PŘÍLOHA Č. 18 – TABULKY POŽADOVANÝCH TECHNICKÝCH PARAMETRŮ

V rámci této přílohy jsou specifikovány technické parametry ke každému dílčímu projektu z přílohy č. 6 – Funkční a technické požadavky.

1 TECHNICKÉ A FUNKČNÍ SPECIFIKACE NABÍZENÉHO ŘEŠENÍ

1.1 OBLAST DATOVÝCH CENTER

1.1.1 KONSOLIDACE SERVERŮ V DATOVÝCH CENTRECH

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.1.2 MIGRACE KI DC DO NOVÉ LOKALITY

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.1.3 VYBUDOVÁNÍ KOMUNIKAČNÍ INFRASTRUKTURY PRO NOVÉ DATOVÉ CENTRUM

1.1.3.1 ARCHITEKTURA KOMUNIKAČNÍ INFRASTRUKTURY DATOVÉHO CENTRA

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Výrobce systému	
Odkaz na www stránky výrobce systému, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	
Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Architektura sítě je typu Spine-Leaf	
Řízení celého řešení pomocí řadiče (controlleru)	
OSPFv2	
BGPv4	
802.1q	
VXLAN bridging	
VXLAN routing	
NVGRE bridging	
NVGRE routing	
Integrace s Hypervisorem VMware vSphere	
Integrace s Hypervisorem Microsoft Hyper-V	
Integrace se zařízením F5 BigIP	
Integrace se zařízením Checkpoint Firewall	

1.1.3.2 PRVEK LEAF

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	
Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Typ zařízení: přepínač	
Formát zařízení: fixní	
Minimálně 6 portů 40GE formátu QSFP	
Minimálně 48 portů 1/10GE formátu SFP/SFP+	
Neblokující architektura	
Minimálně 96000 záznamů v MAC address tabulce	
IEEE 802.3ad (Link aggregation – LAG)	
IEEE 802.3ad přes více přepínačů v rámci fabric	
Velikost 1RU	
IEEE 802.1Q	
Minimálně 4096 aktivních VLAN	
Minimálně 88000 záznamů IP adres připojených stanic	
Jumbo rámce – min. 9000 bajtů	
Detekce protilehlého zařízení (např. LLDP)	
Minimálně 1000 VRF kontextů	
Minimálně 4 SPAN relace	
Minimálně 128 VXLAN VTEP na VLAN	

1.1.3.3 PRVEK SPINE

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: přepínač	
Formát zařízení: fixní	
Minimálně 32 portů 40GE formátu QSFP	
Neblokující architektura	
Minimálně 96000 záznamů v MAC address tabulce	
IEEE 802.3ad (Link aggregation – LAG)	
IEEE 802.3ad přes více přepínačů v rámci fabric	
Velikost 1RU	
IEEE 802.1Q	
Minimálně 4096 aktivních VLAN	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Minimálně 88000 záznamů IP adres připojených stanic	
Jumbo rámce – min. 9000 bajtů	
Detekce protilehlého zařízení (např. LLDP)	
Minimálně 1000 VRF kontextů	
Minimálně 4 SPAN relace	
Minimálně 128 VXLAN VTEP na VLAN	

1.1.3.4 PRVEK CENTRÁLNÍ ŘADIČ

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (pokud je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: řadič	
Řadič s redundancí min. N+2	
Všechny řadiče jsou aktivní (režim *all active*)	
Grafické uživatelské rozhraní součástí řešení	
Přístupová práva založená na uživatelských rolích	
Možnost rozdělit správu řešení mezi více vzájemně oddělených organizací (multitenantní řešení)	
Dokumentované programátorské rozhraní pro volání všech dostupných funkcí řadiče, včetně těch, které jsou použity v grafickém uživatelském rozhraní	
Možnost definice aplikačních politik, kde jsou servery (fyzické i virtální) a další koncové stanice členěny do skupin podle své funkce na základě charakteristik, jako je IP adresa, MAC adresa, lokace za určitým portem, příslušnosti do VLAN, VXLAN, NVGRE a podobných. Ke skupinám jsou pak definovány na abstraktní úrovni komunikační požadavky vůči jiným skupinám	

1.1.3.5 PRVEK ILO/LOM PŘEPÍNAČ

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: přepínač	
Formát zařízení: fixní	
Dva dedikované stohovací porty	
Možnost mít alespoň 8 zařízení ve stohu	
Minimální kapacita sběrnice stohu 80 Gb/s	
Minimálně 48 portů 10/100/1000 Base-TX	
Minimálně 4 1GE uplink porty s volitelným fyzickým rozhraním	
Jeden osazený 1GE port modulem 1000Base-SX	
Minimálně 16000 záznamů v MAC address tabulce	
IEEE 802.3ad (Link aggregation – LAG)	
IEEE 802.3ad přes více přepínačů ve stohu	
Minimálně 8 linek jako součást LAG trunku	
Minimálně 20 konfigurovatelných LAG trunků	
IEEE 802.1Q	
Minimálně 1000 aktivních VLAN	
IEEE 802.1w – Rapid Spanning Tree Protocol	
Jumbo rámce – min. 9190 bytes	
Detekce protilehlého zařízení (např. LLDP)	
IGMPv2/IGMPv3 snooping	
IPv6 services (SSH, Syslog)	
IPv6 QoS	
IPv6 MLDv1 & v2 snooping	
IPv6 First Hop Security (Port ACL, RA guard)	
IPv6 ACL	
QoS classification – ACL, DSCP, CoS based	
QoS marking – DSCP, CoS	
QoS – Strict Priority Queue	
IEEE 802.1x	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	
Možnost provozu 802.1x v tzv. monitorovacím módu bez omezování přístupu koncových uživatelů	
RADIUS CoA (RFC 5176)	
IEEE 802.1x Multi-domain authentication	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové IP adresy	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	
Možnost definovat povolené MAC adresy na portu	
Monitorování aplikačních toků prostřednictvím technologie NetFlow nebo ekvivalentní technologie	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	
Interní nástroje pro debugging procházejícího provozu	
DHCP server	
SSHv2	
CLI rozhraní	
SNMPv2/v3	
TACACS+ nebo RADIUS klient pro AAA	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Vzdálený port mirroring (RSPAN)	
L2 traceroute	

1.1.3.6 PRVEK WAN SMĚROVAČ

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: směrovač	
Formát zařízení: modulární	
Minimálně 2 porty GigabitEthernet 1000Base-TX	
Minimálně 2 porty 10 GigabitEthernet 10GBASE-SR	
Oddělený procesor pro funkce směrování a forwardování paketů	
Směrování IPv4	
Směrování IPv6	
Propustnost systému minimálně 35 Gb/s	
Výkon směrovače minimálně 28 Mpps	
Minimálně 1 mil. záznamů ve směrovací tabulce pro IPv4	
Minimálně 0,5 mil. záznamů ve směrovací tabulce pro IPv6	
IEEE 802.3ad	
OSPFv2	
BGPv4	
Podpora 4-byte ASN v BGP	
Možnost směrování provozu dle dynamicky měřených metrik (zatížení linky, zpoždění, ztrátovost paketů, jitter)	
First Hop Redundancy Protokol (např. VRRP, HSRP)	
GRE (Generic Routing Encapsulation)	
Policy-based routing podle ACL	
IP Multicast (PIM SSM, PIM SM)	
IGMPv2, IGMPv3	
uRPF	
DHCP relay	
First Hop Redundancy Protokol pro IPv6	
OSPFv3	
MP BGP	
IPv6 Multicast (MLDv1 & v2)	
IPv6 Multicast (PIM SM)	
IPv6 Multicast (PIM SSM)	
IPv6 SLA nebo ekvivalentní technologie	
uRPF pro IPv6	
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels	
IPv6 over IPv4 Multipoint VPN nebo ekvivalentní technologie	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
DHCPv6 Relay	
QoS classification – ACL, DSCP, CoS, MPLS EXP based	
QoS marking – DSCP, CoS, MPLS EXP	
QoS Shaping and Policing	
Class Based and Priority queuing	
Rate Limiting	
Hierarchický QoS s min. třemi úrovněmi	
RSVP	
MPLS	
MPLS VPN	
Technologie pro vytváření L2 propojení nad IP infrastruktoru pro účely vzájemného propojení datových center	
Virtualizace směrovacích tabulek – např. Virtual Routing and Forwarding (VRF)	
Minimálně 50 oddělených (nezávislých) směrovacích tabulek	
Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)	
ACL na rozhraní IN/OUT (včetně virtuálních – VLAN, loopback)	
IPSec AES 256	
Hardwarová akcelerace šifrování pro IPSec AES 256	
Minimálně 4 Gb/s šifrovací výkon pro IPSec AES 256 (IMIX provoz)	
IKEv2	
SHA-2 (SHA-256, SHA-512)	
Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami (např. pro IPT provoz)	
Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů	
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	
Vynucení QoS parametrů pro takto rozpoznané aplikace a skupiny aplikací – marking, garance šířky pásma pro jednotlivé aplikace, shaping, policing	
Měření statistik a výkonnostních charakteristik přenášených multimediálních, realtimových a aplikačních toků – využívané pásmo	
Měření statistik a výkonnostních charakteristik přenášených multimediálních, realtimových a aplikačních toků – odezvy aplikací	
Měření statistik a výkonnostních charakteristik přenášených multimediálních, realtimových a aplikačních toků – počty aplikačních spojení	
Sběr a vyhodnocování statistik a výkonnostních charakteristik multimediálních toků: využívané pásmo, odezvy aplikací, RTP statistiky	
Monitorování aplikačních toků s využitím technologie NetFlow	
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně paramterů: zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód	
Podpora minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat)	
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA (nebo ekvivalentní)	
Interní nástroje pro debugging procházejícího provozu	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
SSHv2	
CLI rozhraní	
SNMPv2/v3	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	
NTP server	

1.1.3.7 PRVEK INTERNETOVÝ SMĚROVAČ

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení směrovač	
Formát zařízení modulární	
Minimálně 4 porty 10/100/1000Base-TX	
Směrování IPv4	
Směrování IPv6	
OSPFv2	
BGPv4	
Podpora 4-byte ASN v BGP	
Možnost směrování provozu dle dynamicky měřených metrik (zatížení linky, zpoždění, ztrátovost paketů, jitter)	
First Hop Redundancy Protokol (např. VRRP, HSRP)	
GRE (Generic Routing Encapsulation)	
Policy-based routing podle ACL	
IP Multicast (PIM SSM, PIM SM)	
IGMPv2, IGMPv3	
uRPF	
DHCP relay	
First Hop Redundancy Protokol pro IPv6	
OSPFv3	
MP BGP	
IPv6 Multicast (MLD v1 & v2)	
IPv6 Multicast (PIM SM)	
IPv6 Multicast (PIM SSM)	
IPv6 SLA nebo ekvivalentní technologie	
uRPF pro IPv6	
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels	
IPv6 over IPv4 Multipoint VPN nebo ekvivalentní technologie	
DHCPv6 Relay	
QoS classification – ACL, DSCP, CoS based	
QoS marking – DSCP, CoS	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
QoS Shaping and Policing	
Class Based and Priority queuing	
Rate Limiting	
HierarchickýQoS s min. třemi úrovněmi	
RSVP	
Virtualizace směrovacích tabulek – např. Virtual Routing and Forwarding (VRF)	
Minimálně 50 oddělených (nezávislých) směrovacích tabulek	
Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING, VoIP gateway)	
ACL na rozhraní IN/OUT (včetně virtuálních – VLAN, loopback)	
Zone-based firewall	
IPSec AES 256	
Hardwarová akcelerace šifrování pro IPSec AES 256	
Minimální propustnost směrovače 1 Gb/s při aktivovaných službách IPSec šifrování a Hierachical QoS měřená pro IMIX provoz	
IKEv2	
SHA-2 (SHA-256, SHA-512)	
Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami (např. pro IPT provoz)	
Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů	
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	
Vynucení QoS parametrů pro takto rozpoznané aplikace a skupiny aplikací – marking, garance šířky pásma pro jednotlivé aplikace, shaping, policing	
Měření statistik a výkonnostních charakteristik přenášených multimediálních, realtimových a aplikačních toků – využívané pásmo	
Měření statistik a výkonnostních charakteristik přenášených multimediálních, realtimových a aplikačních toků – odezvy aplikací	
Měření statistik a výkonnostních charakteristik přenášených multimediálních, realtimových a aplikačních toků – počty aplikačních spojení	
Sběr a vyhodnocování statistik a výkonnostních charakteristik multimediálních toků: využívané pásmo, odezvy aplikací, RTP statistiky	
Monitorování aplikačních toků s využitím technologie NetFlow	
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód	
Podpora minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat)	
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA (nebo ekvivalentní)	
Interní nástroje pro debugging procházejícího provozu	
SSHv2	
CLI rozhraní	
SNMPv2/v3	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	
NTP server	

1.1.4 Systém přístupu uživatelů k síťovým prvkům

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.1.5 Propojení nového DC pomocí DWDM technologie

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.1.6 Virtualizace serverů v demilitarizované zóně (DMZ)

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.1.7 Zajištění VPN přístupu servisních organizací

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce řešení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného řešení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Umístění centrálního prvku řešení v datovém centru	
Forma centrálního prvku je virtuální appliance do Zadavatelem používané virtualizační platformy	
Minimálně 500 licencovaných klientů	
Možnost rozšířit počet klientů na 2000	
Oddělení od současného VPN systému pro běžné uživatele	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Podpora dvoufaktorové autentizace	
Autentizace pomocí nového systému infrastrukturní autentizace – viz 6.4.1	
VPN musí být sestavovány, autentizovány a šifrovány silnými algoritmy, dnes považovanými za neprolomitelné a bezchybné, např. RSA, DSA, AES, RC4, SHA	
Podpora klientského softwaru na platformě Windows	
Podpora klientského softwaru na platformě MAC OS-X	
Podpora klientského softwaru na platformě Linux	
Podpora klientského softwaru na platformě Android	
Podpora klientského softwaru na platformě iOS	
Podpora více režimů připojení na klientovi, od osobního systému jednoduchého uživatele až po vzdálenou bránu připojující více sítí	
Podpora řízení přístupu klienta na předem definované zdroje, IP adresy a porty dle jeho úrovně oprávnění	
Podpora spouštění jakékoli aplikace, skriptu na klientské straně na základě specifikované události	
Možnost ověření přítomnosti a aktuálnosti specifikovaných aplikací na klientské straně	
Škálovatelnost počtu připojených klientů až do řádu 100000	
Podpora HA (active, standby)	
Podpora Datagram Transport Layer Service (DTLS) nad UDP a TLS nad TCP	
Obsahuje API umožňující aplikacím třetích stran integraci na straně serveru i klienta	

1.1.8 ZVÝŠENÍ ODOLNOSTI CENTRÁLNÍHO SYSTÉMU SLUŽEB DNS, DHCP, IPAM

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Systém musí nadále plnit všechny požadavky, které jsou kladeny na současný systém – viz popis současného stavu	
Systém musí podpořit minimálně 40 000 klientů (síťové prvky, IP adresní rozsahy, servery, stanice, IP telefony…)	
Navrhovaný systém splňuje minimálně stejné vlastnosti, které splňuje současný systém – viz popis současného stavu	
Systém musí poskytovat funkce zejména (některé požadavky taktéž vychází ze současného stavu – viz popis současného stavu):	
• Musí spojovat informace z DNS, DHCP a IPAM a přes grafické rozhraní umožnit řízení těchto služeb	
• IPAM funkce musí umožnit hierarchické stromové členění adresního prostoru do kontejnerů, subkontejnerů a dále na úroveň sítí. U vytvořených kontejnerů a sítí je následně možná změna jejich velikosti, rozdělení či sjednocení bez nutnosti smazání. Rovněž musí přehledně informovat o zaplněnosti prostoru kontejnerů/sítí, a to též formou mapy a dashboardu (nástěnky) statistik a aktuálních údajů zdraví	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
• Musí umožňovat řídit externí DNS a DHCP postavené na platformě Windows	
• Možnost integrace a podpora centrálního řízení externí BigIP F5	
• Musí umožňovat řídit systém rozvažování mezi datovými centry na stávající platformě (viz popis současného stavu)	
• Podpora HA každého z členských systémů a FT řešení mezi členskými systémy navzájem	
• Musí umožnit vkládání vlastních atributů k jednotlivým objektům (např. lokace) a následně třídění objektů či vyhledávání pomocí těchto vlastních atributů	
• Možnost tvorby vlastních logických pohledů a struktur organizace	
• DNS musí podporovat funkci DNS views pro tvorbu různých obsahů stejných zón. Dále musí plně podporovat DNSSec	
• DHCP musí podporovat automatické rozvažování mezi servery systému tak, aby nedocházelo ke ztrátám adres v poolech	
• Systém poskytnout musí grafické rozhraní a též	
• command line přístup	
• skriptovací API rozhraní (pro programovatelné ovládání)	
• integrovanou možnost importu a exportu všech (nebo vytříděných) objektů a jejich atributů (s možností editace importem)	
• Musí plně podporovat IPv4 i IPv6	
• Musí umožňovat vyhledávání v celé databázi objektů či jejích částech, za využití full textu či regulárních výrazů. S objekty ve výsledku vyhledávání lze pracovat (edit/delete) a exportovat je	
• V rámci jednotlivých kategorií objekty třídit podle vybraných kategoriií, filtrovat je a vyhledávat	
• Zobrazovat přehledné mapy obsazenosti sítí	
• Umožnit delegaci práv systémem Role Based Administration až do úrovně práv ke konkrétnímu objektu, s přehledným nástrojem pro delegaci práv za využití třídění objektů podle rozšířených kategorií a dalších vlastností, uzpůsobený pro nastavování prostředí s velkými počty objektů (např. tisíce sítí a statisíce objektů)	
• Do skupiny systémů tvořící řešení musí být možno přidávat další členy, a to jak formou fyzické appliancí, tak virtuální	
• Řídit přístup uživatelů s možností napojení na AD nebo LDAP	
• Poskytovat nástroje centrální správy celého prostředí DDI – řízený upgrade jednotlivých systémů, centrální konfigurace	
• Napojení a synchronizace s NTP serverem	
• Snadné a centrální zálohování a obnova konfigurace celého prostředí nebo jednotlivých členských systémů	
• Auditní záznamy o změnách konfigurace formou syslog zpráv	
• Komunikace mezi členskými systémy je šifrována a je ověřována na základě certifikátů	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
• Konfigurační změny realizovat formou transakcí (garance dokončení celé změny)	

