virtuálních sítí (VLAN) do monitorovacího rozhraní (ekvivalent funkce SPAN)	ANO	ANO
Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
DHCP server	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
SNMPv2/v3	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
NTPv3 server	ANO	ANO

Tabulka 3 Funkční specifikace přístupového LAN přepínače – 24 portů

Požadovaná funkcionálnita/vlastnost	Způsob splnění požadované funkcionálnity/vlastnosti	Doplň Uchazeč dle nabízeného zařízení
108 ks LAN přepínačů - 24 portů		
Výrobce zařízení	Uvedení výrobce	Cisco Systems, Inc.
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	WS-C3650-24PS-S

Požadovaná funkcionální/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplň Uchazeč dle nabízeného zařízení
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3650-series-switches/datasheet-c78-729449.html
Typ přepínače	L3 přepínač	L3 přepínač
Formát přepínače	Stohovatelný nebo modulární	Stohovatelný
V případě stohovatelného přepínače možnost rozšířit přepínač o dedikovaný stohovací modul	ANO	ANO
Minimální počet zařízení ve stohu/min. počet slotů v šasi	8	9
Minimální kapacita sběrnice stohu/min. kapacita per slot modulárního šasi	160Gb/s	160Gb/s
Stateful Switch Over v rámci stohu nebo šasi	ANO	ANO
Počet portů 10/100/1000 Base-TX s PoE napájením	24	24
Minimální počet 1GE uplink portů s volitelným fyzickým rozhraním	4	4
Velikost MAC address tabulky	30000	ANO – až 32000
IEEE 802.3ad (Link Aggregation)	ANO	ANO
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	64	ANO - až 128
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	1000	ANO - až 1024
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	ANO
RADIUS CoA	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora jumbo rámců (min. 9198 bytes)	ANO	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2	ANO	ANO
OSPFv3	ANO	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
Reverse path check (uRPF)	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
DHCP relay	ANO	ANO
Minimální počet HW QoS front	8	8
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking - DSCP, CoS	ANO	ANO
QoS - Strict Priority Queue	ANO	ANO

Požadovaná funkcionální/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplň Uchazeč dle nabízeného zařízení
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS Policing	ANO	ANO
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO	ANO
IPv6 services (Telnet, SSH, Syslog, DHCP)	ANO	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping)	ANO	ANO
IPv6 ACL	ANO	ANO
Možnost definovat povolené MAC adresy na portu	ANO	ANO
PACL, VACL	ANO	ANO
IEEE 802.1ae na 1GE uplink portech	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	ANO
IEEE 802.3af	ANO	ANO
IEEE 802.3at	ANO	ANO
Minimální PoE budget	390W	390W
IEEE 802.3az	ANO	ANO
Možnost automatické aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO
Integrovaný WLAN kontrolér	ANO	ANO
Vyhodnocování kvality signálu bezdrátové sítě v reálném čase, zpracování a reakce na informace o rušivých signálech (interference) z AP	ANO	ANO
Podpora 802.11i, respektive jeho implementací WPA a WPA2 včetně enterprise variant autentizace/šifrování	ANO	ANO
Aplikace QoS per WLAN AP, WLAN SSID, WLAN klient	ANO	ANO
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	ANO	ANO
Zrcadlení provozu na úrovni jednotlivých fyzických rozhraní i virtuálních sítí (VLAN) do monitorovacího rozhraní (ekvivalent funkce SPAN)	ANO	ANO
Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
DHCP server	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
SNMPv2/v3	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
NTPv3 server	ANO	ANO

3. Komunikační moduly

K implementaci síťových prvků je počítáno s 325 transceiver moduly.

V současné době je v rámci LAN provozováno 285ks optických 1000Base-SX transceiver modulů od společnosti Cisco Systems – typové označení GLC-SX-MM a GLC-SX-MMD na duplexních multimodových trasách.

Dále pak 40ks optických transceiver modulů 1000Base-LX/LH od společnosti Cisco Systems – typové označení GLC-LH-SM a GLC-LH-SMD na duplexních singlemodových trasách.

Dle doporučení Zadavatele jsou stávající transceivery použité v navrženém řešení. Všechny výše uvedené transceiver moduly jsou plně kompatibilní (plná podpora výrobcem) s navrženým směrovačem Cisco ISR4331-SEC/K9a navrženými LAN přepínači Cisco WS-C3650-48PS-S a Cisco WS-C3650-24PS-S.

Veškerá optická propojení tak budou realizována prostřednictvím stávajících transceiver modulů, což představuje pro Zadavatele nulové náklady na pořízení a ochranu dříve vynaložených investic do těchto transceiver modulů.

Požadovaná funkcionální/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplň Uchazeč dle nabízeného zařízení
40 ks Singlemode SFP (LC) transceivery		
Výrobce zařízení	Uvedení výrobce	Cisco Systems, Inc.
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	GLC-LH-SM GLC-LH-SMD
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-gbic-sfp-modules/product_data_sheet0900aecd8033f885.html
285 ks Multimode SFP (LC) transceivery		
Výrobce zařízení	Uvedení výrobce	Cisco Systems, Inc.
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	GLC-SX-MM GLC-SX-MMD
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-gbic-sfp-modules/product_data_sheet0900aecd8033f885.html

4. Nástroj pro řízení přístupu do sítě a podpůrné aplikace

Pro řízení přístupu a kontrolu politik pro drátové, bezdrátové a VPN platformy je využito řešení společnosti Cisco Systems – Cisco Identity Services Engine (Cisco ISE).

Podpůrné aplikace zajišťující jednoduchou správu MAC adres a lokalizaci zařízení jsou realizovány prostřednictvím aplikací od společnosti Alef Nula. Správa MAC adres je řešena aplikací Alefit MAB Keeper, lokalizace zařízení prostřednictvím aplikace Alefit Office Locator.

A) 2 ks zařízení pro řízení přístupu včetně podpory pro 10.000 současných koncových zařízení = Cisco ISE-VM-K9=

Pro řízení přístupu a kontrolu politik pro drátové, bezdrátové a VPN platformy je využito řešení společnosti Cisco Systems – Cisco Identity Services Engine (Cisco ISE). Nasazení Cisco ISE bude v podobě virtuální appliance do virtualizačního prostředí zadavatele. Pro zajištění vysoké dostupnosti bude nasazena dvojice Cisco ISE appliance v HA módu. Podporu 10 000 současných koncových zařízení zajišťuje licence L-ISE-BSE-10K= (Cisco Identity Services Engine 10000 EndPoint Base License).

Zajištění síťové administrace prostřednictvím TACACS+ protokolu zajišťuje licence L-ISE-TACACS= (Cisco ISE Device Admin License).

Využití řešení Cisco Identity Services Engine zvyšuje úroveň síťového zabezpečení v LAN/ WIFI/ VPN komunikační infrastruktuře prostřednictvím:

- Identifikace koncového zařízení
- Autentizace koncových zařízení (uživatelů)
- Autorizace koncových zařízení (uživatelů)
- Logování přístupů připojovaných zařízení (uživatelů)

Mezi další vlastnosti Cisco ISE, patří:

- Schopnost registrovat zařízení interních/externích zaměstnanců
- Automatický proces vydávání certifikátů na registrované zařízení
- Nastavení síťových profilů na zařízeních a vydávání certifikátů
- Možnost kontroly, zda zařízení splňuje definované bezpečnostní parametry (kontrola může být provedena dotazem na externí aplikaci, poskytující tyto údaje)
- zpracování požadavků zasílaných protokoly RADIUS (NAC) a TACACS+ (síťová administrace).
- Centrální správa (V případě výpadku centrálního serveru nebude ohrožen chod sítě).

Tabulka 4 Funkční specifikace nástroje pro řízení a kontrolu přístupu

Požadovaná funkcionality/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplň Uchazeč dle nabízeného zařízení
2 ks zařízení pro řízení přístupu včetně funkcionality a podpory pro 10.000 současných koncových zařízení		
Výrobce zařízení	Uvedení výrobce	Cisco Systems, Inc.
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	ISE-VM-K9=
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	http://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html
Obecná charakteristika ověřovacího řešení		

Požadovaná funkcionální/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplň Uchazeč dle nabízeného zařízení
Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení apod.)	ANO	ANO
Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo řídicími moduly, VPN branami) poskytuje ochranu před neoprávněným přístupem k pevné LAN síti, bezdrátové wifi síti (metodou 802.1x) a pro VPN přístup	ANO	ANO
Poskytuje AAA funkce (viz níže)	ANO	ANO
Podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control)	ANO	ANO
Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování kapacity	ANO	ANO
Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace	ANO	ANO
Je dostupné ve formě Appliance (hardware i software podporovaný jedním výrobcem)	ANO	ANO
Je dostupné ve formě Virtuálního stroje na platformách ESX nebo ESXi	ANO	ANO
AAA funkce (ověřování, autorizace a záznamy o průběhu připojování uživatelů a zařízení k síti)		
Podporované protokoly		
RADIUS pro autentizaci, autorizaci, logování	ANO	ANO
proxy funkce pro externí RADIUS	ANO	ANO
TACACS+ pro autentizaci, autorizaci a logování	ANO	ANO
TACACS+ pro funkci TACACS+ proxy	ANO	ANO
PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST, EAP-TTLS	ANO	ANO
Podporované databáze uživatelů (s možností definovat pořadí průchodu)		
Interní (pro uživatele i koncová zařízení)	ANO	ANO
Active Directory	ANO	ANO
Active Directory – více nezávislých domén	ANO	ANO
LDAP (RFC 2251)	ANO	ANO
RADIUS Token identity source (RFC 2865)	ANO	ANO
RSA RADIUS token server	ANO	ANO
Ověřování certifikátu koncových stanic/uživatelů na základě definovaného pole z certifikátu.	ANO	ANO
Ověřování uživatelů a zařízení		
Ověření uživatelů heslem nebo certifikátem	ANO	ANO
Ověření MAC adresou připojovaného zařízení	ANO	ANO
Rozpoznávání typu koncových zařízení a jejich stavu		
Automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se síťovou infrastrukturou	ANO	ANO
Předdefinované profily pro běžná mobilní zařízení (zařízení s OS Android, SymbianOS, Apple, Blackberry, HTC)	ANO	ANO
Autorizace: pružný systém pro definici pravidel pro přístup k síti		

Požadovaná funkcionální/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplíní Uchazeč dle nabízeného zařízení
Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle <ul style="list-style-type: none"> • uživatele (role, skupiny), • stavu a typu koncového zařízení (viz výše), • místa připojení, • historie připojení 	ANO	ANO
Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě	ANO	ANO
Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě	ANO	ANO
Podpora Change of Authorization (CoA, RFC 3576)	ANO	ANO
Možnost jednoduše identifikovat/označit přenášovaná data uživatele (rámce) v chráněné oblasti	ANO	ANO
Accounting		
Zaznamenávání aktivity uživatelů a zařízení připojených k síti	ANO	ANO
Dotazovací systém, korelace záznamů, centralizované výkazy	ANO	ANO
Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů)	ANO	ANO
Funkce GUEST serveru		
Vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i WiFi	ANO	ANO
Oprávnění přidělována správcem přístupu přes portál pro snadné vytváření dočasných účtů	ANO	ANO
Samoobslužný portál pro uživatele	ANO	ANO
Další vlastnosti		
Aktivace šifrování MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují)	ANO	ANO
Integrace s MDM systémy	ANO	ANO
Funkce pro správu ověřovacího systému		
Centralizovaná správa	ANO	ANO
Definice rolí administrátorů a úrovně přístupu k ověřovacímu systému	ANO	ANO
Zjednodušení správy vytváření skupin uživatelů, koncových a síťových zařízení	ANO	ANO
Grafické rozhraní pro definici pravidel přístupu k síti	ANO	ANO
Grafické rozhraní pro monitorování, definici výkazů, řešení problémů	ANO	ANO
Diagnostika problémů (systémová, údaje o chybách přihlašování, TCP dump, packet capture)	ANO	ANO
Zaznamenávání událostí na externí syslog server	ANO	ANO