1.1.9 Optimalizace služby NTP

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.1.10 Upgrade serverů s nepodporovaných operačním systémem (Windows + Linux)

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.1.11 Implementace IPv6 v datových centrech MPSV

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.1.12 Automatizace poskytování KI v DC

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: řadič	
Řadič s redundancí min. N+2	
Všechny řadiče jsou aktivní (režim *all active*)	
Grafické uživatelské rozhraní součástí řešení	
Přístupová práva založená na uživatelských rolích	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Možnost rozdělit správu řešení mezi více vzájemně oddělených organizací (multitenantní řešení)	
Dokumentované programátorské rozhraní pro volání všech dostupných funkcí řadiče, včetně těch, které jsou použity v grafickém uživatelském rozhraní	
Možnost definice aplikačních politik, kde jsou servery (fyzické i virtální) a další koncové stanice členěny do skupin podle své funkce na základě charakteristik, jako je IP adresa, MAC adresa, lokace za určitým portem, příslušnost do VLAN, VXLAN, NVGRE a podobných. Ke skupinám jsou pak definovány na abstraktní úrovni komunikační požadavky vůči jiným skupinám	

1.1.13 Obměna nepodporovaného HW v Datových centrech

Typ zařízení s vyhlášeným ukončením podpory ze strany výrobce	Počet kusů
Zařízení typu A: Supervizor s PN WS-SUP720-3B (doplnění stávajících centr. přepínačů)	4
Zařízení typu B: Centrální WAN směrovač (záložní)	10
Zařízení typu C: Přístupový DC přepínač	4
Zařízení typu D: Karta s PN WS-X4306-GB (doplnění stávajícího centr. přepínače)	2

1.1.13.1 Zařízení typu B: Centrální WAN směrovač (záložní)

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: směrovač	
Formát zařízení: modulární	
Min. 3x10/100/1000Base-TX WAN portů	
Minimální paketový výkon směrovače 700 kpps	
Min. 4 sloty pro rozšiřující moduly	
Směrování IPv4	
Směrování IPv6	
OSPFv2	
BGPv4	
Podpora 4 byte AS numbers in BGP	
First Hop Redundancy Protokol (např. VRRP, HSRP)	
GRE (Generic Routing Encapsulation)	
Policy-based routing podle ACL	
IP Multicast (PIM SSM, PIM SM)	
IGMPv2, IGMPv3	
uRPF	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
First Hop Redundancy Protokol pro IPv6	
OSPFv3	
MP BGP	
MPLS	
MPLS VPN	
Alespoň 50 oddělených (nezávislých) směrovacích tabulek	
MPLS VPN over mGRE	
IPv6 MPLS VPN (6VPE)	
IPv6 Multicast (MLDv1 & v2)	
IPv6 Multicast (PIM SM)	
IPv6 Multicast (PIM SSM)	
uRPF pro IPv6	
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels	
QoS classification – ACL, DSCP, CoS, MPLS based	
QoS marking – DSCP, CoS, MPLS	
QoS Shaping	
Class Based and Priority queuing	
Rate Limiting	
Alespoň tříúrovňový hierarchický QoS	
Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, PING, traceroute)	
ACL na rozhraní IN/OUT	
Zone based firewall	
IPSec AES 256	
Hardwarová akcelerace šifrování pro IPSec AES 256	
Propustnost směrovače min. 95 Mbit/s při aktivovaných službách IPSec šifrování a QoS měřená pro IMIX provoz	
IKEv2	
SHA-2 (SHA-256, SHA-512)	
QoS pre-classification pro IPSec	
Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami (např. pro IPT provoz)	
Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů	
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	
Vynucení QoS parametrů pro takto rozpoznané aplikace a skupiny aplikací – marking, garance šířky pásma pro jednotlivé aplikace, shaping, policing	
Sběr a vyhodnocování statistik a výkonnostních charakteristik aplikačních toků: využívané pásmo, odezvy aplikací	
Monitorování aplikačních toků (za účelem detekce bezpečnostních incidentů) prostřednictvím technologie NetFlow nebo ekvivalentní	
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód	
Podpora minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat)	
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	
SSHv2	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
CLI rozhraní	
SNMPv2/v3	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	
NTPv3 server	

1.1.13.2 ZAŘÍZENÍ TYPU C: PŘÍSTUPOVÝ DC PŘEPÍNAČ

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Formát zařízení: modulární	
Redundantní zdroj	
Celková propustnost přepínače alespoň 1,44 Tbit/s	
Alespoň 48 neblokovaných portů typu 10GE s volitelným fyzickým rozhraním	
Alespoň 6 neblokovaných portů 40GE s volitelným fyzickým rozhraním typu QSFP+	
VXLAN bridging	
VXLAN gateway	
IEEE 802.3ad	
IEEE 802.3ad přes více šasi (Multichassis PortChannel)	
Minimálně 32 linek jako součást PortChannel trunku	
Minimálně 256 konfigurovatelných PortChannel trunků	
Podpora „Jumbo“ rámců alespoň 9216 bajtů	
IEEE 802.1Q	
Minimálně 4000 aktivních VLAN	
Podpora alespoň 256 instancí Spanning-Tree protokolu per VLAN	
IEEE 802.1w – Rapid Spanning Tree Protocol	
Detekce protilehlého zařízení (např. LLDP)	
Minimálně 80000 MAC záznamů	
QoS classification – ACL, DSCP, CoS based	
QoS marking – DSCP, CoS	
QoS – Priority Based Flow Control (IEEE 802.1Qbb)	
WRED	
Minimálně 80000 host IPv4 cest	
First Hop Redundancy Protokol (např. VRRP, HSRP)	
OSPFv2	
BGP	
ECMP přes alespoň 64 cest	
IGMPv2, IGMPv3	
IGMP snooping	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
IP Multicast (PIM SSM, PIM SM)	
Reverse path check (uRPF)	
Virtualizace směrovacích tabulek – např. Virtual Routing and Forwarding (VRF)	
First Hop Redundancy Protokol pro IPv6	
OSPFv3	
MP BGP	
ACL na rozhraní IN/OUT	
Port ACL, VLAN ACL	
Control Plane Policing	
Integrace s VMware vCenter umožňující zobrazit virtuální servery připojené na jednotlivé fyzické porty přepínače	
Integrace s VMware vCenter umožňující automatickou konfiguraci VLAN instancí pro připojení virtuálních serverů	
OpenStack Neutron Plug-in	
Python scripting	
CLI rozhraní	
SSHv2	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	
SNMPv3	
NTP server	
RADIUS klient pro AAA (autentizace, autorizace, accounting)	
TACACS+ klient	
Port mirroring (SPAN)	
Vzdálený port mirroring	
Alespoň 4 SPAN relace	
Syslog	
Role Based Access Control	

1.1.14 Redesign load-balancingu a SSL off-loadingu v DC MPSV

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Výrobce komponent řešení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nasazení čtveřice nezávislých HW zařízení ve funkci load-balancer a SSL akcelerátoru, každý pár v jiné lokalitě DC	
Podpora IPv6	
Možnost připojení min. 8x 10/100/1000BaseTX	
Možnost rozšíření o SFP+ moduly	
Nezávislé rozhraní pro management	
Datová propustnost zařízení alespoň 10 Gbps či více na L4/L7	

Minimální propustnost L4 HTTP požadavků: 1,25 M za sekundu	
Minimální počet současných L4 spojení: 10 M	
SSL akcelerace v HW	
Počet SSL transakcí za sekundu min. 4500 (při použití 2K klíče)	
Počet současných SSL transakcí min. 850 tisíc	
Integrace s nástrojem na detekci zranitelností webových aplikací (separátní projekt)	
Zdvojené napájení	
Možnost doprogramovat si filtrovací pravidla pro aplikace	
Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force)	
Ochrana SMTP a FTP na alikační úrovni	
Podpora SSL (šifrování a dešifrování)	
Podpora různých typů reportů – PCI, geolokační reporty	
Autentikace klientů přes LDAP/Radius	
Možnost aktivovat L4-7 LoadBalancing, ICSA certifikovaný webový a síťový firewall, SSL VPN na jedné platformě HW	
Možnost připojení k monitorovacích nástrojů třetích stran prostřednictvím otevřeného API	
Možnost přidat vlastní funkce pomocí skriptování	
Podpora Active-Active, Active-Pasive módů	
Povolení/zakázání ICMP pro VIP	
Podpora pro TLS 1.2	
Podpora SSL Forward proxy	
Granulární logování / logování per aplikace	
K dispozici jako autonomní box nebo ve formě šasi	
Management: sériový port, GUI, příkazový řádek, iLO	
Podpora alespoň pro 15 metod rozvažování zátěže	
Podpora filtrace paketů	
Podpora ToS, QoS (marking/preservation/mimic)	
Podpora rozvažování zátěže založené na poměrech (ratio based) s CARP perzistencí	
Plná podpora IPv6, IPv4/IPv6 gateway	
Podpora SSL certifikátů podepsaných SHA-2 algoritmem	
Podpora práce s 4096-bit klíči	
Podpora SNMP (v1/v2c/v3)	

1.1.15 Redesign centrálních DC přepínačů (vč. dodávky HW)

1.1.15.1 Architektura komunikační infrastruktury datového centra

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Výrobce komponent řešení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Architektura sítě je typu Spine-Leaf	
Řízení celého řešení pomocí řadiče (controlleru)	
OSPFv2	
BGPv4	
802.1q	
VXLAN bridging	
VXLAN routing	
NVGRE bridging	
NVGRE routing	
Integrace s Hypervisorem VMware vSphere	
Integrace s Hypervisorem Microsoft Hyper-V	
Integrace se zařízením F5 BigIP	
Integrace se zařízením Checkpoint Firewall	

1.1.15.2 PRVEK LEAF

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: přepínač	
Formát zařízení: fixní	
Minimálně 6 portů 40GE formátu QSFP	
Minimálně 48 portů 1/10GE formátu SFP/SFP+	
Neblokující architektura	
Minimálně 96000 záznamů v MAC address tabulce	
IEEE 802.3ad (Link aggregation – LAG)	
IEEE 802.3ad přes více přepínačů v rámci fabric	
Velikost 1RU	
IEEE 802.1Q	
Minimálně 4096 aktivních VLAN	
Minimálně 88000 záznamů IP adres připojených stanic	
Jumbo rámce – min. 9000 bajtů	
Detekce protilehlého zařízení (např. LLDP)	
Minimálně 1000 VRF kontextů	
Minimálně 4 SPAN relace	
Minimálně 128 VXLAN VTEP na VLAN	

1.1.15.3 PRVEK SPINE

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: přepínač	
Formát zařízení: fixní	
Minimálně 32 portů 40GE formátu QSFP	
Neblokující architektura	
Minimálně 96000 záznamů v MAC address tabulce	
IEEE 802.3ad (Link aggregation – LAG)	
IEEE 802.3ad přes více přepínačů v rámci fabric	
Velikost 1RU	
IEEE 802.1Q	
Minimálně 4096 aktivních VLAN	
Minimálně 88000 záznamů IP adres připojených stanic	
Jumbo rámce – min. 9000 bajtů	
Detekce protilehlého zařízení (např. LLDP)	
Minimálně 1000 VRF kontextů	
Minimálně 4 SPAN relace	
Minimálně 128 VXLAN VTEP na VLAN	

1.1.15.4 PRVEK ILO/LOM PŘEPÍNAČ

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: přepínač	
Formát zařízení: fixní	
Dva dedikované stohovací porty	
Možnost mít alespoň 8 zařízení ve stohu	
Minimální kapacita sběrnice stohu 80 Gb/s	
Minimálně 48 portů 10/100/1000 Base-TX	
Minimálně 4 1GE uplink porty s volitelným fyzickým rozhraním	
Jeden osazený 1GE port modulem 1000Base-SX	
Minimálně 16000 záznamů v MAC address tabulce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
IEEE 802.3ad (Link aggregation – LAG)	
IEEE 802.3ad přes více přepínačů ve stohu	
Minimálně 8 linek jako součást LAG trunku	
Minimálně 20 konfigurovatelných LAG trunků	
IEEE 802.1Q	
Minimálně 1000 aktivních VLAN	
IEEE 802.1w – Rapid Spanning Tree Protocol	
Jumbo rámce – min. 9190 bytes	
Detekce protilehlého zařízení (např. LLDP)	
IGMPv2/IGMPv3 snooping	
IPv6 services (SSH, Syslog)	
IPv6 QoS	
IPv6 MLDv1 & v2 snooping	
IPv6 First Hop Security (Port ACL, RA guard)	
IPv6 ACL	
QoS classification – ACL, DSCP, CoS based	
QoS marking – DSCP, CoS	
QoS – Strict Priority Queue	
IEEE 802.1x	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	
Možnost provozu 802.1x v tzv. monitorovacím módu bez omezování přístupu koncových uživatelů	
RADIUS CoA (RFC 5176)	
IEEE 802.1x Multi-domain authentication	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové IP adresy	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	
Možnost definovat povolené MAC adresy na portu	
Monitorování aplikačních toků prostřednictvím technologie NetFlow nebo ekvivalentní technologie	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	
Interní nástroje pro debugging procházejícího provozu	
DHCP server	
SSHv2	
CLI rozhraní	
SNMPv2/v3	
TACACS+ nebo RADIUS klient pro AAA	
Vzdálený port mirroring (RSPAN)	
L2 traceroute	

1.2 Oblast komunikační infrastruktury

1.2.1 Celková analýza měnících se požadavků na KI a návrh efektivního zajištění souladu služeb poskytovaných KI

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.2 Implementace šifrování ve WAN MPSV

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.3 Unifikace IP VPN ve WAN MPSV

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.4 Migrace Ethernet spojnic na IP VPN, nasazení šifrování, redukce počtu směrovačů

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.5 Změna telekomunikačního operátora

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.6 Systém pro discovery sítě

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Automatické rozpoznání všech zařízení v síti	
Možnost vyhledávání nových zařízení	
Možnost zobrazování změn v síti oproti předchozímu sběru (discovery)	
Schopnost rozpoznávat typ zařízení dle MAC adresy	
Podpora SNMP i HTTP při discovery	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Podpora CDP, LLDP, ARP při discovery	
Možnost aktualizace popisů rozhraní síťových zařízení (zápisem na zařízení)	
Možnost kontroly dodržování konvence popisů rozhraní síťových zařízení	
Možnost aktualizace hodnot Location a Contact u síťových zařízení	
Možnost zobrazení topologie KI	
Možnost vázat zařízení na seznamy Part Number od dodavatelů zařízení	
Schopnost rozpoznání síťových zařízení ve stohu	
Schopnost identifikace Serial Number zařízení	
Schopnost identifikace Serial Number modulů síťových prvků	
Schopnost jednoznačně identifikovat zapojení modulů, aby nedocházelo k duplicitám v dokumentaci	
Schopnost identifikovat operační systém včetně verze	
Reportovací a sumarizační vlastnosti	
Schopnost sestavit report využití rozhraní síťových prvků	
Schopnost sestavit report využití modulů pro modulární zařízení	
Schopnost sestavit report připojení uživatelských telefonních přístrojů včetně telefonního čísla a jména uživatele	
Schopnost sestavit report použitých IP adres	
Schopnost sestavit report použitých MAC adres	
Schopnost sestavit report použitých Interface, VLAN	
Schopnost sestavit report použitých VLAN	
Schopnost sestavit report pro identifikaci nemanagovatelných zařízení (HUB)	
Schopnost sestavit sumární report použitého hardwaru	
Schopnost exportovat topologické mapy v grafickém formátu Visio	
Schopnost exportovat topologické mapy v xml formátu Visio	
Schopnost exportovat topologické mapy v xml formátu ePD	
Propojení s ostatními systémy	
Schopnost propojení se systémem pro dohled dostupnosti zařízení (viz příloha č. 10 – Popis současného stavu komunikační a systémové infrastruktury a WAN MPSV)	
Schopnost propojení s centrálním systémem sledování výkonnosti (viz příloha č. 10)	
Schopnost propojení se systémem monitorování provozu v síti (viz příloha č. 10)	
Schopnost propojení s centrálním systémem správy chybových stavů (viz příloha č. 10)	

1.2.7 MOBILITA UŽIVATELŮ – BEZDRÁTOVÉ PŘIPOJENÍ DO KI MPSV

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: bezdrátový řadič (wireless controller)	
Formát zařízení: fixní	
Minimálně 8 SFP Gigabit Ethernet portů	
Řízení a centrální správa přístupových bodů kdekoliv v síti	
Podpora 50 přístupových bodů	
Možnost rozšíření podporovaných přístupových bodů až na 500	
Podpora 802.11ac	
Aktivní centrální správa radiofrekvenčního spektra, realtime a historické informace o výkonu a rušení v používaném spektru	
Detekce podvržených a cizích přístupových bodů a ad-hoc klientů na všech dostupných kanálech, detekce základních typů útoků na bezdrátovou infrastrukturu	
Aplikační inspekce přenášeného uživatelského provozu, možnost řízení provozu na základě rozpoznaných aplikací	
Podpora autentizace přes centrální autentikační systém dodaný v projektu „Vytvoření systému infrastrukturní autentizace“	
Řízený přístup pro návštěvníky přes web portál a jednorázově vygenerovaná hesla, tunelování návštěvnického provozu až do DMZ	
Možnost rozvoje konceptu BYOD, možnost automatického přiřazení bezpečnostní politiky na základě způsobu autentizace a typu/výrobce klienta	
Podpora IPv4/IPv6 protokolu pro management bezdrátové infrastruktury	
Podpora pro IPv4/IPv6 klientů, podpora mechanismů IPv4/IPv6 First Hop Security	