Požadovaná funkcionální/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
Podpora SNMPv3	ANO	ANO
NTP pro synchronizaci času	ANO	ANO
SMTP pro zasílání zpráv a výstrah přes e-mail	ANO	ANO
Centrální server musí umět autorizovat mobilních zařízení do wifi sítě na základě kontroly jejich „zdraví“ (kontrola, zda zařízení není rootnuto, má antivír, ...) pomocí napojeného MDM systému Zákazníka (Mobile Iron)	ANO	ANO

B) Podpůrná aplikace pro správu MAC adres

Podpůrné aplikace zajišťující jednoduchou správu MAC adres a lokalizaci zařízení jsou realizovány prostřednictvím aplikací od společnosti Alef Nula. Správa MAC adres je řešena aplikací Alefit MAB Keeper, lokalizace zařízení prostřednictvím aplikace Alefit Office Locator.

Alefit MAB Keeper (APL-MAB-1X-UR)

Aplikace umožňuje spravovat některá nastavení autentizačního systému bez přístupu do konfiguračního rozhraní systému Cisco ISE. Přístupová oprávnění jsou přidělována na základě rolí administrátorů.

Díky jednoduchému a přehlednému uživatelskému rozhraní nemusí administrátoři znát detailně technologii Cisco ISE. Operace lze provádět přímo prostřednictvím GUI nebo automatizovaně díky vestavěnému REST API. Jednotlivé typy operací jsou zpracovány formou workflow a odděleny do separátních modulů.

Vlastnosti a parametry aplikace:

- Správa MAC adres
- Možnost přidávání/odebírání MAC adres kontraktorů, interních zaměstnanců, počítačů určených k nové instalaci nebo k reinstalaci a speciálních zařízení
- Integrace s ISE
- Správa uživatelských účtů a rolí
- Integrace s Microsoft AD
- High Availability režim

C) Podpůrná aplikace pro lokalizaci zařízení

Podpůrné aplikace zajišťující jednoduchou správu MAC adres a lokalizaci zařízení jsou realizovány prostřednictvím aplikací od společnosti Alef Nula. Správa MAC adres je řešena aplikací Alefit MAB Keeper, lokalizace zařízení prostřednictvím aplikace Alefit Office Locator.

Alefit Office Locator (APL-OFL-1X-UR)

Aplikace poskytuje komplexní informace o stavu autentizace zařízení a jeho lokaci na úrovni konkrétního přepínače a portu. V případě řešení problému umožňuje načíst autentizační logy z Cisco ISE, zkontrolovat účet workstation nebo uživatele v LDAP, zkontrolovat konfiguraci portu přepínače nebo restartovat autentizační session pomocí CoA zprávy. Tyto informace jsou pro oprávněného uživatele dostupné na jednom místě bez nutnosti přistupovat do ostatních systémů. Aplikace je plně integrovaná s aplikací AleFIT MAB Keeper.

Vlastnosti a parametry aplikace:

- resolving MAC adresy vůči síťovému jménu (jméno uživatele nebo počítače)
- lokalizace na úroveň přepínače a portu
- historie událostí na daném portu

Tabulka 5 Funkční specifikace podpůrných aplikací

Požadovaná funkcionality/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplň Uchazeč dle nabízeného zařízení
Podpůrná aplikace pro správu MAC adres		
Výrobce aplikace	Uvedení výrobce	ALEF NULA, a.s.
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	APL-MAB-1X-UR
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.alef.com/alefnula/ke-stazeni/alef-datasheet-mabol-cz.dm-774.pdf
Podpora funkcionality hromadného přidávání a mazání MAC adres v autentizačním systému	ANO	ANO
Podpora funkcionality manuálního přidávání a mazání MAC adres v autentizačním systému	ANO	ANO
Podpora funkcionality Wake On LAN pro zařízení v prostředí 802.1x	ANO	ANO
Umožnit řízení přístupu různých uživatelů v rámci aplikace	ANO	ANO
Umožnit rozlišení read-only / read-write přístupu v rámci aplikace	ANO	ANO
Umožnit uživatelsky přívětivou správu aplikace prostřednictvím webového rozhraní	ANO	ANO
Umožnit jednoduchou blokadu přístupu vybraným zařízeními	ANO	ANO
Umožnit funkcionality aplikace v rámci HA clusteru	ANO	ANO
Podpora auditovacích akcí	ANO	ANO
Podpůrná aplikace pro lokalizaci zařízení		
Výrobce aplikace	Uvedení výrobce	ALEF NULA a.s.
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	APL-OFL-1X-UR

Požadovaná funkcionální/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplň Uchazeč dle nabízeného zařízení
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.alef.com/alefnula/ke-stazeni/alef-datasheet-mabol-cz.dm-774.pdf
Umožnit funkcionální vyhledání portu, na kterém je uživatel připojen	ANO	ANO
Umožnit zjištění stavu autentizace příslušného portu	ANO	ANO
Umožnit zjištění stavu autentizace vybraného uživatele	ANO	ANO
Umožnit správu síťových přepínačů v rámci aplikace	ANO	ANO
Umožnit funkcionální aplikace v rámci HA clusteru	ANO	ANO

Výrobce nabízených zařízení – společnost Cisco Systems má implementován a zveřejněn proces pro nahlášení, uveřejňování a opravy bezpečnostních problémů a zranitelností, a dále má výrobce u nabízených aktivních síťových prvků implementován tzv. “SDL - secure development lifecycle” při vývoji svých produktů a tzv. “SIRT - Security Incident Response Team” pro reportování bezpečnostních incidentů spojených s nabízenými produkty.

Popisy bezpečnostních problémů a zranitelností, včetně návodů na jejich eliminaci před vydáním opravené verze firmware jsou dostupné na internetových stránkách výrobce.

Níže jsou uvedeny odkazy, kde jsou požadované informace výrobcem zveřejňovány:

Zveřejňování bezp. problémů a zranitelností - SIRT
<https://tools.cisco.com/security/center/publicationListing.x>

SDL – Secure Development Lifecycle
<http://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle/sdl-process.html>

PROTOKOL O AKCEPTACI

Předvedení funkcionalit dodaných zařízení v souladu s podmínkami vyplývajících ze zadávacích podmínek veřejné zakázky ev. číslo: 638583 s názvem „Náhrada zastaralých routerů a switchů na pracovištích CS a GŘC“ (dále jen „veřejná zakázka“).

Uchazeč se zavázal prokázat funkcionality implementovaného systému v prostředí zadavatele a poskytnout plnou součinnost pro provedení níže uvedených testů dle požadavků zadavatele.

Uchazeč se zavázal zajistit pro předvedení v rámci prokázání funkcionalit veškeré nabízené produkty včetně nezbytných licencí a všechny potřebné nástroje pro simulaci provozu a měření požadovaných hodnot. Předvedení a prokázání funkcionalit proběhlo ve dnech 4. a 5. 1. 2017 s výsledky dle následující tabulky.

Tabulka 6 Popis funkčních testů

Testovaná funkcionalita		Možný výsledek	Výsledek
WAN směrovač - typ A			
Detekce přímo připojených zařízení			
1	Detekce přímo připojeného zařízení pomocí LLDP	ANO/NE	ANO
2	Detekce přímo připojeného zařízení pomocí CDP	ANO/NE	ANO
Routing			
3	OSPF pro IPv4	ANO/NE	ANO
4	OSPF pro IPv6	ANO/NE	ANO
5	OSPF pro IPv4 a IPv6 běžící současně	ANO/NE	ANO
6	OSPF autentizace MD5	ANO/NE	ANO
7	BGPv4	ANO/NE	ANO
8	Podpora 4 byte AS number v BGP	ANO/NE	ANO
9	BGP Multiprotocol Support	ANO/NE	ANO
10	Generic Routing Encapsulation (GRE)	ANO/NE	ANO
11	Multipoint Generic Routing Encapsulation (mGRE)	ANO/NE	ANO
12	Unicast Reverse path check (uRPF)	ANO/NE	ANO
13	Virtualizace směrovacích tabulek – VRF nebo kompatibilní	ANO/NE	ANO
14	Alespoň 30 oddělených a nezávislých routovacích tabulek	ANO/NE	ANO
15	Protokoly a služby per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)	ANO/NE	ANO
16	Policy based routing na základě ACL	ANO/NE	ANO
17	First Hop Redundancy protokol pro IPv4	ANO/NE	ANO
18	First Hop Redundancy protokol pro IPv6	ANO/NE	ANO
Multicast			
19	IGMP v3	ANO/NE	ANO
20	MLD v2	ANO/NE	ANO
21	PIM Sparse Mode	ANO/NE	ANO
22	PIM Dense Mode	ANO/NE	ANO

23	PIM Sparse-Dense Mode	ANO/NE	ANO
24	PIM Source Specific Multicast	ANO/NE	ANO
Bezpečnost			
25	ACL na rozhraní IN/OUT	ANO/NE	ANO
26	Zone-based firewall	ANO/NE	ANO
27	Šifrování GRE tunelů	ANO/NE	ANO
28	IPSec AES-GCM-256	ANO/NE	ANO
29	Propustnost minimálně 90 Mbit (IMIX provoz) při aktivovaných službách IPSec šifrování a QoS	ANO/NE	ANO
30	Zvýšení propustnosti směrovače na alespoň 270 Mbit (IMIX provoz) při aktivovaných službách IPSec šifrování a QoS, např. formou licence	ANO/NE	ANO
31	IKEv2	ANO/NE	ANO
32	SHA-2 (SHA-256, SHA-512)	ANO/NE	ANO
33	Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami	ANO/NE	ANO
34	Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů	ANO/NE	ANO
35	Ochrana Control Plane směrovače před DoS útoky	ANO/NE	ANO
Monitorování Aplikačních toků			
36	Monitorování vstupních a výstupních toků na interface současně	ANO/NE	ANO
37	Monitoring bez vlivu na výkonnost zařízení	ANO/NE	ANO
38	Monitoring bez vlivu na propustnost zařízení	ANO/NE	ANO
39	Monitoring IPv4 a IPv6	ANO/NE	ANO
40	Lokální zobrazení shromážděných dat na směrovači	ANO/NE	ANO
41	Export dat ve formátu Netflow v9	ANO/NE	ANO
42	Export dat ve formátu IPFIX	ANO/NE	ANO
43	Monitoring všech procházejících paketů (nesamplovaný)	ANO/NE	ANO
44	Detekce a klasifikace aplikačních dat procházejících směrovačem až do 7. vrstvy OSI modelu (Deep Packet Inspection)	ANO/NE	ANO
45	Interní nástroje pro on-line měření kvality sítě infrastruktury, např. IP SLA nebo ekvivalentní	ANO/NE	ANO
Quality of Service			
46	Klasifikace procházející dopravy na základě CoS	ANO/NE	ANO
47	Klasifikace procházející dopravy na základě DSCP	ANO/NE	ANO
48	Klasifikace procházející dopravy na základě ACL	ANO/NE	ANO
49	Klasifikace procházející dopravy na základě analýzy až 7. vrstvy OSI modelu	ANO/NE	ANO
50	Značení procházející dopravy pomocí CoS	ANO/NE	ANO
51	Značení procházející dopravy pomocí DSCP	ANO/NE	ANO
52	Zařazování procházejícího provozu do front na základě dříve rozlišených tříd dopravy	ANO/NE	ANO
53	Prioritní fronta pro citlivé aplikace jako je voice a video	ANO/NE	ANO