1.2.8 Profylaxe KI v DC a WAN MPSV

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.9 Rekognoskace aktuálního stavu UPS pro síťové prvky v DC a WAN MPSV

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.10 SNMP MODULY DO UPS (BEZ DODÁVKY HW)

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.11 IPV6 ADRESNÍ PLÁN WAN

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.12 IMPLEMENTACE IPV6 VE WAN SÍTI MPSV

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.13 AKCELERACE VE WAN SÍTI

1.2.13.1 PRVEK AKCELERÁTOR DO DC

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: zařízení pro akceleraci aplikací ve WAN	
Typické pozicování zařízení: centrála nebo DC	
Formát zařízení appliancí	
Velikost max. 2RU	
Minimálně 12 portů 10/100/1000Base-TX	
Stavová redundance jednotlivých spojení mezi zařízeními	
Možnost rozšíření o optické 1GE porty	
Možnost rozšíření o optické 10GE porty	
Minimálně 16000 optimalizovaných TCP spojení	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Požadavky na redukci přenášených dat	
Zařízení musí poskytnout cachovací techniky na pevném disku pro redukci přenášených dat po WAN	
Obsah dočasně uložených dát na disku musí být šifrovaný standardem FIPS 140-2 level 2, 256-bit AES	
Zařízení musí dovolit vzorkování binárních dat a jejich zpětné rozeznávaní, tak aby bylo možné přenášet změny provedené v souborech a obnovení zbytku obsahu ze vzorků v cache	
Zařízení musí disponovat kompresí na úrovni bytů, ne na úrovni souborů, tak aby docházelo k přenášení změn a ne celých souborů	
Zařízení musí přizpůsobit ukládání vzorků binárních dat (šetřit kapacitu cache) primárnímu směru toku dat jednotlivých aplikací (např. při virtualizaci desktopů)	
Zařízení musí využívat uložených vzorků v centrálním zařízení pro více vzdálených lokalit (šetřit kapacitu cache, zvýšit škálování)	
Řešení musí být transparentní pro síťovou infrastrukturu (zachovávat klíčové informace o datových tocích) a neovlivňovat chování nástrojů závislých na informacích v TCP/IP záhlaví, zejména s ohledem na technologie netflow, QoS, firewall	
Řešení musí podporovat možnost zachování ToS/DSCP QoS značky na optimalizovaných spojeních	
Vlastnosti akcelerace TCP/IP	
TCP akcelerace (libovolná metoda změny velikosti okna, selektivní potvrzování nebo kombinace) může být použita jedině v případě zachování datové integrity	
Pro TCP akceleraci musí být použito doporučení ze standardů RFC 1323, RFC 2018, RFC 3390	
TCP akcelerace musí být transparentní, tj. zachovávat IP a TCP údaje obsažené v hlavičce paketu (zdrojové a cílové IP adresy, čísla TCP portů, QoS)	
Akcelerační zařízení musí být schopno přizpůsobit WAN optimalizaci chování linky (latence, ztrátovost paketů)	
Vlastnosti akcelerace CIFS	
Akcelerační zařízení musí poskytnout lokálně metadata CIFS a být schopno dočasně uchovat caching-metadata, jako jsou atributy souborů nebo adresářová struktura	
Funkce pro zrychlení protokolu a minimalizaci aplikačního zpoždění, včetně načítání aplikací v předstihu, předvídání výpočetních operací, multiplexing datových přenosů, zřetězené zpracování dat (pipelining) a dávkové zpracování výpočetních operací (operation batching)	
Nevyžaduje žádné změny v autentifikačních či autorizačních konfiguracích Windows jako např. v Microsoft Active directory	
Plná podpora autentifikace systémů Windows NT LAN Manager a Kerberos pro žádosti v protokolu CIFS	
Nikdy si nepřivlastňuje vzorovou kopii souboru nebo datového prvku ani stav zamykání souborů	
Plně zachovává a dodržuje sémantiku protokolu, chrání soudržnost dat a směrodatnou kopii musí vždy vlastnit výchozí zařízení	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Centralizovaně řízená distribuce dat a služba přednačítání obsahu, tedy možnost centrálně přesouvat soubory do pobočkových zařízení	
Možnost přístupu k souboru i při výpadku konektivity WAN dle definovaných pravidel	
Vlastnosti akcelerace aplikací	
Akcelerační zařízení musí podporovat akceleraci HTTP	
Akcelerační zařízení musí podporovat akceleraci SSL	
Akcelerační zařízení musí podporovat přechod z optimalizovaného HTTP na optimalizované SSL během navazování spojení	
Akcelerační zařízení musí podporovat akceleraci CIFS	
Akcelerační zařízení musí podporovat ověřování platnost certifikátů (např. OSCP protokol)	
Akcelerační zařízení musí podporovat ověřování pomocí klientských i serverových certifikátů	
Zařízení musí podporovat licencovanou akceleraci MAPI	
Zařízení musí podporovat licencovanou akceleraci Encrypted MAPI	
Zařízení musí dovolovat škálování pro nové aplikace bez požadavků na rekonfiguraci	
Print Services: zařízení musí podporovat akceleraci tiskových služeb pro pobočkový a centrální tisk včetně distribuce/managementu tiskových driverů	
Microsoft SMS: podpora akcelerace SMS	
Akcelerační zařízení musí podporovat akceleraci SMBv2	
Akcelerační zařízení musí podporovat akceleraci ICA, včetně ICA over SSL	
Management	
Řešení musí dovolit kompletní centrální správu všech akceleračních zařízení centrálním managementem	
Řešení musí poskytnout nástroje na odstraňování problémů	
Řešení musí poskytnout nástroje pro odeslání upozornění pomocí SNMP TRAP, SMTP nebo SYSLOG	
Management musí být možné konfigurovat jako redundantní do geograficky oddělených datových center s L3 konektivitou	
Autentizace správců pomocí RADIUS nebo LDAP	
Řešení může umožnit nastavení rolí pro jednotlivé správce a skupiny správců (RBAC)	
Řešení musí podporovat SNMPv3	
Komunikace managementu a akceleračních zařízení musí být zabezpečená/šifrovaná	
Přístup správců k lokálnímu managementu akceleračních zařízení musí být zabezpečen/šifrován metodami ssh, https	
Sběr a prezentace dat výkonností aplikací ze vzdálených lokalit v centrálním managementu	
Řešení musí umožnit automatickou instalaci a konfiguraci vzdáleného akceleračního zařízení	
Export dat pomocí protokolu NetFlow v9	
Možnosti implementace	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Zařízení musí dovolit flexibilní nasazení mimo cestu (WCCP, PBR) a/nebo nasazení transparentně přímo do cesty	
Zařízení musí umožňovat dynamickou formaci dvojic odpovědných za akceleraci a de-akceleraci toků (peer autodiscovery)	
Možnost rozšiřování WAN optimalizace bez jejího přerušení	
Řešení s daným zařízením musí podporovat load-sharing přes několik akceleračních zařízení v případě, že jedno nedovede obsloužit všechny požadavky	
Schopnost flexibilního a elastického rozšiřování – kombinace fyzických WAN optimalizátorů i virtuálních optimalizátorů (běžící v prostředí VMware apod.) do jedné sady/skupiny	
Automatické rovnoměrné rozkládání zátěže mezi optimalizátory v dané skupině	
Automatické rozkládání zátěže mezi optimalizátory v dané skupině, nebo mezi skupiny optimalizátorů dle konfigurovatelných politik či aplikací či v případě vzájemného zálohování	
Řešení s daným zařízením musí podporovat redundantní WAN linky a asymetrické směrování v infrastruktuře při zachováním akcelerace	
Zařízení musí být schopno transparentně propouštět neakcelerovaný provoz	
Zařízení musí být schopno akcelerovat selektivně podle L2 VLAN	
Jedno zařízení musí být schopno akcelerovat provoz ve více VRF současně se zachováním oddělení provozu	
Automatické vyhledávání a identifikace „peer“ akceleračních zařízení pro in-line i off-path implementace	
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu samostatné appliance	
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu modulu do směrovače	
Zařízení musí akcelerovat i proti "peer" zařízení tvořeném vlastním směrovačem bez přídavných modulů	
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu virtuálního zařízení v VMWare	

1.2.13.2 PRVEK AKCELERÁTOR PRO VELKOU POBOČKU

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: zařízení pro akceleraci aplikací ve WAN	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typické pozicování zařízení: pobočka	
Formát zařízení: univerzální modul do směrovače nebo appliance	
Minimálně 1200 optimalizovaných TCP spojení	
Požadavky na redukci přenášených dat	
Zařízení musí poskytnout cachovací techniky na pevném disku pro redukci přenášených dat po WAN	
Obsah dočasně uložených dát na disku musí být šifrovaný standardem FIPS 140-2 level 2, 256-bit AES	
Zařízení musí dovolit vzorkování binárních dat a jejich zpětné rozeznávaní, aby bylo možné přenášet změny provedené v souborech a obnovení zbytku obsahu ze vzorků v cache	
Zařízení musí disponovat kompresí na úrovni bytů, ne na úrovni souborů, aby docházelo k přenášení změn a ne celých souborů	
Zařízení musí přizpůsobit ukládání vzorků binárních dat (šetřit kapacitu cache) primárnímu směru toku dat jednotlivých aplikací (např. při virtualizaci desktopů)	
Zařízení musí využívat uložených vzorků v centrálním zařízení pro více vzdálených lokalit (šetřit kapacitu cache, zvýšit škálování)	
Řešení musí být transparentní pro síťovou infrastrukturu (zachovávat klíčové informace o datových tocích) a neovlivňovat chování nástrojů závislých na informacích v TCP/IP záhlaví, zejména s ohledem na technologie netflow, QoS, firewall	
Řešení musí podporovat možnost zachování ToS/DSCP QoS značky na optimalizovaných spojeních	
Vlastnosti akcelerace TCP/IP	
TCP akcelerace (libovolná metoda změny velikosti okna, selektivní potvrzování nebo kombinace) může být použita jedině v případě zachování datové integrity	
Pro TCP akceleraci musí být použito doporučení ze standardů RFC 1323, RFC 2018, RFC 3390	
TCP akcelerace musí být transparentní, tj. zachovávat IP a TCP údaje obsažené v hlavičce paketu (zdrojové a cílové IP adresy, čísla TCP portů, QoS)	
Akcelerační zařízení musí být schopno přizpůsobit WAN optimalizaci chování linky (latence, ztrátovost paketů)	
Vlastnosti akcelerace CIFS	
Akcelerační zařízení musí poskytnout lokálně metadata CIFS a být schopno dočasně uchovat caching-metadata, jako jsou atributy souborů nebo adresářová struktura	
Akcelerační zařízení musí poskytnout lokální úložiště pro pobočkové uživatele	
Funkce pro zrychlení protokolu a minimalizaci aplikačního zpoždění, včetně načítání aplikací v předstihu, předvídání výpočetních operací, multiplexing datových přenosů, zřetězené zpracování dat (pipelining) a dávkové zpracování výpočetních operací (operation batching)	
Nevyžaduje žádné změny v autentifikačních či autorizačních konfiguracích Windows jako např. v Microsoft Active directory	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Plná podpora autentizace systémů Windows NT LAN Manager a Kerberos pro žádosti v protokolu CIFS	
Nikdy si nepřivlastňuje vzorovou kopii souboru nebo datového prvku ani stav zamykání souborů	
Plně zachovává a dodržuje sémantiku protokolu, chrání soudržnost dat a směrodatnou kopii musí vždy vlastnit výchozí zařízení	
Centralizovaně řízená distribuce dat a služba přednačítání obsahu, tedy možnost centrálně přesouvat soubory do pobočkových zařízení	
Možnost přístupu k souboru i při výpadku konektivity WAN dle definovaných pravidel	
Vlastnosti akcelerace aplikací	
Akcelerační zařízení musí podporovat akceleraci HTTP	
Akcelerační zařízení musí podporovat akceleraci SSL	
Akcelerační zařízení musí podporovat přechod z optimalizovaného HTTP na optimalizované SSL během navazování spojení	
Akcelerační zařízení musí podporovat akceleraci CIFS	
Možnost rozšíření o využívání internetových content distribution nebo content cahcing služeb (např. Akamai)	
Akcelerační zařízení musí podporovat ověřování platnost certifikátů (např. OSCP protokol)	
Akcelerační zařízení musí podporovat ověřování pomocí klientských i serverových certifikátů	
Zařízení musí podporovat licencovanou akceleraci MAPI	
Zařízení musí podporovat licencovanou akceleraci Encrypted MAPI	
Zařízení musí dovolovat škálování pro nové aplikace bez požadavků na rekonfiguraci	
Print Services: zařízení musí podporovat akceleraci tiskových služeb pro pobočkový a centrální tisk včetně distribuce/managementu tiskových driverů	
Microsoft SMS: podpora akcelerace SMS	
Akcelerační zařízení musí podporovat akceleraci SMBv2	
Akcelerační zařízení musí podporovat akceleraci ICA, včetně ICA over SSL	
Management	
Řešení musí dovolit kompletní centrální správu všech akceleračních zařízení centrálním managementem	
Řešení musí poskytnout nástroje na odstraňování problémů	
Řešení musí poskytnout nástroje pro odeslání upozornění pomocí SNMP TRAP, SMTP nebo SYSLOG	
Management musí být možné konfigurovat jako redundantní do geograficky oddělených datových center s L3 konektivitou	
Autentizace správců pomocí RADIUS nebo LDAP	
Řešení může umožnit nastavení rolí pro jednotlivé správce a skupiny správců (RBAC)	
Řešení musí podporovat SNMPv3	
Komunikace managementu a akceleračních zařízení musí být zabezpečená/šifrovaná	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Přístup správců k lokálnímu managementu akceleračních zařízení musí být zabezpečen/šifrován metodami ssh, https	
Detailní rozpoznání a klasifikace přenášených aplikací (Deep Packet Inspection)	
Vynucování politik dle detailního rozpoznání aplikací	
Sběr a prezentace dat výkonností aplikací ze vzdálených lokalit v centrálním managementu	
Řešení musí umožnit automatickou instalaci a konfiguraci vzdáleného akceleračního zařízení	
Export dat pomocí protokolu NetFlow v9	
Možnosti implementace	
Zařízení musí dovolit flexibilní nasazení mimo cestu (WCCP, PBR) a/nebo nasazení transparentně přímo do cesty	
Zařízení musí umožňovat dynamickou formaci dvojic odpovědných za akceleraci a de-akceleraci toků (peer autodiscovery)	
Řešení s daným zařízením musí podporovat load-sharing přes několik akceleračních zařízení v případě, že jedno nedovede obsloužit všechny požadavky	
Řešení s daným zařízením musí podporovat redundantní WAN linky a asymetrické směrování v infrastruktuře při zachování akcelerace	
Jedno zařízení musí být schopno akcelerovat provoz ve více VRF současně se zachováním oddělení provozu	
Automatické vyhledávání a identifikace „peer“ akceleračních zařízení pro in-line i off-path implementace	
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu samostatné appliance	
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu modulu do směrovače	
Zařízení musí akcelerovat i proti "peer" zařízení tvořenému vlastním směrovačem bez přídavných modulů	
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu virtuálního zařízení v VMware	

1.2.13.3 PRVEK AKCELERÁTOR PRO MALOU POBOČKU

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: zařízení pro akceleraci aplikací ve WAN	
Typické pozicování zařízení: pobočka	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Formát zařízení appliancí	
Velikost maximálně 1RU	
Minimálně 2 porty 10/100/1000Base-TX	
Možnost rozšíření o rozhraní s možností HW bypassu	
Minimálně 8 dostupných modulů 1000Base-T rozhraní s možností HW bypassu	
Možnost hostování minimálně dvou virtuálních serverů	
Minimálně 200 optimalizovaných TCP spojení	
Požadavky na redukci přenášených dat	
Zařízení musí poskytnout cachovací techniky na pevném disku pro redukci přenášených dat po WAN	
Obsah dočasně uložených dát na disku musí být šifrován standardem FIPS 140-2 level 2, 256-bit AES	
Zařízení musí dovolit vzorkování binárních dat a jejich zpětné rozeznávání, aby bylo možné přenášet změny provedené v souborech a obnovení zbytku obsahu ze vzorků v cache	
Zařízení musí disponovat kompresí na úrovni bytů, ne na úrovni souborů, aby docházelo k přenášení změn a ne celých souborů	
Zařízení musí přizpůsobit ukládání vzorků binárních dat (šetřit kapacitu cache) primárnímu směru toku dat jednotlivých aplikací (např. při virtualizaci desktopů)	
Zařízení musí využívat uložených vzorků v centrálním zařízení pro více vzdálených lokalit (šetřit kapacitu cache, zvýšit škálování)	
Řešení musí být transparentní pro síťovou infrastrukturu (zachovávat klíčové informace o datových tocích) a neovlivňovat chování nástrojů závislých na informacích v TCP/IP záhlaví, zejména s ohledem na technologie netflow, QoS, firewall	
Řešení musí podporovat možnost zachování ToS/DSCP QoS značky na optimalizovaných spojeních	
Možnost instalace Windows Server Core 2008 ve virtuálním prostředí pro následující služby: AD, DNS, DHCP, Print	
Vlastnosti akcelerace TCP/IP	
TCP akcelerace (libovolná metoda změny velikosti okna, selektivní potvrzování nebo kombinace) může být použita jen v případě zachování datové integrity	
Pro TCP akceleraci musí být použito doporučení ze standardů RFC 1323, RFC 2018, RFC 3390	
TCP akcelerace musí být transparentní, tj. zachovávat IP a TCP údaje obsažené v hlavičce paketu (zdrojové a cílové IP adresy, čísla TCP portů, QoS)	
Akcelerační zařízení musí být schopno přizpůsobit WAN optimalizaci chování linky (latence, ztrátovost paketů)	
Vlastnosti akcelerace CIFS	
Akcelerační zařízení musí poskytnout lokálně metadata CIFS a být schopno dočasně uchovat caching-metadata, jako jsou atributy souborů nebo adresářová struktura	
Akcelerační zařízení musí poskytnout lokální úložiště pro pobočkové uživatele	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Funkce pro zrychlení protokolu a minimalizaci aplikačního zpoždění, včetně načítání aplikací v předstihu, předvídání výpočetních operací, multiplexing datových přenosů, zřetězené zpracování dat (pipelining) a dávkové zpracování výpočetních operací (operation batching)	
Nevyžaduje žádné změny v autentifikačních či autorizačních konfiguracích Windows jako např. v Microsoft Active directory	
Plná podpora autentifikace systémů Windows NT LAN Manager a Kerberos pro žádosti v protokolu CIFS	
Nikdy si nepřivlastňuje vzorovou kopii souboru nebo datového prvku ani stav zamykání souborů	
Plně zachovává a dodržuje sémantiku protokolu, chrání soudržnost dat a směrodatnou kopii musí vždy vlastnit výchozí zařízení	
Centralizovaně řízená distribuce dat a služba přednačítání obsahu, tedy možnost centrálně přesouvat soubory do pobočkových zařízení	
Možnost přístupu k souboru i při výpadku konektivity WAN dle definovaných pravidel	
Vlastnosti akcelerace aplikací	
Akcelerační zařízení musí podporovat akceleraci HTTP	
Akcelerační zařízení musí podporovat akceleraci SSL	
Akcelerační zařízení musí podporovat přechod z optimalizovaného HTTP na optimalizované SSL během navazování spojení	
Akcelerační zařízení musí podporovat akceleraci CIFS	
Možnost rozšíření o využívání internetových content distribution nebo content cahcing služeb (např. Akamai)	
Akcelerační zařízení musí podporovat ověřování platnost certifikátů (např. OSCP protokol)	
Akcelerační zařízení musí podporovat ověřování pomocí klientských i serverových certifikátů	
Zařízení musí podporovat licencovanou akceleraci MAPI	
Zařízení musí podporovat licencovanou akceleraci Encrypted MAPI	
Zařízení musí dovolovat škálování pro nové aplikace bez požadavků na rekonfiguraci	
Print Services: zařízení musí podporovat akceleraci tiskových služeb pro pobočkový a centrální tisk včetně distribuce/managementu tiskových driverů	
Microsoft SMS: podpora akcelerace SMS	
Akcelerační zařízení musí podporovat akceleraci SMBv2	
Akcelerační zařízení musí podporovat akceleraci ICA, včetně ICA over SSL	
Management	
Řešení musí dovolit kompletní centrální správu všech akceleračních zařízení centrálním managementem	
Řešení musí poskytnout nástroje na odstraňování problémů	
Řešení musí poskytnout nástroje pro odeslání upozornění pomocí SNMP TRAP, SMTP nebo SYSLOG	
Management musí být možné konfigurovat jako redundantní do geograficky oddělených datových center s L3 konektivitou	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Autentizace správců pomocí RADIUS nebo LDAP	
Řešení může umožnit nastavení rolí pro jednotlivé správce a skupiny správců (RBAC)	
Řešení musí podporovat SNMPv3	
Komunikace managementu a akceleračních zařízení musí být zabezpečená/šifrovaná	
Přístup správců k lokálnímu managementu akceleračních zařízení musí být zabezpečen/šifrován metodami ssh, https	
Možnost instalace RMONv1, v2 sondy jako doplněk, virtuální stroj do akceleračního zařízení	
Řešení pobočky musí implementovat detailní rozpoznání a klasifikace přenášených aplikací (Deep Packet Inspection)	
Řešení pobočky musí implementovat vynucování politik dle detailního rozpoznání aplikací	
Sběr a prezentace dat výkonností aplikací ze vzdálených lokalit v centrálním managementu	
Řešení musí umožnit automatickou instalaci a konfiguraci vzdáleného akceleračního zařízení	
Export dat pomocí protokolu NetFlow v9	
Možnosti implementace	
Zařízení musí dovolit flexibilní nasazení mimo cestu (WCCP, PBR) a/nebo nasazení transparentně přímo do cesty	
Zařízení musí umožňovat dynamickou formaci dvojic odpovědných za akceleraci a de-akceleraci toků (peer autodiscovery)	
Řešení s daným zařízením musí podporovat load-sharing přes několik akceleračních zařízení v případě, že jedno nedovede obsloužit všechny požadavky	
Řešení s daným zařízením musí podporovat redundantní WAN linky a asymetrické směrování v infrastruktuře při zachování akcelerace	
Zařízení musí být schopno transparentně propouštět neakcelerovaný provoz	
Jedno zařízení musí být schopno akcelerovat provoz ve více VRF současně se zachováním oddělení provozu	
Automatické vyhledávání a identifikace „peer“ akceleračních zařízení pro in-line i off-path implementace	
Zařízení musí akcelerovat i proti „peer“ zařízení, které je ve formátu samostatné appliance	
Zařízení musí akcelerovat i proti „peer“ zařízení, které je ve formátu modulu do směrovače	
Zařízení musí akcelerovat i proti „peer“ zařízení tvořenému vlastním směrovačem bez přídavných modulů	
Zařízení musí akcelerovat i proti „peer“ zařízení, které je ve formátu virtuálního zařízení VMware	

1.2.14 AUDIT ACL VE WAN

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.15 Řízení přístupu k datovým zdrojům podle rolí (vč. relevantní obměny HW)

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.16 Centrální ovládání komunikační infrastruktury ve WAN MPSV

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.17 Logické oddělení managementu aktivních prvků, datového provozu a řídicího provozu pro virtualizační platformu

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.18 Facility management

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.2.19 Obměna nepodporovaného HW ve WAN

Typ zařízení s vyhlášeným ukončením podpory ze strany výrobce	Počet kusů
Zařízení typu E: přepínač pro lokalitu 4. úrovně, 48 portů s napájením	65
Zařízení typu F: přepínač pro lokalitu 4. úrovně, 24 portů, z toho min. 8 portů s napájením	230
Zařízení typu G: přepínač pro lokalitu 4. úrovně, 24 portů s napájením	75
Zařízení typu H: směrovač pro lokalitu 4. úrovně	230
Zařízení typu I: směrovač pro lokalitu 3. úrovně a 4. úrovně s větší přípojkou	125
Zařízení typu J: přepínač pro lokalitu 3. úrovně, 48 portů s napájením	280
Zařízení typu K: přepínač pro lokalitu 3. úrovně, 24 portů s napájením	340
Zařízení typu L: kompaktní přepínač, 8 portů s napájením	20
Zařízení typu M: agregační optický přepínač	2

1.2.19.1 Zařízení typu E: přepínač pro lokalitu 4. úrovně, 48 portů s napájením

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: L2 přepínač	
Formát zařízení: fixní	
Dva dedikované stohovací porty	
Možnost mít alespoň 6 zařízení ve stohu	
Minimální kapacita sběrnice stohu 80 Gb/s	
Minimálně 48 portů 10/100/1000 Base-TX s PoE	
Celkový příkon pro PoE porty min. 740 W	
IEEE 802.1at pro alespoň 24 portů najednou (tzn. dostupný příkon pro každý port min. 30 W)	
IEEE 802.1af pro všech 48 portů najednou (tzn. dostupný příkon pro každý port min. 15,4 W)	
Minimálně 4 1GE uplink porty s volitelným fyzickým rozhraním (porty použité pro stohování nelze započítat jako uplink port)	
IEEE 802.3ad (Link aggregation – LAG)	
IEEE 802.3ad přes více přepínačů ve stohu	
Minimálně 8 linek jako součást LAG trunku	
Minimálně 20 konfigurovatelných LAG trunků	
IEEE 802.1Q	
Minimálně 64 aktivních VLAN	
IEEE 802.1w – Rapid Spanning Tree Protocol	
Jumbo rámce – min. 9190 bajtů	
Detekce protilehlého zařízení (např. LLDP)	
IGMPv2/IGMPv3 snooping	
IPv6 services (SSH, Syslog)	
IPv6 QoS	
IPv6 MLDv1 & v2 snooping	
IPv6 First Hop Security (Port ACL, RA guard)	
IPv6 ACL	
QoS classification – ACL, DSCP, CoS based	
QoS marking – DSCP, CoS	
QoS – Strict Priority Queue	
Alespoň 8 HW QoS front	
IEEE 802.1x	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	
Možnost provozu 802.1x v tzv. monitorovacím módu bez omezování přístupu koncových uživatelů	
RADIUS CoA (RFC 5176)	
IEEE 802.1x Multi-domain authentication	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové IP adresy	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	
Source-Group Tag Exchange Protocol	
Možnost definovat povolené MAC adresy na portu	
Monitorování aplikačních toků prostřednictvím technologie NetFlow nebo ekvivalentní technologie	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	
Interní nástroje pro debugging procházejícího provozu	
DHCP server	
SSHv2	
CLI rozhraní	
SNMPv2/v3	
TACACS+ nebo RADIUS klient pro AAA	
Vzdálený port mirroring (RSPAN)	

1.2.19.2 Zařízení typu F: přepínač pro lokalitu 4. úrovně, 24 portů, z toho min. 8 portů s napájením

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: L2 přepínač	
Formát zařízení: fixní	
Minimálně 24 portů 10/100/1000 Base-TX, z toho alespoň 8 s podporou PoE	
Minimálně 2 1GE uplink porty s volitelným fyzickým rozhraním a min. 2 uplink porty 10/100/1000 Base-TX	
Celkový příkon pro PoE porty min. 110W	
Podpora IEEE 802.1at pro alespoň 3 porty najednou (tzn. dostupný příkon pro každý port min. 30 W)	
Podpora IEEE 802.1af pro alespoň 7 portů najednou (tzn. dostupný příkon pro každý port min. 15,4 W)	
IEEE 802.3ad (Link aggregation – LAG)	
IEEE 802.3ad přes více přepínačů ve stohu	
Minimálně 8 linek jako součást LAG trunku	
Minimálně 20 konfigurovatelných LAG trunků	
IEEE 802.1Q	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Minimálně 64 aktivních VLAN	
IEEE 802.1w – Rapid Spanning Tree Protocol	
Jumbo rámce – min. 9190 bytes	
Detekce protilehlého zařízení (např. LLDP)	
IGMPv2/IGMPv3 snooping	
IPv6 services (SSH, Syslog)	
IPv6 QoS	
IPv6 MLDv1 & v2 snooping	
IPv6 First Hop Security (Port ACL, RA guard)	
IPv6 ACL	
QoS classification – ACL, DSCP, CoS based	
QoS marking – DSCP, CoS	
QoS – Strict Priority Queue	
Alespoň 8 HW QoS front	
IEEE 802.1x	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	
Možnost provozu 802.1x v tzv. monitorovacím módu bez omezování přístupu koncových uživatelů	
RADIUS CoA (RFC 5176)	
IEEE 802.1x Multi-domain authentication	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové IP adresy	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	
Source- Group Tag Exchange Protocol	
Možnost definovat povolené MAC adresy na portu	
Monitorování aplikačních toků prostřednictvím technologie NetFlow nebo ekvivalentní technologie	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	
Interní nástroje pro debugging procházejícího provozu	
DHCP server	
SSHv2	
CLI rozhraní	
SNMPv2/v3	
TACACS+ nebo RADIUS klient pro AAA	
Vzdálený port mirroring (RSPAN)	

1.2.19.3 Zařízení typu G: přepínač pro lokalitu 4. úrovně, 24 portů s napájením

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: L2 přepínač	
Formát zařízení: fixní	
Dva dedikované stohovací porty	
Možnost mít alespoň 6 zařízení ve stohu	
Minimální kapacita sběrnice stohu 80 Gb/s	
Minimálně 24 portů 10/100/1000 Base-TX s PoE	
Celkový příkon pro PoE porty min. 370 W	
Podpora IEEE 802.1at pro alespoň 12 portů najednou (tzn. dostupný příkon pro každý port min. 30 W)	
Podpora IEEE 802.1af pro všech 24 portů najednou (tzn. dostupný příkon pro každý port min. 15,4 W)	
Minimálně 4 1GE uplink porty s volitelným fyzickým rozhraním (porty použité pro stohování nelze započítat jako uplink port)	
IEEE 802.3ad (Link aggregation – LAG)	
IEEE 802.3ad přes více přepínačů ve stohu	
Minimálně 8 linek jako součást LAG trunku	
Minimálně 20 konfigurovatelných LAG trunků	
IEEE 802.1Q	
Minimálně 64 aktivních VLAN	
IEEE 802.1w – Rapid Spanning Tree Protocol	
Jumbo rámce – min. 9190 bytes	
Detekce protilehlého zařízení (např. LLDP)	
IGMPv2/IGMPv3 snooping	
IPv6 services (SSH, Syslog)	
IPv6 QoS	
IPv6 MLDv1 & v2 snooping	
IPv6 First Hop Security (Port ACL, RA guard)	
IPv6 ACL	
QoS classification – ACL, DSCP, CoS based	
QoS marking – DSCP, CoS	
QoS – Strict Priority Queue	
Alespoň 8 HW QoS front	
IEEE 802.1x	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	
Možnost provozu 802.1x v tzv. monitorovacím módu bez omezování přístupu koncových uživatelů	
RADIUS CoA (RFC 5176)	
IEEE 802.1x Multi-domain authentication	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové IP adresy	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	
Source- Group Tag Exchange Protocol	
Možnost definovat povolené MAC adresy na portu	
Monitorování aplikačních toků prostřednictvím technologie NetFlow nebo ekvivalentní technologie	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Interní nástroje pro debugging procházejícího provozu	
DHCP server	
SSHv2	
CLI rozhraní	
SNMPv2/v3	
TACACS+ nebo RADIUS klient pro AAA	
Vzdálený port mirroring (RSPAN)	

1.2.19.4 ZAŘÍZENÍ TYPU H: SMĚROVAČ PRO LOKALITU 4. ÚROVNĚ

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení směrovač	
Formát zařízení fixní	
Integrovaný LAN přepínač s minimálně 8 10/100/1000 Base-TX porty s auto MDI/MDX	
Minimálně 1 WAN GE duální port (10/100/1000 Base-TX nebo volitelné fyzické rozhraní SFP)	
Min. jeden USB 2.0 port	
LAN přepínač – 802.1D (Spanning Tree Protocol)	
LAN přepínač – min. 14 802.1Q VLAN	
LAN přepínač – MAC filtering	
LAN přepínač – 802.3af na alespoň 4 portech (tzn. dostupný příkon pro každý port min. 15,4 W)	
LAN přepínač – Switched Port Analyzer (SPAN)	
LAN přepínač – Storm Control	
LAN přepínač – Port Security	
LAN přepínač – IGMPv3 snooping	
LAN přepínač – 802.1X	
Směrování IPv4 unicast a multicast	
ICMP	
IGMPv2	
IGMPv3	
uRPF	
Směrování IPv6 unicast a multicast	
ICMPv6	
IPv6 PMTU	
IPv6 Neighbor Discovery	
IPv6 bezstavová autokonfigurace adres (SLAAC)	
uRPF pro IPv6	
MLDv1	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
MLDv2	
Alespoň 5 směrovacích instancí (oddělené směrovací tabulky)	
RIPv1	
RIPv2	
RIPng	
OSPFv2	
OSPFv3	
MP-BGP	
Podpora 4 byte AS numbers v BGP	
First Hop Redundancy Protocol pro IPv4 (např. VRRP, HSRP)	
First Hop Redundancy Protokol pro IPv6	
BFD	
GRE	
Multipoint GRE (MGRE)	
NHRP	
PIM SSM pro IPv4	
PIM SM pro IPv4	
PIM SSM pro IPv6	
PIM SM pro IPv6	
MPLS	
MPLS VPN	
MPLS VPN over mGRE	
IPv6 MPLS VPN (6VPE)	
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels	
L2TP	
L2TPv3	
Statický a dynamický NAT a PAT	
DHCP server, relay a klient	
DHCPv6 relay	
DNS server	
DNS proxy	
Seznamy pro řízení přístupu (ACL)	
Hardwarová akcelerace šifrování pro IPSec AES 256	
Minimální propustnost směrovače 20 Mbit/s při aktivovaných službách IPSec šifrování a QoS měřená pro IMIX provoz	
IKEv2	
SHA-2 (SHA-256, SHA-512)	
Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami (např. pro IPT provoz)	
Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů	
QoS pre-classification pro IPSec	
Zone-Based Policy Firewall	
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	
Vynucení QoS parametrů pro takto rozpoznané aplikace a skupiny aplikací – marking, garance šířky pásma pro jednotlivé aplikace, shaping, policing	
QoS classification – ACL, DSCP, CoS, MPLS based	
QoS marking – DSCP, CoS, MPLS	
QoS Shaping	
QoS strategie pro frontu založená na třídách s prioritní frontou (LLQ)	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Policy-Based Routing (PBR) podle ACL	
Alespoň tříúrovňový hierarchický QoS	
Správa přes Telnet a CLI	
Správa přes SNMPv2	
Správa přes SNMPv3	
Správa přes SSHv2 a CLI	
Správa přes HTTP(S)	
RADIUS nebo TACACS+ klient pro AAA	
Sběr a vyhodnocování statistik a výkonnostních charakteristik aplikačních toků: využívané pásmo, odezvy aplikací	
Monitorování aplikačních toků (za účelem detekce bezpečnostních incidentů) prostřednictvím technologie NetFlow nebo ekvivalentní	
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód	
Podpora minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat)	
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	
NTPv3 server	