54	Definice šířky pásma pro jednotlivé fronty	ANO/NE	ANO
55	Definice délky jednotlivých front	ANO/NE	ANO
56	Shaping odcházejícího provozu	ANO/NE	ANO
57	Policing odcházejícího a přicházejícího provozu	ANO/NE	ANO
58	Rate-limiting odcházejícího a přicházejícího provozu	ANO/NE	ANO
59	RSVP	ANO/NE	ANO
60	Hierarchický QoS, minimálně 3 úrovně	ANO/NE	ANO
Přístupový LAN přepínač 48 portů			
Napájecí zdroje a ventilátory			
1	Redundantní napájecí zdroje	ANO/NE	ANO
2	Redundantní ventilátory	ANO/NE	ANO
3	Plnohodnotná funkce přepínače v případě výpadku kteréhokoliv redundantního prvku	ANO/NE	ANO
4	Výpadek redundantního prvku nezpůsobí ztrátu konektivity připojeného zařízení	ANO/NE	ANO
5	U PoE zařízení nesmí dojít v případě výpadku zdroje k výpadku napájení	ANO/NE	ANO
6	Všechny redundantní prvky jsou vyměnitelné za chodu a to bez dopadu na provoz procházející přepínačem	ANO/NE	ANO
Napájení po datovém kabelu			
7	Napájení koncového zařízení 15W (802.2af)	ANO/NE	ANO
8	Napájení koncového zařízení 30W (802.3at)	ANO/NE	ANO
9	Napájení až 13x 30W současně	ANO/NE	ANO
10	Napájení až 13x 30W současně při jediném funkčním napájecím zdroji	ANO/NE	ANO
Detekce přímo připojených zařízení			
11	Detekce přímo připojeného zařízení pomocí LLDP	ANO/NE	ANO
12	Detekce přímo připojeného zařízení pomocí CDP	ANO/NE	ANO
VLAN			
13	Vytvoření VLAN v rozsahu 1 - 4094	ANO/NE	ANO
14	1000 aktivních a funkčních VLAN zároveň	ANO/NE	ANO
15	Tagování 802.1Q	ANO/NE	ANO
16	Tagování 802.1Q v 802.1Q	ANO/NE	ANO
17	Centralizovaná zpráva VLAN databáze	ANO/NE	ANO
18	Zařízení slouží jako řídicí prvek pro zprávu VLAN databáze	ANO/NE	ANO
19	VLAN databáze je chráněna proti nežádoucím změnám	ANO/NE	ANO
20	VLAN databáze může být změněna pouze na centrálním prvku	ANO/NE	ANO
21	VLAN databáze je chráněna heslem	ANO/NE	ANO
Spanning Tree Protocol			
22	802.1w – RSTP	ANO/NE	ANO
23	Zpětná kompatibilita s 802.1D – STP	ANO/NE	ANO
24	Samostatná STP instance pro alespoň 128 VLAN	ANO/NE	ANO
25	Zařízení připraveno na nasazení 802.1s – MSTP	ANO/NE	ANO

26	Šíření MSTP konfigurace mezi přepínači z centrálního přepínače	ANO/NE	ANO
27	Možnost měnit konfiguraci MSTP regionu pouze na centrálním přepínači	ANO/NE	ANO
28	Konfigurace MSTP chráněna heslem	ANO/NE	ANO
29	Porty ke koncovým zařízením přecházejí okamžitě do stavu forwarding	ANO/NE	ANO
30	Ochrana koncových portů proti připojení nežádoucího přepínače na základě kontroly přijímaných BPDU	ANO/NE	ANO
31	Ochrana proti změně STP centrálního switche	ANO/NE	ANO
32	Zabránění vzniku smyčky v případě, že port přestane dostávat BPDU (jednosměrná smyčka)	ANO/NE	ANO
33	Detekce jednosměrné linky (optické i metalické) mechanismem nezávislým na STP (UDLD nebo kompatibilní)	ANO/NE	ANO
Routing			
34	OSPF pro IPv4	ANO/NE	ANO
35	OSPF pro IPv6	ANO/NE	ANO
36	OSPF pro IPv4 a IPv6 běžící současně	ANO/NE	ANO
37	OSPF autentizace MD5	ANO/NE	ANO
38	First Hop Redundancy protokol pro IPv4	ANO/NE	ANO
39	First Hop Redundancy protokol pro IPv6	ANO/NE	ANO
40	Unicast Reverse path check (uRPF)	ANO/NE	ANO
Multicast			
41	IGMP snooping v3	ANO/NE	ANO
42	MLD snooping v2	ANO/NE	ANO
43	PIM Sparse Mode	ANO/NE	ANO
44	PIM Dense Mode	ANO/NE	ANO
45	PIM Sparse-Dense Mode	ANO/NE	ANO
46	PIM Source Specific Multicast	ANO/NE	ANO
Bezpečnost			
47	Limitování počtu povolených MAC adres na port	ANO/NE	ANO
48	802.1x ověřování koncových zařízení	ANO/NE	ANO
49	Ochrana proti podvržení DHCP serveru	ANO/NE	ANO
50	Ochrana proti podvržení DHCP release a decline zpráv	ANO/NE	ANO
51	Kontrola MAC adresy v DHCP request zprávě vůči MAC adrese v ethernetovém rámci (Ochrana proti DoS)	ANO/NE	ANO
52	DHCP messages rate-limiting (Ochrana proti DoS)	ANO/NE	ANO
53	Ochrana proti podvržení IP adresy	ANO/NE	ANO
54	Ochrana proti podvržení MAC adresy	ANO/NE	ANO
55	Ochrana proti podvržení ARP zprávy – kontrola a ověření jednotlivých polí v ARP zprávě	ANO/NE	ANO
56	ARP messages rate-limiting (Ochrana proti DoS)	ANO/NE	ANO
57	Ochrana proti podvržení DHCPv6 serveru	ANO/NE	ANO
58	Ochrana proti podvržení IPv6 Router Advertisement	ANO/NE	ANO