1.2.19.5 Zařízení typu I: směrovač pro lokalitu 3. úrovně a 4. úrovně s větší přípojkou

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení směrovač	
Formát zařízení modulární	
Alespoň 2x10/100/1000Base-TX WAN portů	
Min. 2 sloty pro rozšiřující moduly	
Směrování IPv4	
Směrování IPv6	
OSPFv2	
BGPv4	
Podpora 4 byte AS numbers v BGP	
First Hop Redundancy Protokol (např. VRRP, HSRP)	
GRE (Generic Routing Encapsulation)	
Policy-based routing podle ACL	
IP Multicast (PIM SSM, PIM SM)	
IGMPv2, IGMPv3	
uRPF	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
First Hop Redundancy Protokol pro IPv6	
OSPFv3	
MP BGP	
MPLS	
MPLS VPN	
Alespoň 15 oddělených (nezávislých) směrovacích tabulek	
MPLS VPN over mGRE	
IPv6 MPLS VPN (6VPE)	
IPv6 Multicast (MLDv1 & v2)	
IPv6 Multicast (PIM SM)	
IPv6 Multicast (PIM SSM)	
uRPF pro IPv6	
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels	
QoS classification – ACL, DSCP, CoS, MPLS based	
QoS marking – DSCP, CoS, MPLS	
QoS Shaping	
Class Based and Priority queuing	
Rate Limiting	
Alespoň tříúrovňový hierarchický QoS	
Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, PING, traceroute)	
ACL na rozhraní IN/OUT	
Zone based firewall	
IPSec AES 256	
Hardwarová akcelerace šifrování pro IPSec AES 256	
Minimální propustnost směrovače 40 Mbit/s při aktivovaných službách IPSec šifrování a QoS měřená pro IMIX provoz	
IKEv2	
SHA-2 (SHA-256, SHA-512)	
QoS pre-classification pro IPSec	
Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami (např. pro IPT provoz)	
Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů	
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	
Vynucení QoS parametrů pro takto rozpoznané aplikace a skupiny aplikací – marking, garance šířky pásma pro jednotlivé aplikace, shaping, policing	
Sběr a vyhodnocování statistik a výkonnostních charakteristik aplikačních toků: využívané pásmo, odezvy aplikací	
Monitorování aplikačních toků (za účelem detekce bezpečnostních incidentů) prostřednictvím technologie NetFlow nebo ekvivalentní	
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód	
Podpora minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat)	
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	
SSHv2	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
CLI rozhraní	
SNMPv2/v3	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	
NTPv3 server	

1.2.19.6 Zařízení typu J: přepínač pro lokalitu 3. úrovně, 48 portů s napájením

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: L3 přepínač	
Formát přepínače: fixní stohovatelný nebo modulární	
Alespoň dva dedikované stohovací porty v případě stohovatelného přepínače	
Možnost mít alespoň 6 zařízení ve stohu nebo šest slotů v šasi	
Minimální kapacita sběrnice stohu 120 Gbit/s nebo min. kapacita modulárního šasi na slot 80 Gbit/s	
Stateful Switch Over v rámci stohu nebo šasi	
Možnost instalovat interní redundantní napájecí zdroj	
Minimálně 48 portů 10/100/1000 Base-TX s PoE	
Celkový příkon pro PoE porty min. 740W	
Podpora IEEE 802.1at pro alespoň 24 portů najednou (tzn. dostupný příkon pro každý port min. 30 W)	
Podpora IEEE 802.1af pro všech 48 portů najednou (tzn. dostupný příkon pro každý port min. 15,4 W)	
Minimálně 4 1GE uplink porty s volitelným fyzickým rozhraním (porty použité pro stohování nelze započítat jako uplink port)	
Minimálně 30000 záznamů v MAC address tabulce	
IEEE 802.3ad	
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	
Minimálně 8 linek jako součást PortChannel trunků	
Minimálně 64 konfigurovatelných PortChannel trunků	
IEEE 802.1Q	
Minimálně 128 aktivních VLAN	
IEEE 802.1x	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-host authentication nebo ekvivalentní)	
Možnost provozu 802.1x v tzv. monitor módu bez omezování přístupu koncových uživatelů	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
RADIUS CoA (RFC 5176)	
IEEE 802.1w – Rapid Spanning Tree Protocol	
Podpora instance Rapid Spanning Tree Protokolu per VLAN	
Podpora jumbo rámců (9198 bytes)	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	
Směrování protokolů IPv4 a IPv6 v hardware	
OSPFv2	
OSPFv3	
First Hop Redundancy Protokol (např. VRRP, HSRP)	
Reverse path check (uRPF)	
IGMPv2, IGMPv3	
Minimálně 8 HW QoS front	
QoS classification – ACL, DSCP, CoS based	
QoS marking – DSCP, CoS	
QoS – Strict Priority Queue	
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	
QoS Policing	
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	
IPv6 services (SSH, Syslog, DHCP)	
IPv6 QoS	
IPv6 First Hop Security (Port ACL, RA guard, DHCPv6 snooping)	
IPv6 ACL	
Možnost definovat povolené MAC adresy na portu	
ACL na rozhraní IN/OUT (včetně virtuálních – VLAN)	
IEEE 802.1ae na uplink portech	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	
Source-Group Tag Exchange Protocol	
IEEE 802.3az	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	
Inteligentní PoE management – zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	
Zrcadlení provozu na úrovni jednotlivých fyzických rozhraní i virtuálních sítí (VLAN) do monitorovacího rozhraní (ekvivalent funkce SPAN)	
Monitorování aplikačních toků (za účelem detekce bezpečnostních incidentů) prostřednictvím technologie NetFlow nebo ekvivalentní	
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód	
Možnost definovat minimálně dva různé monitory datových toků současně, jeden monitor pro sběr parametrů datových toků potřebných pro výkonnostní plánování, druhý monitor pro sběr parametrů datových toků potřebných pro detekci bezpečnostních incidentů	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
DHCP server	
SSHv2	
CLI rozhraní	
SNMPv2/v3	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	
NTPv3 server	

1.2.19.7 ZAŘÍZENÍ TYPU K: PŘEPÍNAČ PRO LOKALITU 3. ÚROVNĚ, 24 PORTŮ S NAPÁJENÍM

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: L3 přepínač	
Formát přepínače: fixní stohovatelný nebo modulární	
Alespoň dva dedikované stohovací porty v případě stohovatelného přepínače	
Možnost mít alespoň 6 zařízení ve stohu nebo 6 slotů v šasi	
Minimální kapacita sběrnice stohu 120 Gbit/s nebo min. kapacita modulárního šasi na slot 80 Gbit/s	
Stateful Switch Over v rámci stohu nebo šasi	
Možnost instalovat interní redundantní napájecí zdroj	
Minimálně 24 portů 10/100/1000 Base-TX s PoE	
Celkový příkon pro PoE porty min. 370 W	
Podpora IEEE 802.1at pro alespoň 12 portů najednou (tzn. dostupný příkon pro každý port min. 30 W)	
Podpora IEEE 802.1af pro všech 24 portů najednou (tzn. dostupný příkon pro každý port min. 15,4 W)	
Minimálně 4 1GE uplink porty s volitelným fyzickým rozhraním (porty použité pro stohování nelze započítat jako uplink port)	
Minimálně 30000 záznamů v MAC address tabulce	
IEEE 802.3ad	
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasi	
Minimálně 8 linek jako součást PortChannel trunků	
Minimálně 64 konfigurovatelných PortChannel trunků	
IEEE 802.1Q	
Minimálně 128 aktivních VLAN	
IEEE 802.1x	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-host authentication nebo ekvivalentní)	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Možnost provozu 802.1x v tzv. monitor módu bez omezování přístupu koncových uživatelů	
RADIUS CoA (RFC 5176)	
IEEE 802.1w – Rapid Spanning Tree Protocol	
Podpora instance Rapid Spanning Tree Protokolu per VLAN	
Podpora jumbo rámců (9198 bytes)	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	
Směrování protokolů IPv4 a IPv6 v hardwaru	
OSPFv2	
OSPFv3	
First Hop Redundancy Protokol (např. VRRP, HSRP)	
Reverse path check (uRPF)	
IGMPv2, IGMPv3	
Minimálně 8 HW QoS front	
QoS classification – ACL, DSCP, CoS based	
QoS marking – DSCP, CoS	
QoS – Strict Priority Queue	
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	
QoS Policing	
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	
IPv6 services (SSH, Syslog, DHCP)	
IPv6 QoS	
IPv6 First Hop Security (Port ACL, RA guard, DHCPv6 snooping)	
IPv6 ACL	
Možnost definovat povolené MAC adresy na portu	
ACL na rozhraní IN/OUT (včetně virtuálních – VLAN)	
IEEE 802.1ae na uplink portech	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	
Source-Group Tag Exchange Protocol	
IEEE 802.3az	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	
Inteligentní PoE management – zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	
Zrcadlení provozu na úrovni jednotlivých fyzických rozhraní i virtuálních sítí (VLAN) do monitorovacího rozhraní (ekvivalent funkce SPAN)	
Monitorování aplikačních toků (za účelem detekce bezpečnostních incidentů) prostřednictvím technologie NetFlow nebo ekvivalentní	
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Možnost definovat minimálně dva různé monitory datových toků současně, jeden monitor pro sběr parametrů datových toků potřebných pro výkonnostní plánování, druhý monitor pro sběr parametrů datových toků potřebných pro detekci bezpečnostních incidentů	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	
DHCP server	
SSHv2	
CLI rozhraní	
SNMPv2/v3	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	
NTPv3 server	

1.2.19.8 ZAŘÍZENÍ TYPU L: KOMPAKTNÍ PŘEPÍNAČ, MIN. 8 PORTŮ S NAPÁJENÍM

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení L2 přepínač	
Formát přepínače fixní	
Minimálně 8 10/100/1000 Base-TX portů s PoE napájením	
Minimálně 2 1GE uplink porty s volitelným fyzickým rozhraním	
IEEE 802.3ad	
IEEE 802.1Q	
Minimálně 64 aktivních VLAN	
IEEE 802.1x	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-host authentication nebo ekvivalentní)	
Možnost provozu 802.1x v tzv. monitor módu bez omezování přístupu koncových uživatelů	
RADIUS CoA (RFC 5176)	
IEEE 802.1w – Rapid Spanning Tree Protocol	
Podpora instance Rapid Spanning Tree Protokolu per VLAN	
Podpora jumbo rámců (9000 bytes)	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	
IGMP snooping	
IPv6 MLD snooping	
Minimálně 4 HW QoS front	
QoS classification – ACL, DSCP, CoS based	
QoS marking – DSCP, CoS	
QoS – Strict Priority Queue	
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	
QoS Policing	
IPv6 QoS	
IPv6 First Hop Security (Port ACL, RA guard, DHCPv6 snooping)	
IPv6 ACL	
Možnost definovat povolené MAC adresy na portu	
ACL na rozhraní IN/OUT (včetně virtuálních – VLAN)	
IEEE 802.1ae na uplink portech	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	
Source- Group Tag Exchange Protocol	
IEEE 802.3af	
IEEE 802.3at	
Minimálně 120W PoE budget	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	
Inteligentní PoE management – zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	
Zrcadlení provozu do monitorovacího rozhraní (ekvivalent funkce SPAN)	
DHCP server	
SSHv2	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
CLI rozhraní	
SNMPv2/v3	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	
NTPv3	

1.2.19.9 Zařízení typu M: agregační optický přepínač

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného zařízení
Výrobce zařízení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ zařízení: L3 přepínač	
Formát přepínače: stohovatelný nebo modulární	
Alespoň 2 dedikované stohovací porty	
Možnost alespoň 6 zařízení ve stohu/minimálně. 6 slotů v šasi	
Alespoň 160 Gbit/s kapacita sběrnice stohu/alespoň 80 Gbit/s kapacita na slot modulárního šasi	
Stateful Switch Over v rámci stohu nebo šasi	
Možnost instalovat interní redundantní napájecí zdroj	
Alespoň 12 1GE portů s volitelným fyzickým rozhraním	
Možnost instalovat modul s 2x10GE porty s volitelným fyzickým rozhraním	
Alespoň 30 000 záznamů v tabulce MAC adres	
IEEE 802.3ad	
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	
Minimálně 8 linek jako součást PortChannel trunků	
Alespoň 64 konfigurovatelných PortChannel trunků	
IEEE 802.1Q	
Minimálně 250 aktivních VLAN	
IEEE 802.1x	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-host authentication nebo ekvivalentní)	
Možnost provozu 802.1x v tzv. monitor módu bez omezování přístupu koncových uživatelů	
RADIUS CoA (RFC 5176)	
IEEE 802.1w – Rapid Spanning Tree Protocol	
Podpora alespoň 250 instancí Rapid Spanning Tree Protokolu per VLAN	
Podpora jumbo rámců (9198 bytes)	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Směrování protokolů IPv4 a IPv6 v hardwaru	
OSPFv2	
OSPFv3	
BGPv4	
MP BGP	
Virtualizace směrovacích tabulek – např. Virtual Routing and Forwarding (VRF)	
First Hop Redundancy Protocol (např. VRRP, HSRP)	
Reverse path check (uRPF)	
IGMPv2, IGMPv3	
Minimálně 8 HW QoS front	
QoS classification – ACL, DSCP, CoS based	
QoS marking – DSCP, CoS	
QoS – Strict Priority Queue	
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	
QoS Policing	
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	
IPv6 services (SSH, Syslog, DHCP)	
IPv6 QoS	
IPv6 First Hop Security (Port ACL, RA guard, DHCPv6 snooping)	
IPv6 ACL	
Možnost definovat povolené MAC adresy na portu	
ACL na rozhraní IN/OUT (včetně virtuálních – VLAN)	
IEEE 802.1ae na všech portech	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	
Source-Group Tag Exchange Protocol	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	
Zrcadlení provozu na úrovni jednotlivých fyzických rozhraní i virtuálních sítí (VLAN) do monitorovacího rozhraní (ekvivalent funkce SPAN)	
Monitorování aplikačních toků (za účelem detekce bezpečnostních incidentů) prostřednictvím technologie NetFlow nebo ekvivalentní	
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód	
Možnost definovat minimálně dva různé monitory datových toků současně, jeden monitor pro sběr parametrů datových toků potřebných pro výkonnostní plánování, druhý monitor pro sběr parametrů datových toků potřebných pro detekci bezpečnostních incidentů	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	
DHCP server	
SSHv2	
CLI rozhraní	
SNMPv2/v3	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	
NTPv3 server	

1.3 Oblast systémové infrastruktury

1.3.1 Migrace active directory (AD), MS Exchange, Certifikační autority (CA) do vlastních datových center – bez součinnosti současného dodavatele

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Řešení poskytuje minimálně stejné vlastnosti jako současné řešení – viz popis současného stavu	
Řešení pokryje až 15 000 uživatelů	
Řešení pokryje až 20 000 stanic	
Řešení umožňuje přihlášení uživatele pomocí certifikátu i pomocí jména a hesla	
Výsledné řešení autentizace pomocí certifikátu bude postaveno na SHA-2 certifikátech, které budou na současných čipových kartách	
Po migraci musí být zajištěno, aby autentizační prostředky ze zdrojového prostředí (certifikáty/účty) nebylo možné použít v prostředí cílovém k přihlašování	
Migrace musí počítat se zachováním funkčnosti a případnou úpravou systémů přímo navázaných na migrované systémy, viz popis současného stavu	
Podpora geoclusteru pro řešení	
Během migrace nedojde ke ztrátě uživatelských dat	
Během migrace nedojde ke ztrátě atributů uživatelských účtů, skupin a kontaktů (vyjma systémových jako SID apod.)	

1.3.2 Migrace active directory (AD), MS Exchange, Certifikační autority (CA) do vlastních datových center – se součinností současného dodavatele

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Řešení poskytuje minimálně stejné vlastnosti jako současné řešení	
Řešení pokryje až 15 000 uživatelů	
Řešení pokryje až 20 000 stanic	
Řešení umožňuje přihlášení uživatele pomocí certifikátu i pomocí jména a hesla	
Výsledné řešení autentizace pomocí certifikátu bude postaveno na SHA-2 certifikátech, které budou na současných čipových kartách	
Po migraci musí být zajištěno, aby autentizační prostředky ze zdrojového prostředí (certifikáty/účty) nebylo možné použít v prostředí cílovém k přihlašování	

Migrace musí počítat se zachováním funkčnosti a případnou úpravou systémů přímo navázaných na migrované systémy; viz popis současného stavu	
Podpora geoclusteru pro řešení	
Během migrace nedojde ke ztrátě uživatelských dat	
Během migrace nedojde ke ztrátě atributů uživatelských účtů, skupin a kontaktů (SID musí být přenesen min jako SIDHistory)	
Během migrace nedojde ke ztrátě uživatelských profilů	
Během migrace nedojde ke ztrátě uživatelských oprávnění, zejména na sdílených úložištích (share), ale i v databázích a na dalších objektech s vlastním nastavením práv	

1.3.3 Monitorování Infrastruktury AD a poštovního systému

Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Navržený systém maximálně využívá licence uvedené v kapitole 8.1 v příloze č. 10	
Nasazený systém využije maximálně stávajících licencí – viz popis současného stavu	
Nativní podpora dohledu Microsoft produktů s možností plné customizace a též možností dohledu non-Microsoft platforem, včetně síťových zařízení	
Systém musí mít předpřipravené balíky konfigurací pro dohled konkrétních Microsoft produktů (Windows Server, Active Directory, Exchange Server apod.) tak, aby nebylo nutné manuálně definovat jejich parametry, nicméně aby bylo možné konfiguraci měnit. Systém rovněž musí umožnit tvorbu vlastních balíků konfigurací dohledu a tato platforma musí být otevřená tak, aby i výrobci třetích stran mohli balíky konfigurací tvořit pro své produkty	
Monitoring expirace vydaných certifikátů jak před expirací, tak po ní	
Monitoring publikování a dostupnosti CRL	
Monitoring správné funkce jednotlivých rolí Microsoft Exchange serveru, zejména Mailbox Serveru, Client Access Serveru a Hub Transport Serveru	
Monitoring všech aspektů správné funkce Active Directory a Active Directory Certificate Services	
Monitoring správné funkce procesů, na kterých funkce AD přímo závisí, včetně replikace souborů, funkce LDAP služeb, správné funkce vztahů důvěry, služeb Windows Time a KDC	
Sběr výkonnostních čítačů monitorovaných systémů	
Možnost generování reportů, včetně statistik dostupnosti služeb a reportů pro plánování kapacit systémů	
Propojení systému s centrálním dohledovým systémem MPSV	
Systém musí umožnit delegaci správy principem Role Based Administration	
Systém musí umožnit customizaci pohledů na spravovanou infrastrukturu tak, aby různé skupiny administrátorů „viděly“ jen pro ně relevantní monitorované entity	
Systém musí umožnit agregování monitorovaných entit, které dohromady tvoří aplikaci/službu tak, aby sledoval její celkové zdraví a SLA	

Systém musí podporovat zasílání notifikací či filtrovaných notifikací různými kanály (minimálně prostřednictvím e-mailu a sms) na různé skupiny administrátorů/řešitelů či do nadřazených dohledových systémů	

1.3.4 CUSTOMIZACE DOHLEDU AD INFRASTRUKTURY PRO LOKÁLNÍ SPRÁVCE

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Rozhraní monitorovacího nástroje musí být přizpůsobeno tak, aby informatik viděl zjednodušený pohled na centrální systémy a získal přehled zejména o:	
• Celkovém zdraví služeb AD, Exchange a Certifikační autority, ideálně formou přehledové mapy/diagramu	
• Aktuálních neuzavřených výstrahách centrálních služeb	
• Stavu zdraví serverů centrálních systémů a dalších komponent tvořících služby AD, Exchange a Certifikační autoritu	
Přístup informatiků musí být na úrovni read-only	

1.3.5 IDM – NÁHRADA SOUČASNÉHO ŘEŠENÍ ISU (MIIS)

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Řešení musí pokrýt minimálně 15 000 uživatelů s možností budoucího rozšíření	
Integrace nové AD s nově navrhovaným řešením	
• Synchronizace uživatelských účtů, distribučních skupin a kontaktů mezi novou AD a nově navrhovaným řešením	
Integrace nové AD s EPD v rámci nově navrhovaného řešení – Číselník pracovišť	
• Přenos displayName, názvu, kódu a zkratky pracoviště z ePD do nové AD	
Integrace nově navrhovaného řešení s certifikační autoritou MPSV	
• Aktualizace uživatelských certifikátů v nově navrhovaném řešení	
Integrace nové AD s PIS v rámci nově navrhovaného řešení	
• Aktualizace uživatelských účtů v nové AD (organizační data zaměstnanců MPSV)	
Integrace nové AD s AD Státního úřadu inspekce práce (SÚIP) v rámci nově navrhovaného řešení	
• Import kontaktů z AD SÚIP do GAL nové AD	
Integrace nové AD s libovolným personálním systémem pomocí nově navrhovaného řešení	
Integrace nové AD s různými dalšími AD pomocí nově navrhovaného řešení	
Zajištění autentizace a autorizace pro ePD (Elektronická provozní dokumentace) v rámci nově navrhovaného řešení	
• Autentizace do aplikace certifikátem	
• Autorizační údaje uloženy v nově navrhovaném řešení	
Zajištění autentizace a autorizace pro Dohledový systém v rámci nově navrhovaného řešení	
• Autentizace do aplikace certifikátem	
• Autorizační údaje uloženy v nově navrhovaném řešení	
Webová aplikace pro centralizovanou správu uživatelských účtů v nové AD a centrální přidělování práv k integrovaným aplikacím ve WAN	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
• Autentizace certifikátem	
• Autorizace podle rolí (správce, schvalovatel, běžný uživatel)	
• Rozsah práv získaných přidělenými rolemi musí respektovat organizační jednotky definované v nové AD	
• Vyhledávání uživatelských účtů, skupin, poštovních distribučních seznamů a poštovních kontaktů ve vybraných kontejnerech nové AD podle hodnot atributů	
• Zobrazování vyhledaných objektů formou tabulky	
• Zobrazování detailů vybraného objektu	
• Vytváření uživatelských účtů a skupin v nové AD prostřednictvím jednoduchého schvalovacího workflow	
• Modifikace uživatelských účtů a skupin (včetně členství ve skupinách)	
• Hromadná změna vybraných vlastností (atributů) uživatelských účtů a skupin	
• Služba typu Self-Service (běžný uživatel si sám může změnit povolené atributy svého uživatelského účtu)	
• Přidělování práv k integrovaným aplikacím ve WAN	
• Práce s certifikáty (vložení, zobrazení, vymazání)	
• Zaznamenávání činnosti správců i běžných uživatelů do protokolačního souboru (historie)	
• Vytváření reportů	

1.3.6 CENTRÁLNÍ PATCH MANAGEMENT PRO SERVERY

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Všechny záplaty pro servery budou uloženy na centrálním úložišti, servery budou stahovat záplaty z tohoto úložiště	
Systém umožní definovat oblasti s různým nastavením parametrů aktualizace Windows a kategorií záplat nabízených serveru	
Systém musí umožnit schvalování či zamítnutí záplat, a to jak manuálně, tak automaticky	
Automatické řešení „supersedence“ záplat (vyřazování zastaralých verzí či verzí nahrazených jinou záplatou)	
Systém musí umožnit tvorbu testovacích skupin pro testování záplat k nasazení	
Systém musí umožnit i záplatování dalších Microsoft produktů (např. SQL server, Exchange Server, System Center, Office apod.)	

1.3.7 KONSOLIDACE SERVERŮ NA ÚP ČR

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Hypervizor s nízkou režií, bez závislosti na hostovaném operačním systému s podporou 64 a 32bitové virtualizace na x86 platformě (bez omezení na konkrétního výrobce). Hypervizor bez omezení na operační paměť, počet připojovaných rozhraní (např. iSCSI, FC, LAN), jader CPU, diskových polí, běžících hostů (virtuálních strojů) mimo limitů vyplývajících z technických a existujících možností v době realizace zakázky (např. schopnost adresace omezené velikosti paměti, velikosti virtuálních disků daných technickými možnostmi hypervizoru)	
Podpora monitoringu jednotlivých aplikací virtualizovaných strojů s automatizovanou reakci na stav služeb (aplikací) na těchto strojích. Podpora restartu služeb, aplikací nebo celého virtuálního serveru	
Podpora tvorby šablon a klonování virtuálních strojů, přenášení konfigurace, hromadné úpravy nastavení parametrů a konfigurací. Podpora skriptování a ovládání přes příkazovou řádku (shell apod.) s podporou otevřeného API	
Řešení pokryje všechny lokality ÚP ČR	
Řešení zachová plnou funkčnost konsolidovaných serverů po jejich virtualizaci ve srovnání se současným stavem	
Řešení podporuje logické oddělení managementu aktivních prvků, datového provozu a řídicího provozu pro virtualizační platformu	
Podpora tvorby šablon a klonování virtuálních strojů, přenášení konfigurace, hromadné úpravy nastavení parametrů a konfigurací. Podpora scriptování a ovládání přes příkazovou řádku (shell apod.) s podporou otevřeného API	
Podpora otevřených rozhraní a přístup do systému třetím stranám pomocí API	
Možnost budoucí centrální správy a monitoring pomocí instalovaného klienta a webového klienta pro efektivní hromadnou správu, nastavení a monitorování	
Možnost budoucí centrální správy s podporou přidělování práv na základě LDAP (Active Directory), přidělování rolí, oprávnění a definování oprávnění na jednotlivé servery nebo další prostředky infrastruktury	

1.3.8 SPRÁVA KONCOVÝCH STANIC MPSV A ÚP ČR

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Navržený systém maximálně využívá licence uvedené v kapitole 8.1 v příloze č. 10	
Nasazený systém podpoří minimálně 20 000 stanic	
Nasazený systém umožní částečnou decentralizaci, zejména s ohledem na úsporu zatížení WAN sítě (balíčky SW/OS/Patch umístěny co „nejblíže“ stanicím)	
Automatizovaná inventarizace HW	
Automatizovaná inventarizace SW	
Měření využití SW na klientských stanicích	
Centrální příprava instalačních balíčků SW	
Škálovatelná distribuce SW	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Systém je možné provozovat paralelně se současným systémem pro správu stanic (viz současný stav) a v případě nutnosti může být jeho zálohou	
Optimalizace toku dat v souvislosti s distribucí SW/OS/Patch na koncová zařízení	
Možnost vytvoření webového katalogu aplikací pro samoobslužnou instalaci aplikací na koncové stanice	
Vzdálený přístup na pracovní stanice s možností převzetí řízení a vizuální spolupráce uživatele stanice	
Centrální správa distribuce patchů pro Windows a další produkty Microsoft (Office apod.) s možností plánování instalace na konkrétní čas pro různé skupiny uživatelů	
Možnost využití Branch cache na klientech ve vzdálených lokalitách (bez serverů v této vzdálené lokalitě)	
Migrace uživatelských profilů, dat a specifických nastavení pracovních stanic při výměně HW/reinstalaci OS	
Podpora pro 64bitové prostředí operačních systémů	
Podpora role based administration modelu s možností k defaultním rolím vytvářet role vlastní dle potřeby	
Možnost tvorby reportů z inventarizace, instalací, aktualizací a OS deploymentů; možnost customizace reportů	
Možnost sledování využití instalovaných aplikací a sledování zdraví klienta (s případnou remediací)	
Správa aplikací v těchto aspektech: instalace, odinstalování, správa verzí, návaznost na katalog aplikací	
Nasazení operačního systému Windows – instalace ze sítě přímo na HW (bare metal) pro nové stanice nebo vybrané stanice (reinstall). Podpora customizace instalace a sekvencí post-instalačních úkonů. Semi-automatizace tvorby instalačních image (pro aktualizace image apod.).	

1.3.9 Využití MS licencí pro kolaborační systém a integrace s videokonferencí

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Výrobce systému	
Produktové číslo (typ) nabízeného systému (v případě, že je systém popsán více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného systému)	
Odkaz na www stránky výrobce systému, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Typ systému: systém pro spolupráci a komunikaci	
Rychlá textová komunikace (instant messaging)	
Chat (rozesílání rychlých textových zpráv na skupinu uživatelů)	
Komplexní informace o stavu (vazba na MS produkty)	
Klient pro mobilní telefon (IOS, Android, Windows…)	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Webový klient	
Podnikové hlasové funkce (např. sledování zlomyslných volání, parkování hovorů)	
Videokonference mezi dvěma uživateli	
Videokonference ve skupině uživatelů	
Propojení na velké konference (Cisco/Tandberg/Polycom/Vidyo/Radvision atd.)	
Tvorba virtuální konferenční místnosti (meeting rooms)	
Sdílení zvuku/videa/obsahu mezi třemi a více účastníky	
Audiokonference (meet me, konference)	
Mobilní videokonference (videokonference na mobilním zařízení)	
Vzdálené připojení komunikátoru z internetu (bez VPN tunelu)	
Pasivní sdílení plochy/dokumentů (pasivní náhled na dokument)	
Aktivní sdílení plochy/dokumentů (společná možnost upravovat dokument)	
Aktivní sharing dokumentů s možností audiokonference	
Aktivní sharing dokumentů s možností audio a videokonference	
Tvorba virtuální konferenční místnosti (meeting rooms)	
Ovládací prvky schůzky (organizátor, možnosti předsálí, možnosti připojení)	
Možnost plného propojení s externími organizacemi na úrovni protokolu SIP	
Možnost propojení s veřejnými IM sítěmi založenými za protokolu SIP (IM, presence)	
Možnost propojení s veřejnými IM sítěmi založenými za protokolu XMPP (IM, presence)	
Možnost propojení se stávajícím interním hlasovým telefonním systémem založeným na protokolu IP (VoIP)	
Možnost propojení se stávajícím videokonferenčním systémem – audio, video	
Možnost komunikace z mobilních platforem (Windows Phone, iOS, Android)	
Možnost integrace s intranet aplikacemi (např. seznam uživatelů – propagace stavu presence)	

1.3.10 Upgrade videokonferencí

1.3.10.1 Prvek multikonferenční server

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Výrobce systému	
Produktové číslo (typ) nabízeného systému (v případě, že je systém popsán více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného systému)	
Odkaz na www stránky výrobce systému, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje

	požadavek (doplní Uchazeč) ANO/NE
Typ prvku je multikonferenční server	
Podpora spojení pomoci protokolů H.323, SIP a TIP	
Kapacita serveru pro 5xHD1080p spojení	
Škálovatelnost kapacity při spojení nižší kvalitou než HD1080p, a to dvojnásobná kapacita při spoení kvalitou HD720p(10x spojení), čtyřnásobná při spojení kvalitou SD (20x spojení) a osminásobnou kapacitu při kvalitě CIF (40x spojení)	
Možnost rozšíření kapacity serveru zakoupením SW licence bez nutnosti zakupovat další HW doplňky až pro 15xHD1080p spojení v režimu Continuous Presence a až 80xHD720p spojení v režimu přepínání za hlasem	
Podpora audio protokolu G.711a/u	
Podpora audio protokolu G.722	
Podpora audio protokolu G.722.1C	
Podpora audio protokolu G.722.1	
Podpora audio protokolu G.723.1	
Podpora video protokolů H.261	
Podpora video protokolů H.263	
Podpora video protokolů H.263++	
Podpora video protokolů H.264	
Podpora video protokolů H.264HP	
Podpora sdílení obrazu v sekundárním video streamu protokolem H.239 a BFCP	
Možnost rozšíření o ISDN PRI modul	
Podpora integrace s nahrávacím a streamovacím serverem Polycom RSS2000	
Podpora protokolu SNMPv3 pro monitoring	
AES media encryption	
Integrovaná technologie pro obnovu ztracených paketů	
Ovládání pomocí FECC	
Rozšířená 2letá záruka se zasláním vadného dílu nejpozději do 24 hodin v pracovních dnech po nahlášení závady	

1.3.10.2 PRVEK STREAMOVACÍ SERVER

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Výrobce systému	
Produktové číslo (typ) nabízeného systému (v případě, že je systém popsán více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného systému)	
Odkaz na www stránky výrobce systému, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Splňuje (ano/ne)

Typ prvku je streamovací server	
Streamování libovolného hovoru na protokolu SIP a H.323	
Možnost streamování 2 nezávislých hovorů	
Ovládání a správa přes webové rozhraní s úrovní oprávnění minimálně uživatel a administrátor	
Podpora streamování hovoru minimálně v kvalitě CIF, SIF, 4CIF, SD, HD, XGA, VGA	
Podpora streamování druhého kanálu se sdílenou prezentací pomoci protokolu H.239	
Možnost zobrazení streamovaného hovoru pro až 50 účastníků	
Streamování na PC s SW vybavením Windows Media player nebo RealPlayer	
Možnost ovládání z videokonferenční jednotky pomoci FECC	
Podpora audio protokolu G.711a/u	
Podpora audio protokolu G.722	
Podpora audio protokolu G.722.1C	
Podpora audio protokolu G.722.1	
Podpora video protokolu H.261	
Podpora video protokolu H.263	
Podpora video protokolu H.264	

1.3.10.3 PRVEK VIDEOKONFERENČNÍ JEDNOTKA

Požadovaná funkcionalita/vlastnost	**Doplní Uchazeč dle nabízeného řešení**
Výrobce systému	
Produktové číslo (typ) nabízeného systému (v případě, že je systém popsán více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného systému)	
Odkaz na www stránky výrobce systému, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	**Splňuje (ano/ne)**
Typ prvku je videokonferenční jednotka	
Podpora spojení video hovorů na protokolu SIP a H.323	
Výstup minimálně na 1 zobrazovací jednotku pomocí digitálního video výstupu HDMI nebo DVI	
Vstup video signálu pomocí konektoru DVI-I, nebo kombinace HDMI a VGA	
Podpora audio protokolu G.711a/u	
Podpora audio protokolu G.722	
Podpora audio protokolu G.722.1C	
Podpora audio protokolu G.722.1	
Podpora audio protokolu G.728	
Podpora video protokolu H.261	
Podpora video protokolu H.263	
Podpora video protokolu H.263++	
Podpora video protokolu H.264	

Požadovaná funkcionalita/vlastnost	Splňuje (ano/ne)
Podpora video protokolu H.264HP	
Přenos obrazu v kvalitě HD 720p	
Možnost rozšíření kvality přenášeného obrazu zakoupením licence až na FullHD 1080p	
Kamera s možností natáčení z dálkového ovládání a s alespoň 10násobným optickým zoomem	
Externí mikrofon s funkci echo-canceler a záběrem alespoň 3m od mikrofonu	
Profesionální zobrazovací jednotku bez TV tuneru o velikosti alespoň 50" a technologií LED	
Stojan na kolečkách pro umístění celé videokonferenční sestavy (zobrazovací jednotka, kamera, videokonferenční kodek) pro trvalé umístění a snadnou a bezpečnou manipulaci celé sestavy	

1.3.11 Evidence IT majetku a správy SW licencí

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Propojení na modul majetku systému EKIS	
Řízení životního cyklu hardwaru a softwaru	
Evidence smluv a smluvních podmínek	
Evidence dodavatelů	
Strukturované sledování jednorázových a opakovaných nákladů	
Evidence vlastnictví softwaru a podpora licenční čistoty – SW Asset Management	
Evidence různých produktů SW a jejich parametrů	
Evidence nákupů SW licencí	
Evidence vazby na hardware, kde je software instalován	
Evidence práva užívání k softwarovým produktům	
Evidence licencí – oprávnění užívat software pro uživatele, lokality, organizace, počítače	
Evidence smluv o softwarové podpoře nebo pronájmu licencí	
Propojení informace SW s evidencí majetkových prvků v ePD	
Propojení informace SW s evidencí provozních prvků v ePD	

1.3.12 Virtualizace stanic MPSV/ÚP ČR

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Hypervizor s nízkou režií, bez závislosti na hostovaném operačním systému s podporou 64 a 32bitové virtualizace na x86 platformě (bez omezení na konkrétního výrobce). Hypervizor bez omezení na operační paměť, počet připojovaných rozhraní (např. iSCSI, FC, LAN), jader CPU, diskových polí, běžících hostů (virtuálních strojů) mimo limitů vyplývajících z technických a existujících možností v době realizace zakázky (např. schopnost adresace omezené velikosti paměti, velikosti virtuálních disků daných technickými možnostmi hypervizoru).	