59	Ochrana proti podvržení IPv6 Neighbor Discovery	ANO/NE	ANO
60	Ochrana proti podvržení IPv6 adresy	ANO/NE	ANO
61	802.1ae – MACsec, line-rate šifrování na L2	ANO/NE	ANO
62	802.1ae mezi přepínači	ANO/NE	ANO
63	802.1ae ke koncovým stanicím	ANO/NE	ANO
64	Ochrana Control Plane přepínače před DoS útoky	ANO/NE	ANO
Monitorování Aplikačních toků			
65	Monitorování vstupních a výstupních toků na interface současně	ANO/NE	ANO
66	Monitoring bez vlivu na výkonnost zařízení	ANO/NE	ANO
67	Monitoring bez vlivu na propustnost zařízení	ANO/NE	ANO
68	Monitoring IPv4 a IPv6	ANO/NE	ANO
69	Lokální zobrazení shromážděných dat na přepínači	ANO/NE	ANO
70	Export dat ve formátu Netflow v9	ANO/NE	ANO
71	Export dat ve formátu IPFIX	ANO/NE	ANO
72	Monitoring všech procházejících paketů (nesamplovaný)	ANO/NE	ANO
Quality of Service			
73	Klasifikace procházející dopravy na základě CoS	ANO/NE	ANO
74	Klasifikace procházející dopravy na základě DSCP	ANO/NE	ANO
75	Klasifikace procházející dopravy na základě ACL	ANO/NE	ANO
76	Značení procházející dopravy pomocí CoS	ANO/NE	ANO
77	Značení procházející dopravy pomocí DSCP	ANO/NE	ANO
78	Zařazování procházejícího provozu do front na základě dříve rozlišených tříd dopravy	ANO/NE	ANO
79	Prioritní fronta pro citlivé aplikace jako je voice a video	ANO/NE	ANO
80	Definice šířky pásma pro jednotlivé fronty	ANO/NE	ANO
81	Definice délky jednotlivých front	ANO/NE	ANO
82	Shaping odcházejícího provozu	ANO/NE	ANO
83	Policing odcházejícího a přicházejícího provozu	ANO/NE	ANO
84	Hierarchický QoS, minimálně 2 úrovně	ANO/NE	ANO
Řízení přístupu do sítě			
85	Aplikovat critical VLAN v případě nedostupnosti AAA	ANO/NE	ANO
86	VLAN loadbalancing	ANO/NE	ANO
87	Umožnit Radius CoA	ANO/NE	ANO
Přístupový LAN přepínač 24 portů			
Napájecí zdroje a ventilátory			
1	Redundantní napájecí zdroje	ANO/NE	ANO
2	Redundantní ventilátory	ANO/NE	ANO
3	Plnohodnotná funkce přepínače v případě výpadku kteréhokoliv redundantního prvku	ANO/NE	ANO
4	Výpadek redundantního prvku nezpůsobí ztrátu konektivity připojeného zařízení	ANO/NE	ANO
5	U PoE zařízení nesmí dojít v případě výpadku zdroje	ANO/NE	ANO

	k výpadku napájení		
6	Všechny redundantní prvky jsou vyměnitelné za chodu a to bez dopadu na provoz procházející přepínačem	ANO/NE	ANO
Napájení po datovém kabelu			
7	Napájení koncového zařízení 15W (802.2af)	ANO/NE	ANO
8	Napájení koncového zařízení 30W (802.3at)	ANO/NE	ANO
9	Napájení až 13x 30W současně	ANO/NE	ANO
10	Napájení až 13x 30W současně při jediném funkčním napájecím zdroji	ANO/NE	ANO
Detekce přímo připojených zařízení			
11	Detekce přímo připojeného zařízení pomocí LLDP	ANO/NE	ANO
12	Detekce přímo připojeného zařízení pomocí CDP	ANO/NE	ANO
VLAN			
13	Vytvoření VLAN v rozsahu 1 - 4094	ANO/NE	ANO
14	1000 aktivních a funkčních VLAN zároveň	ANO/NE	ANO
15	Tagování 802.1Q	ANO/NE	ANO
16	Tagování 802.1Q v 802.1Q	ANO/NE	ANO
17	Centralizovaná zpráva VLAN databáze	ANO/NE	ANO
18	Zařízení slouží jako řídicí prvek pro zprávu VLAN databáze	ANO/NE	ANO
19	VLAN databáze je chráněna proti nežádoucím změnám	ANO/NE	ANO
20	VLAN databáze může být změněna pouze na centrálním prvku	ANO/NE	ANO
21	VLAN databáze je chráněna heslem	ANO/NE	ANO
Spanning Tree Protocol			
22	802.1w – RSTP	ANO/NE	ANO
23	Zpětná kompatibilita s 802.1D – STP	ANO/NE	ANO
24	Samostatná STP instance pro alespoň 128 VLAN	ANO/NE	ANO
25	Zařízení připraveno na nasazení 802.1s – MSTP	ANO/NE	ANO
26	Šíření MSTP konfigurace mezi přepínači z centrálního přepínače	ANO/NE	ANO
27	Možnost měnit konfiguraci MSTP regionu pouze na centrálním přepínači	ANO/NE	ANO
28	Konfigurace MSTP chráněna heslem	ANO/NE	ANO
29	Porty ke koncovým zařízením přecházejí okamžitě do stavu forwarding	ANO/NE	ANO
30	Ochrana koncových portů proti připojení nežádoucího přepínače na základě kontroly přijímaných BPDU	ANO/NE	ANO
31	Ochrana proti změně STP centrálního switche	ANO/NE	ANO
32	Zabránění vzniku smyčky v případě, že port přestane dostávat BPDU (jednosměrná smyčka)	ANO/NE	ANO
33	Detekce jednosměrné linky (optické i metalické) mechanismem nezávislým na STP (UDLD nebo kompatibilní)	ANO/NE	ANO
Routing			
34	OSPF pro IPv4	ANO/NE	ANO
35	OSPF pro IPv6	ANO/NE	ANO