Automatický „clustering“ s distribucí zátěže, podporou vysoké dostupnosti (HA) a automatizovanou migrací běžících virtuálních desktopů	
Podpora pokročilého síťování (distribuované síťové nastavení – distribuovaný switch, „port mirroring“, LACP, podpora SDN sítí na úrovni komunikace s fyzickými přepínači, „load balancing“)	
Podpora virtualizace grafických procesorů (GPU procesory, rozšiřující karty)	
Podpora definování a kontroly IOPS dle definovaných pravidel a zásad pro vymezení, oddělení a tvorbě priorit pro jednotlivé virtuální desktopy	
Tvorba souvisejících „poolů“ hostů (virtualizovaných desktopů) s možností definování přidělených kapacit, postupnému startu strojů v definovaném pořadí, omezení nebo naopak přidělení prostředků)	
Podpora úpravy kvality a nároků přenosového protokolu	
Podpora lokálních USB zařízení	
Podpora dvoufaktorové autentizace	
Podpora tvorby šablon a klonování virtuálních strojů, přenášení konfigurace, hromadné úpravy nastavení parametrů a konfigurací. Podpora skriptování a ovládání přes příkazovou řádku (shell apod.) s podporou otevřeného API	
Podpora otevřených rozhraní a přístup do systému třetím stranám pomocí API	
Řešení podporuje logické oddělení managementu aktivních prvků, datového provozu a řídicího provozu pro virtualizační platformu	
Centrální správa a monitoring pomocí instalovaného klienta a webového klienta pro efektivní hromadnou správu, nastavení a monitorování	
Centrální správa s podporou přidělování práv na základě LDAP (Active Directory), přidělování rolí, oprávnění a definování oprávnění na jednotlivé servery nebo další prostředky infrastruktury	
Centrální monitorovací nástroje pro sledování zdrojů, jejich archivace, vyhodnocování a predikci s ohledem na vývoj celé infrastruktury. Kapacitní plánování na základě měřených a dlouhodobě sledovaných dat, sledování zátěže, CPU, IOPS diskových systémů, chyb a jejich odhalování v dlouhodobém sledování, aplikační monitoring a jeho automatické vyhodnocování nenadálých stavů – pád virtuálního stroje, pád fyzického stoje, pád lokality). Pokročilé monitorování založené na více parametrech (stav datové sítě, stav diskových FC polí, stav fyzických serverů, stav virtuálních systémů – hostů, stav aplikací na těchto hostech)	

1.3.13 VIRTUALIZACE KIOSKŮ ÚP ČR

Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Hypervizor s nízkou režií, bez závislosti na hostovaném operačním systému s podporou 64 a 32bitové virtualizace na x86 platformě (bez omezení na konkrétního výrobce). Hypervizor bez limitu na operační paměť, počet připojovaných rozhraní (např. iSCSI, FC, LAN), jader CPU, diskových polí, běžících hostů (virtuálních strojů) mimo limitů vyplývajících z technických a existujících možností v době realizace zakázky (např. schopnost adresace omezené velikosti paměti, velikosti virtuálních disků daných technickými možnostmi hypervizoru).	
Automatický „clustering“ s distribucí zátěže, podporou vysoké dostupnosti (HA) a automatizovanou migrací běžících virtuálních strojů	
Podpora pokročilého síťování (distribuované síťové nastavení – distribuovaný switch, „port mirroring“, LACP, podpora SDN sítí na úrovni komunikace s fyzickými přepínači, „load balancing“)	
Podpora virtualizace grafických procesorů (GPU procesory, rozšiřující karty)	
Podpora definování a kontroly IOPS dle definovaných pravidel a zásad pro vymezení, oddělení a tvorbě priorit pro jednotlivé virtuální stroje	
Tvorba souvisejících „poolů“ hostů (virtualizovaných strojů) s možností definování přidělených kapacit, postupnému startu strojů v definovaném pořadí, omezení nebo naopak přidělení prostředků)	
Podpora úpravy kvality a nároků přenosového protokolu	
Podpora tvorby šablon a klonování virtuálních strojů, přenášení konfigurace, hromadné úpravy nastavení parametrů a konfigurací. Podpora skriptování a ovládání přes příkazovou řádku (shell apod.) s podporou otevřeného API	
Podpora otevřených rozhraní a přístup do systému třetím stranám pomocí API	
Centrální správa a monitoring pomocí instalovaného klienta a webového klienta pro efektivní hromadnou správu, nastavení a monitorování	
Centrální správa s podporou přidělování práv na základě LDAP (Active Directory), přidělování rolí, oprávnění a definování oprávnění na jednotlivé servery nebo další prostředky infrastruktury	
Centrální monitorovací nástroje pro sledování zdrojů, jejich archivace, vyhodnocování a predikci s ohledem na vývoj celé infrastruktury. Kapacitní plánování na základě měřených a dlouhodobě sledovaných dat, sledování zátěže, CPU, IOPS diskových systémů, chyb a jejich odhalování v dlouhodobém sledování, aplikační monitoring a jeho automatické vyhodnocování nenadálých stavů – pád virtuálního stroje, pád fyzického stoje, pád lokality). Pokročilé monitorování založené na více parametrech (stav datové sítě, stav diskových FC polí, stav fyzických serverů, stav virtuálních systémů – hostů, stav aplikací na těchto hostech)	

1.3.14 REDESIGN ZÁLOHOVÁNÍ VE WAN

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Výrobce systému	

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Odkaz na www stránky výrobce systému, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Dostatečný objem pro stávající i budoucí zálohy s možností rozšíření; viz přílohu č. 6	
Odpovídající datová propustnost pro přenos celkového objemu dat; viz přílohu č. 6	
Záruka trvanlivosti uložení a neměnnost dat garantovaná výrobcem	
Kompatibilita se stávajícím řešením z hlediska HW a SW – viz popis současného stavu	
Pravidelné spuštění aktualizace softwaru	
Možnost vytvářet vlastní a automatické reporty o stavu prostředí	
Systém centralizované distribuce SW na klienty (deployment)	
Zabezpečení datového obsahu šifrováním	
Notifikace stavu aplikace a úloh přes mail, applog, SNMP a SMS	
Možnost kompletního přehledu stavu, úloh, historie, alertů a licencí z jedné obrazovky – dashboard	
Audit změn a úprav v konfiguraci aplikace a prostředí	
Podpora duplikačních a vázaných duplikačních úloh	
Podpora deduplikace	
Granulární zálohy a obnovy	
Podpora záloh SQL a virtualizačních platforem VMware, Hyper-V	
Podpora úložišť SAN, NAS, iSCSI, Tape, USB	
Automatické připomenutí expirace licence/maintenance	
Centrální management a vyrozumívání celého řešení	
Přehledná správa naplánovaných i proběhlých úloh s filtrací a vyhledáváním	
Správa celého prostředí (všech lokalit) z jedné konzole	
Možnost konfigurovat automatické reakce na různé provozní stavy a chyby	
Podpora záloh na pásku, disk a přenosná zařízení	
Podpora syntetických záloh	
Možnost zálohování P2V (konverze do virtuálního stroje)	
Možnost centrálního upgradu klientů z konzole	
Možnost vytvořit virtuální stroj ze zálohy	
Možnost disaster recovery na čistý nebo jiný hardware	

1.3.15 Způsob publikace do internetu pomocí virtuálního prostředí – zabezpečený přístup k aplikacím

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Použité řešení založeno na dedikovaném (vyhrazeném) protokolu s vysokou mírou stability, odezvy a komprese přenosu na datové lince pro efektivní běh	
Řešení podporuje publikaci jednotlivých aplikací	
Řešení podporuje publikaci celé pracovní plochy (Windows)	
Řešení vynucuje šifrování datového toku mezi klientem a infrastrukturou	
Řešení umožňuje konfiguraci politik pro jednotlivé uživatele/aplikace (neumožnění kopírování souborů z/do mobilního zařízení, neumožnění kopírování (copy-paste) z/do mobilního zařízení apod.)	
Řešení umožňuje přístup k publikovaným aplikacím redundantním způsobem (tzv. vysoká dostupnost – HA a rozklad zátěže)	
Řešení musí nabízet možnost přístupu k aplikacím bez explicitní vazby na použité klientské zařízení (PC, notebook, tablet, chytrý telefon, atd.) a bez vazby na konkrétního výrobce (ochrana proti tzv. „vendor lock“ řešení) Klient pro tyto zařízení musí být k dispozici bezplatně	
Řešení podporuje dvoufaktorovou autentizaci bez nutnosti připojení HW k mobilnímu zařízení	
Auditovatelné ověřování uživatelů s možností tvorby reportů	
Řešení je kompatibilní s virtuálním prostředím zadavatele	

1.3.16 CENTRÁLNÍ SYSTÉM TESTOVÁNÍ ODEZVY WAN

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Technické parametry řešení	
Řešení poskytuje Centrální konzoli s možností konfigurace a distribuce testů na testovací body	
Řešení poskytuje Centrální konzoli s možností přehledného zobrazení stavu všech testů	
Řešení poskytuje Centrální konzoli pro provádění hromadných operací s agenty (např. aktivace/deaktivace)	
Centrální konzole podporuje správu testů provozovaných na dedikovaných testovacích agentech, které jsou součástí řešení. (Dedikovaným agentem se myslí aplikace provozovaná na Win/Lin serveru. Takový server vystupuje v roli testovacího bodu, ze kterého se spouští definované testy)	
Centrální konzole podporuje správu testů spouštěných přes IP SLA agenty na současných aktivních prvcích LAN/WAN sítě Zadavatele	
Z každého testovacího bodu je možné aktivovat minimálně tyto typy testů – Ping, http, DNS, DHCP a Jitter	
Test Ping poskytuje round-trip čas dotazu ZDROJ-CÍL minimálně s těmito parametry: - Latency - Packet Loss	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Test http poskytuje round-trip čas získání cílové web stránky minimálně s těmito parametry: - Latency - HTTP DNS Resolution Time - HTTP TCP Connection Time - HTTP Download Time	
Test DNS poskytuje lookup čas dotazu na DNS server minimálně s těmito parametry: - Latency - Packet Loss	
Test DHCP poskytuje round-trip čas pro získání IP adresy minimálně s těmito parametry: - Latency - Packet Loss	
Test Jitter poskytuje zpoždění a ztrátovost spojení ZDROJ-CÍL minimálně s těmito parametry: - Destination to Source Packet Loss - Jitter Busies - Jitter Egress - Jitter Ingress - Jitter Positive Destination to Source - Jitter Positive Source to Destination - Jitter Negative Destination to Source - Jitter Negative Source to Destination - Late Arrival Packet - Latency - Mean Opinion Score - Missing in Action Packet - Packet Loss - Source to Destination Packet Loss	
Řešení podporuje definice vlastního testu – aktivace skriptu, jehož výstup reprezentuje výsledek testu	
Z každého testovacího bodu je možné aktivovat vlastní test	
Řešení poskytuje nástroje pro integraci a přenos nově získaných údajů do současných operátorských rozhraní	
Řešení umožňuje tvorbu vlastních reportů pro všechny měřené parametry testů, včetně parametrů vlastních testů	
Řešení poskytuje nástroje pro začlenění reportů do centrální konzole dohledového systému Zadavatele (viz popis současného stavu)	
Řešení nabízí minimálně tyto typy reportů: - Trendový report pro vybrané parametry nebo jejich skupiny - TopN report pro vybrané parametry nebo jejich skupiny - Přehledový report o stavu metrik jednotlivých agentů - Service/SLA report s možností nastavení hraničních hodnot pro měřené parametry	
Řešení vyhodnocuje měřené parametry okamžitě při jejich přijetí a porovnává je s nastavenými hraničními hodnotami	
Řešení podporuje dynamické hraniční hodnoty s možností nastavení délky okna nebo počtu vzorků pro výpočet hraniční hodnoty v daném čase	
Při překročení hraniční hodnoty je možné zaslat SNMP Trap a jeho obsah je možné upravit	
Historické hodnoty měřených veličin jsou uloženy v databázi	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
s možností přístupu přes SQL dotazy nebo vlastní API rozhraní	
Řešení podporuje provoz ve virtuálním prostředí Zadavatele	
Řešení podporuje propojení se systémem pro dohled dostupnosti prvků (např. zasílání SNMP Trapů). Detaily o dohledu dostupnosti jsou uvedeny v popisu současného stavu Zadavatele	

1.3.17 Rozvoj zastřešujícího monitoringu

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Minimální požadované technické parametry řešení	
Řešení podporuje příjem událostí a dat minimálně přes tato rozhraní: - SNMP Trap - Syslog - zprávy přijímané systémem pro dohled dostupnosti zařízení – viz popis současného stavu	
Řešení nabízí možnost načítání událostí z externí databáze	
Řešení nabízí možnost načítání událostí z textového souboru	
Přijaté události lze doplnit/obohatit o kontextové informace (minimálně 10 parametrů) z externích zdrojů v podobě textového souboru (např. ePD (Elektronická provozní dokumentace)	
Přijaté události lze doplnit/obohatit o kontextové informace (minimálně 10 parametrů) z externích databází (např. ePD (Elektronická provozní dokumentace)	
Systém umožňuje deduplikaci události přijatých přes různá rozhraní (např. deduplikace událostí přijatých jako SNMP trapy s událostmi přijatými přes systém pro dohled dostupnosti zařízení)	
Řešení obsahuje přednastavené integrace minimálně s těmito systémy třetích stran: - dohled dostupnosti zařízení – viz popis současného stavu	
Zastřešující monitoring nabízí sadu korelačních pravidel/logiky pro zpracování událostí a dat	
Řešení umožňuje zpracování událostí v době přijetí do systému	
Řešení umožňuje zpracování událostí jako výstup akce pravidel (např. při překročení nastavené hraniční hodnoty, při příchodu jiné události)	
Řešení umožňuje zpracování událostí dle pravidel vázaných na čas	
Řešení umožňuje zpracování událostí dle pravidel vázaných na výsledek zpracování aktuálně přijatých událostí a vazbou na aktuální informace v externím datovém zdroji (databáze/textový soubor)	
Řešení umožňuje zasílat notifikace v podobě e-mailu	
Řešení umožňuje zasílat notifikace v podobě SNMP Trapu	
Řešení umožňuje zasílat notifikace v podobě hlášení v grafickém rozhraní uživatele	
Řešení umožňuje zasílat notifikace v podobě spuštění skriptu	
Řešení nabízí různé grafické rozhraní pro různé uživatele v roli operátora, informatika (grafické rozhraní přizpůsobené dle příslušnosti informatika ke krajskému pracovišti), manažera	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Řešení podporuje tvorbu vlastních reportů	
Řešení lze provozovat v IPv4 a IPv6 prostředí současně	
Řešení podporuje provoz ve virtuálním prostředí Zadavatele	
Rozšiřující/upřesňující technické parametry řešení	
Zastřešující monitoring podporuje definici služeb a SLA parametrů	
Historické hodnoty měřených veličin jsou uloženy v databázi s možností přístupu přes SQL dotazy nebo vlastní API rozhraní	
Zastřešující monitoring nabízí/obsahuje integraci do CMDB třetích stran	

1.3.18 AD-HOC TESTOVÁNÍ ODEZVY WAN

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Parametry nabízeného řešení	
Řešení umožňuje spustit test odezvy z jakékoliv stanice v síti Zadavatele přes webový prohlížeč	
Řešení podporuje tzv. „off-line“ režim – provoz bez nutnosti připojení k internetu	
Řešení podporuje/nabízí spuštění testů vůči každému datovému centru Zadavatele	
Provedení testu na žádost přehledně zobrazí průběh testu a jeho výsledky	
Výstup testu obsahuje informace o rychlosti uploadu, downloadu a latenci (zpoždění)	
Řešení podporuje provoz více testovacích bodů pro každého z uživatelů současně	
Grafický vzhled rozhraní testů lze upravit (např. doplnit logo, upravit barevné schéma)	
Grafické rozhraní testů je dostupné češtině	
Přístup ke grafickému rozhraní lze omezit na základě IP adresy/rozsahu uživatele	
Řešení podporuje provoz ve virtuálním prostředí Zadavatele	

1.3.19 PŘECHOD NA WINDOW 8.1

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Řešení zajišťuje migraci všech (cca 14000) stanic ve WAN zadavatele	
Řešení při migraci zachová uživatelská data	
Řešení při migraci zachová programové vybavení stanice	
Řešení při migraci zachová uživatelský profil	
Řešení při migraci zachová konfiguraci aplikací	
Řešení při migraci zachová jednotlivá oprávnění u lokálních souborů	
Řešení podporuje tvorbu několika různých instalačních obrazů (image) – viz příloha č. 6	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Součástí řešení je podpora informatikům ÚP ČR po celou dobu migrace	