36	OSPF pro IPv4 a IPv6 běžící současně	ANO/NE	ANO
37	OSPF autentizace MD5	ANO/NE	ANO
38	First Hop Redundancy protokol pro IPv4	ANO/NE	ANO
39	First Hop Redundancy protokol pro IPv6	ANO/NE	ANO
40	Unicast Reverse path check (uRPF)	ANO/NE	ANO
Multicast			
41	IGMP snooping v3	ANO/NE	ANO
42	MLD snooping v2	ANO/NE	ANO
43	PIM Sparse Mode	ANO/NE	ANO
44	PIM Dense Mode	ANO/NE	ANO
45	PIM Sparse-Dense Mode	ANO/NE	ANO
46	PIM Source Specific Multicast	ANO/NE	ANO
Bezpečnost			
47	Limitování počtu povolených MAC adres na port	ANO/NE	ANO
48	802.1x ověřování koncových zařízení	ANO/NE	ANO
49	Ochrana proti podvržení DHCP serveru	ANO/NE	ANO
50	Ochrana proti podvržení DHCP release a decline zpráv	ANO/NE	ANO
51	Kontrola MAC adresy v DHCP request zprávě vůči MAC adrese v ethernetovém rámci (Ochrana proti DoS)	ANO/NE	ANO
52	DHCP messages rate-limiting (Ochrana proti DoS)	ANO/NE	ANO
53	Ochrana proti podvržení IP adresy	ANO/NE	ANO
54	Ochrana proti podvržení MAC adresy	ANO/NE	ANO
55	Ochrana proti podvržení ARP zprávy – kontrola a ověření jednotlivých polí v ARP zprávě	ANO/NE	ANO
56	ARP messages rate-limiting (Ochrana proti DoS)	ANO/NE	ANO
57	Ochrana proti podvržení DHCPv6 serveru	ANO/NE	ANO
58	Ochrana proti podvržení IPv6 Router Advertisement	ANO/NE	ANO
59	Ochrana proti podvržení IPv6 Neighbor Discovery	ANO/NE	ANO
60	Ochrana proti podvržení IPv6 adresy	ANO/NE	ANO
61	802.1ae – MACsec, line-rate šifrování na L2	ANO/NE	ANO
62	802.1ae mezi přepínači	ANO/NE	ANO
63	802.1ae ke koncovým stanicím	ANO/NE	ANO
64	Ochrana Control Plane přepínače před DoS útoky	ANO/NE	ANO
Monitorování Aplikačních toků			
65	Monitorování vstupních a výstupních toků na interface současně	ANO/NE	ANO
66	Monitoring bez vlivu na výkonost zařízení	ANO/NE	ANO
67	Monitoring bez vlivu na propustnost zařízení	ANO/NE	ANO
68	Monitoring IPv4 a IPv6	ANO/NE	ANO
69	Lokální zobrazení shromážděných dat na přepínači	ANO/NE	ANO
70	Export dat ve formátu Netflow v9	ANO/NE	ANO
71	Export dat ve formátu IPFIX	ANO/NE	ANO
72	Monitoring všech procházejících paketů (nesamplovaný)	ANO/NE	ANO

Quality of Service			
73	Klasifikace procházející dopravy na základě CoS	ANO/NE	ANO
74	Klasifikace procházející dopravy na základě DSCP	ANO/NE	ANO
75	Klasifikace procházející dopravy na základě ACL	ANO/NE	ANO
76	Značení procházející dopravy pomocí CoS	ANO/NE	ANO
77	Značení procházející dopravy pomocí DSCP	ANO/NE	ANO
78	Zařazování procházejícího provozu do front na základě dříve rozlišených tříd dopravy	ANO/NE	ANO
79	Prioritní fronta pro citlivé aplikace jako je voice a video	ANO/NE	ANO
80	Definice šířky pásma pro jednotlivé fronty	ANO/NE	ANO
81	Definice délky jednotlivých front	ANO/NE	ANO
82	Shaping odcházejícího provozu	ANO/NE	ANO
83	Policing odcházejícího a přicházejícího provozu	ANO/NE	ANO
84	Hierarchický QoS, minimálně 2 úrovně	ANO/NE	ANO
Řízení přístupu do sítě			
85	Aplikovat critical VLAN v případě nedostupnosti AAA	ANO/NE	ANO
86	VLAN loadbalancing	ANO/NE	ANO
87	Umožnit Radius CoA	ANO/NE	ANO
Nástroje pro řízení, kontrolu a monitoring přístupu do sítě			
System pro řízení přístupu do sítě			
1	Ověřit možnost redundance/loadbalancingu RADIUS komunikace	ANO/NE	ANO
2	Ověřit, že autentizační systém umožňuje autorizaci pomocí Jména, nebo čísla VLAN	ANO/NE	ANO
3	Ověřit možnost zasílat autorizaci pomocí downloadable access listu	ANO/NE	ANO
4	Ověřit autentizaci koncového zařízení na základě MAC adresy	ANO/NE	ANO
5	Ověřit možnost monitorování aktuálních přístupů do sítě včetně historie	ANO/NE	ANO
6	Ověřit možnost zasílání autentizačních informací pomocí syslog protokolu (UDP, TCP, Secure TCP)	ANO/NE	ANO
7	Autentizační server umožňuje ověřování certifikátů koncových stanic / uživatelů	ANO/NE	ANO
8	Ověřit funkcionality stavu certifikátu metodou CRL	ANO/NE	ANO
9	Ověřit funkcionality stavu certifikátu metodou OCSP	ANO/NE	ANO
10	Ověřit funkcionality autentizace IP telefonu do VOICE domény	ANO/NE	ANO
11	Ověřit, že autentizační server je schopen být integrován do více MS AD, které nejsou ve vzájemném „trustu“.	ANO/NE	ANO
12	Ověřit, že integrace s doménou může být provedena pomocí MS KERBEROS protokolu	ANO/NE	ANO
13	Ověřit, že autentizační server umožňuje načítání uživatelských skupin z AD	ANO/NE	ANO

14	Ověřit, že autentizační server umožňuje načítání vlastností objektu typu uživatel	ANO/NE	ANO
15	Ověřit, že autentizační server umožňuje načítání atributů objektu typu machine	ANO/NE	ANO
16	Ověřit podporu Radius CoA	ANO/NE	ANO
17	Ověřit, že autentizační server je schopen shromažďovat informace o typu koncových zařízení	ANO/NE	ANO
18	Ověřit, že autentizační server umožňuje odmítnout vpustit do sítě nedoménového uživatele přihlašujícího se na doménovém zařízení	ANO/NE	ANO
19	Zakomponovat ověřování mobilní laboratoře	ANO/NE	ANO
Podpůrná aplikace pro správu MAC adres			
20	Ověřit možnost hromadného přidávání MAC adres do autentizačního systému	ANO/NE	ANO
21	Ověřit možnost hromadného mazání MAC adres z autentizačního systému	ANO/NE	ANO
22	Ověřit možnost manuálního přidávání MAC adres do autentizačního systému	ANO/NE	ANO
23	Ověřit možnost manuálního mazání MAC adres z autentizačního systému	ANO/NE	ANO
24	Ověřit funkcionálníitu Wake On LAN	ANO/NE	ANO
25	Předvést možnost řízení přístupu různých uživatelů a uživatelských skupin v rámci aplikace	ANO/NE	ANO
26	Předvést možnost rozlišení read-only / read-write přístupu v rámci aplikace	ANO/NE	ANO
27	Předvést funkcionálníitu umožnění přístupu na základě Sponzorského účtu	ANO/NE	ANO
28	Předvést možnost hlídání času validity MAC adres a jejich automatické mazání z databáze autentizačního systému	ANO/NE	ANO
29	Předvést postup blokace přístupu vybraným zařízením	ANO/NE	ANO
30	Předvést možnost samostatné správy konfigurace aplikace prostřednictvím webového rozhraní	ANO/NE	ANO
Podpůrná aplikace pro lokalizaci zařízení			
31	Předvést funkcionálníitu vyhledání portu, na kterém je uživatel připojen	ANO/NE	ANO
32	Zjištění stavu autentizace příslušného portu	ANO/NE	ANO
33	Zjištění stavu autentizace vybraného uživatele	ANO/NE	ANO
34	Předvést správu síťových přepínačů v rámci aplikace	ANO/NE	ANO

Zahájení akceptačních testů: 4. 1. 2017

Ukončení akceptačních testů: 5. 1. 2017

Splnění podmínek akceptačních testů – potvrzení, zda předmět akceptace

splňuje akceptační podmínky akceptace:

splňuje v plném rozsahu

nesplňuje

~~splňuje s těmito výhradami~~

Poznámky:

-

Zadavatel/ Objednatel – Generální ředitelství cel, Budějovická 7, Praha 4:		
--	--	--

Oprávněná osoba:	Telefon, E-mail:	Datum:
------------------	------------------	--------

Uchazeč/Zhotovitel – Vertix s.r.o, Štrossova 291, Pardubice:		
--	--	--

Oprávněná osoba:	Telefon, E-mail:	Datum:
------------------	------------------	--------

Příloha č. 2
Předávací protokol

(část přílohy k smlouvě)

PŘEDÁVACÍ PROTOKOL

Kupující:	Generální ředitelství cel	Číslo smlouvy:	08_11/2016
Prodávající:	VERTIX s.r.o.		

Předmět předání a převzetí (Specifikace rozsahu předávaného plnění včetně uvedení verzí předávaných dokumentů nebo software)
1.
2.
3.
4.
Předáno dne:

Podpisem tohoto Předávacího protokolu potvrzuje Oprávněná osoba Prodávajícího, že uvedený předmět k uvedenému dni řádně předala Oprávněné osobě Kupujícího.

Podpisem tohoto Předávacího protokolu potvrzuje Oprávněná osoba Kupujícího, že uvedený předmět k uvedenému dni řádně převzala v souladu s ustanoveními smlouvy.

Kupující:		
Oprávněná osoba:	Telefon, E-mail:	Datum:

Prodávající:		
Oprávněná osoba:	Telefon, E-mail:	Datum:

Příloha č. 3
Cenová tabulka

Ceník – stanovení celkové nabídkové ceny

Předmět plnění	Cena v Kč/ jednotka (bez DPH)	Počet jednotek	Celková cena v Kč
1. WAN směrovače typ - typ A	44 790,00 Kč	110	4 926 900,00 Kč
2. přístupový LAN přepínač 48 portů	54 660,00 Kč	185	10 112 100,00 Kč
3. přístupový LAN přepínač 24 portů	29 655,00 Kč	108	3 202 740,00 Kč
4. Single mode transceiver	0,00 Kč	40	0,00 Kč
5. Multi mode transceiver	0,00 Kč	285	0,00 Kč
6. zařízení pro řízení přístupu včetně podpory	144 883,00 Kč	2	289 766,00 Kč
7. podpůrná aplikace pro správu MAC adres	14 025,00 Kč	2	28 050,00 Kč
8. podpůrná aplikace pro lokalizaci zařízení	14 025,00 Kč	2	28 050,00 Kč
CELKOVÁ NABÍDKOVÁ CENA ZA KOMPLETNÍ PŘEDMĚT PLNĚNÍ V Kč BEZ DPH			18 587 606,00 Kč
CELKOVÁ NABÍDKOVÁ CENA ZA KOMPLETNÍ PŘEDMĚT PLNĚNÍ V Kč S DPH			22 491 003,26 Kč

Poznámky:

Dle doporučení Zadavatele jsou stávající transceivery použité v navrženém řešení. Všechny výše uvedené transceiver moduly jsou plně kompatibilní (plná podpora výrobcem) s navrženým směrovačem Cisco ISR4331-SEC/K9 a navrženými LAN přepínači Cisco WS-C3650-48PS-S a Cisco WS-C3650-24PS-S.

Veškerá optická propojení tak budou realizována prostřednictvím stávajících transceiver modulů, což představuje pro Zadavatele nulové náklady na pořízení a ochranu dříve vynaložených investic do těchto transceiver modulů.