1.3.20 Přechod serverů z MS W. 2008 Server R2 na W. 2012 Server

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Řešení zajišťuje migraci všech (cca 900) serverů na pracovištích ÚP ČR	
Řešení při migraci zachová aplikační data na serveru	
Řešení při migraci zachová uživatelská data na serveru	
Řešení při migraci zachová plnou funkčnost instalovaných aplikací na serveru	
Řešení při migraci zachová plnou funkčnost instalovaných rolí serveru	
Řešení při migraci zachová jednotlivá oprávnění u lokálních souborů	
Řešení podporuje tvorbu několika různých instalačních obrazů (image) serveru – viz příloha č. 6	
Součástí řešení je podpora informatikům ÚP ČR po celou dobu migrace	

1.3.21 Konsolidace ochrany E-mailu (Antivir, Antispam)

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Výrobce systému	
Odkaz na www stránky výrobce systému, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Řešení musí pokrýt antivirovou a antispamové ochranu SMTP komunikace na perimetru resortu MPSV	
Řešení musí kapacitně pokrýt 15 000 uživatelů	
Navržené a implementované řešení musí výkonově zajistit průchod 15 000 mailů o velikosti 180 kB / hodinu	
Řešení musí být dostupné i ve formě virtuální appliance	
Zajištění jednotné správy formou vestavěného managementu pro více zařízení	
Konfigurace politik ochrany pro každou emailovou doménu	
Jedno vyhledávání v záznamech (logy) prostřednictvím více zařízení	
Automatické aktualizace virových a spamových definic	
Vyhodnocování spamu na základě reputace odesílatele (jeho IP adresy)	
Na základě domény směrování e-mailu na různé down-stream servery	
Podpora pro napojení DLP řešení	
Možnost generování a zasílání denních, týdenních a měsíčních reportů pomocí e-mailu	

Podpora IPv6	
Podpora TLS šifrování	
Podpora zasílání logů off-box na syslog server	
Podpora tvorby dodatečných pravidel pro filtrování poštovní komunikace	

1.3.22 ROZVOJ ZÁLOHOVÁNÍ NA VELKÝCH PRACOVIŠTÍCH L4

Požadovaná funkcionalita/vlastnost	**Doplní Uchazeč dle nabízeného řešení**
Výrobce systému	
Odkaz na www stránky výrobce systému, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Dostatečný objem pro stávající i budoucí zálohy s možností rozšíření (viz příloha 6)	
Odpovídající datová propustnost pro přenos celkového objemu dat (viz příloha 6)	
Záruka trvanlivosti uložení a neměnnost dat garantovaná výrobcem	
Kompatibilita se stávajícím řešením z hlediska HW a SW	
Pravidelné spuštění aktualizace softwaru	
Možnost vytvářet vlastní a automatické reporty o stavu prostředí	
Systém centralizované distribuce SW na klienty (deployment)	
Zabezpečení datového obsahu šifrováním	
Notifikace stavu aplikace a úloh přes e-mail, applog, SNMP a SMS	
Možnost kompletního přehledu stavu, úloh, historie, alertů a licencí z jedné obrazovky – dashboard	
Audit změn a úprav v konfiguraci aplikace a prostředí	
Podpora duplikačních a vázaných duplikačních úloh	
Podpora deduplikace	
Granulární zálohy a obnovy	
Podpora záloh SQL a virtualizačních platforem VMware, Hyper-V	
Podpora úložišť SAN, NAS, iSCSI, Tape, USB	
Automatické připomenutí expirace licence/maintenance	
Centrální management a správa celého řešení	
Přehledná správa naplánovaných i proběhlých úloh s filtrací a vyhledáváním	
Správa celého prostředí (všech lokalit) z jedné konzole	
Možnost konfigurovat automatické reakce na různé provozní stavy a chyby	
Podpora záloh na pásku, disk a přenosná zařízení	
Podpora syntetických záloh	
Možnost zálohování P2V (konverze do virtuálního stroje)	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Možnost centrálního upgradu klientů z konzole	
Možnost vytvořit virtuální stroj ze zálohy	
Možnost disaster recovery na čistý nebo jiný hardware	

1.3.23 ARCHIVACE ELEKTRONICKÉ POŠTY

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Výrobce systému	
Odkaz na www stránky výrobce systému, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Výrobce systému	
Odkaz na www stránky výrobce systému, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	
Řešení musí pokrýt cca 14 000 uživatelů	
Řešená musí snížit objem databází MS Exchange	
Uživatelsky transparentní přístup do archivu z MS Outlook/Outlook Web Access	
Obnovení smazané zprávy bez zásahu administrátora	
Podpora archivace v MS Exchange 2010 a 2013	
Podpora archivace mailboxů a veřejných složek	
Jeden archiv může sloužit pro více MS Exchange serverů	
Podpora Offline archivace OST souborů	
Možnost stejné řešení rozšířit i pro archivaci MS Sharepoint a souborů na filesystému	
Uložené zprávy v archivním úložišti mohou být komprimovány	
Obsah zpráv a příloh v archivním úložišti může být libovolně indexován	
Uživatelské vlastnosti integrované do poštovního klienta MS Outlook musí podporovat vyhledávání v archivu	
Uživatelské vlastnosti integrované do poštovního klienta MS Outlook musí podporovat rušení zpráv v archivu	
Uživatelské vlastnosti integrované do poštovního klienta MS Outlook musí podporovat vyhledávání podle atributů zpráv a příloh	
Uživatelské vlastnosti integrované do poštovního klienta MS Outlook musí podporovat archivaci jednotlivých položek nebo složek	
Podpora Outlook Web Access minimálně na úrovni propojení odkazů s archivem	
Podpora Outlook Web Access minimálně na úrovni prohlížení archivovaných zpráv přes odkazy	
Auditovací mechanismus řešení musí být konfigurovatelný	

Audit všech událostí musí být zaznamenán do SQL databáze	

1.3.24 NÁHRADA TMG

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Řešení zajišťuje migraci současného TMG serveru na nový systém	
Řešení při migraci zachová veškerou současnou funkcionalitu TMG	
Řešení při migraci zjednoduší současná publikační pravidla	
Řešení podporuje IPv6	
Řešení zabezpečuje ochranu AJAX a JSON aplikací	
Řešení zabezpečuje ochranu proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force)	
Podpora SSL (šifrování a dešifrování)	
Podpora application visibility a reportingu – monitorování URI	
Autentikace klientů přes LDAP/Radius	
Podpora pro TLS 1.2	
Podpora SSL Forward proxy	
Podpora SSL certifikátů podepsaných SHA-2 algoritmem	

1.3.25 ZÁLOHOVÁNÍ STANIC – PILOT PRO 500 UŽIVATELŮ

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Výrobce systému	
Odkaz na www stránky výrobce systému, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Záruka trvanlivosti uložení a neměnnost dat garantovaná výrobcem	
Kompatibilita se stávajícím řešením z hlediska HW a SW	
Pravidelné spuštění aktualizace softwaru	
Systém centralizované distribuce SW na klienty (deployment)	
Zabezpečení datového obsahu šifrováním	
Automatické bezobslužné fungování na klientovi	
Možnost vícenásobných automatických sekundárních a offline záloh (duplikace)	
Podpora lokálních, externích, síťových a WAN (FTP) úložišť	
Možnost uživatelem provedené obnovy souborů či složek (granularita)	
Centrální management a správa celého řešení	
Přehledná správa naplánovaných i proběhlých úloh	
Možnost disaster recovery na čistý, jiný nebo virtuální hardware	
Prohledávání záloh na úrovni souborů a složek bez nutnosti předchozí obnovy uživatelem	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Možnost částečné obnovy bez vlivu na stávající data	
Škálovatelná automatická retence a mazání starých záloh	
Možnost zálohování P2V (konverze do virtuálního stroje)	
Možnost přímého bootování do obnovovacího režimu	
Možnost jednorázových nezávislých záloh a konverzí do virtuální podoby	
Možnost kopírování celých logických a fyzických disků	
Podpora komprese záloh	
Možnost automaticky zálohy dělit na požadovanou velikost	
Podpora pre/post skriptů a příkazů	
Možnost škálovat výkon a rychlost zálohování	
Notifikace do logu aplikace, windows logu, e-mailu, SNMP	
Možnost zálohování specifických souborů (dokumenty, média, obrázky, hudba, databáze…)	
Možnost automaticky spuštěných záloh v definovaném případě (instalování/odinstalování nějaké aplikace, start vybrané aplikace, přihlášení/odhlášení uživatele, zvýšená bezpečnostní hrozba)	

1.4 OBLAST BEZPEČNOSTI

1.4.1 VYTVOŘENÍ SYSTÉMU INFRASTRUKTURNÍ AUTENTIZACE

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Výrobce komponent řešení	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Vyšší stupeň bezpečnosti, minimálně úroveň dvoufaktorové autentizace, např. vlastní (tj. personifikovaný) autentizátor a PIN	
Autentizátor bude podporovat platformy OS desktopů Microsoft, Linux, OS X	
Autentizátor bude podporovat i mobilní platformy řady: iOS, Android	
Podpora více elektronických identit – uživatel bude schopen použít jeden autentizátor k ověření u více aplikací, a to různými, vzájemně nezávislými elektronickými identitami	
Nezávislost elektronické identity (respektive identit) uživatele na jeho skutečné osobní identitě	
Řešení bude implementováno v IT prostředí zadavatele („on-premise“), mělo by však mít možnost být provozováno i formou Cloudové služby „SaaS“	

Podpora centrální správy a evidence autentizátorů	
Autentizační systém musí být provozovatelný i ve virtuální prostředí serverů i pracovních stanic	
Řešení bude podporovat čárové kódy anebo QR kódy, pro snadnější interakci uživatele s autentizátorem	
Podpora samoobslužných „selfservice“ procesů pro: inicializaci, zneplatnění a obnovu přístupové (elektronické) identity	
Proces autentizace nebude vyžadovat dodatečné náklady třetích stran (nebude např. vyžadováno zasílání SMS zpráv)	
Proces autentizace neumožní odposlech autentizačních informací a jejich následné zneužití (např. jejich podvržení)	
Kryptooperace, které probíhají v zařízení koncového uživatele, nesmí být možné zneužít jinou aplikací třetí strany (souvisí s předchozím bodem)	
Systém bezpečné autentizace bude podporovat i ověření standardizovanými AAA protokoly, např. TACACS+, Radius	

1.4.2 NASAZENÍ PROCESŮ PRO SOC

Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.4.3 NÁHRADA INTERNETOVÝCH LOAD BALANCERŮ

Požadovaná funkcionalita/vlastnost	**Doplní Uchazeč dle nabízeného řešení**
Výrobce komponent řešení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Nasazení dvojice nezávislých HW zařízení ve funkci rozvažování zátěže příchozího internetového provozu (Internet loadbalancer), každé zařízení v jiné lokalitě	
Podpora DNSSec protokolu	
Datová propustnost alespoň 5 Gbps L4/L7 či více	
Minimální propustnost L4 HTTP 1.0 požadavků: 550 K za sekundu	
Minimální počet současných L4 spojení: 5M	
Možnost připojení min. 8x 1GE 1000BaseTX	
Možnost rozšíření o SFP/SFP+ moduly	
Samostatné rozhraní pro management	
Vestavěná ochrana proti DoS útokům	
Podpora IPv6	
Zdvojené napájení	

Možnost doprogramovat si filtrovaci pravidla pro aplikace	
Automatické nahrávání a aplikování nových signatur	
Blokování útočníků na základě geolokace (až na úroveň regionů)	
Podpora SSL (šifrování a dešifrování)	
Podpora standardů PCI DSS, HIPAA, Basel II a SOX	
Podpora různých typů reportů – PCI, geolokační reporty	
Podpora application visibility a reportingu – monitorování URI	
Podpora aplikačního firewallu ve virtuálních kontextech	
Možnost autentizace klientů přes LDAP/Radius	
Možnost připojení k monitorovacích nástrojů třetích stran prostřednictvím otevřeného API	
Možnost přidat vlastní funkce pomocí skriptování	
Podpora Active-Active, Active-Passive módů	
Povolení/zakázání ICMP pro VIP	
Podpora pro TLS 1.2	
Podpora SSL Forward proxy	
Granulární logování / logování per aplikace	
K dispozici jako autonomní box nebo ve formě šasi	
Management: sériový port, GUI, příkazový řádek, iLO	
Podpora filtrace paketů	
Podpora ToS, QoS (marking/preservation/mimic)	
Podpora rozvažování zátěže založené na poměrech (ratio based) s CARP perzistencí	
Podpora SSL certifikátů podepsaných SHA-2 algoritmem	
Podpora práce s 4096bit klíči	
Podpora SNMP (v1/v2c/v3)	

1.4.4 VYTVOŘENÍ VNITŘNÍCH ŘÍDICÍCH DOKUMENTŮ

Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.4.5 SOC – SIEM A BEZPEČNOSTNÍ FLOW MONITORING, VČ. PROVOZU SLUŽBY NA 2 ROKY

Požadovaná funkcionalita/vlastnost	**Doplní Uchazeč dle nabízeného řešení**
Výrobce komponent řešení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Sběr datových statistik ve formátech NetFlow v5, v9, IPFIX a následné vyhodnocování	
Sledování statistik u protokolů IPv4, IPv6, VLAN, MPLS Schopnost rozeznávání aplikací (např. pomocí NBAR2 či jiné)	
Umístění sledovacích zařízení (sond) ve dvou různých lokalitách DC zadavatele	
Sběr datových statistik v alespoň 6 kritických částech sítě v každé z lokalit DC zadavatele (z tzv. SPAN portů); možnost připojení pomocí GE (1000Base-TX) nebo 10GE (10Gbase-SR)	
Kapacita řešení schopna zpracovat (sledovat) na každém ze sledovaných portů datový tok alespoň cca 0,5 M paketů/s	
Schopnost systému rozeznávat anomálie v datovém provozu	
SIEM nástroj schopný zpracovávat alespoň 5000 EPS	
Napojení SIEM nástroje na nově nasazený systém sběru a vyhodnocování NetFlow statistik i na systém FW, antivirové ochrany, antispamové ochrany, systém IPS, antibot a antimalware systém a systém pro filtraci internetového provozu	
Variabilita v možnostech napojení SIEM nástroje na různé další zdroje bezpečnostních informací, která umožní sběr a vyhodnocování dat ze systémů a aplikací nasazených v síti zadavatele (pro přehled o možných zdrojích těchto informací viz popis stávajícího stavu KSI zadavatele)	
Služba (její technologické prostředky) musí být případně rozšiřitelná o risk management nástroj a jeho výstupy a možnost simulace napadení	
Hlášení (reporty) z technologických prostředků služby by měly zohledňovat skutečnou relevanci událostí nejen dle signatur a pravidel, ale i dle skutečné topologie a prvků v síti, jejich důležitosti a skutečných zranitelností	
Testování zranitelnosti a kontrola souladu konfigurací pro 20 webových aplikací a 100 síťových prvků/serverů. Vytváření reportů a jejich vyhodnocování je požadováno minimálně s periodou 1x kalendářní měsíc	
Strojová inventarizace aktiv:	<prázdné>
Možnost vyhledání a seskupení nalezených aktiv pomocí IP adresy, doménového jména anebo jeho části, NETBIOS jména anebo jeho části, běžící služby (otevřeného portu TCP/UDP), operačního systému	
Možnost přiřazení atributů skupinám identifikovaných aktiv s informacemi o vlastnících aktiv, jejich geografickém umístění, typu zařízení (web server, db server, desktop apod.) a hlavně tzv. business impact atribut, který umožní efektivněji vyhodnocovat dopady nalezených zranitelností	
Skenování webových aplikací:	<prázdné>
Možnost reportů OWASP Top 10 a WASC Top 10	
Vyhnutí se přetížení testovaných aplikací pomocí možnosti nastavení intenzity skenování (alespoň 5 úrovní)	
Možnost zúžení (zrychlení) testu pomocí možnosti definovat a hledat jen určité zranitelnosti	
Další funkce	<prázdné>

Kontrola souladu konfigurací sledovaných serverů a síťových prvků s předefinovanými vzory (knihovna předefinovaných vzorů s možností definice vlastních vzorů a politik)	
Integrace dodaných technologií do celkového SOC řešení – technologická i procesní integrace (návaznost projektu na další projekt tohoto výběrového řízení – „Nasazení procesů pro SOC“ – viz výše)	
Služba (její technologické prostředky) musí být schopna:	<prázdné>
Budování dlouhodobých profilů chování zařízení na síti z hlediska poskytovaých a využívaných služeb, objemů provozu a komunikačních partnerů	
Analýzy profilů chování a odhalování jejich změn (profily pro datové toky, klient/server, komunikační partnery, strukturu provozu, aktivity apod.)	
Detekce anomálií v síti (změn u profilu chování, heterogenní komunikace, přenosů velkých objemů dat, nedostupnosti služeb, cizích zařízení v síti apod.)	
Kontroly chyb na úrovni konfigurace (detekce IP adres bez reverzních DNS záznamů, špatné konfigurace automatických aktualizací, zpoždění na síti apod.)	

1.4.6 SYSTÉM PRO DETEKCI POKROČILÉHO MALWARU (ANTIBOT, ZERO-DAY MALWARE…)

Požadovaná funkcionalita/vlastnost	**Doplní Uchazeč dle nabízeného řešení**
Výrobce komponent řešení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Systém musí umožňovat kontrolu a ochranu kritických segmentů jak vnějších (Internet, DMZ), tak i vnitřních (např. segmenty v DC), návrh seznamu kontrolovaných segmentů a způsobu jejich kontroly bude předmětem souvisejícího projektu	
Možnost integrace řešení do SIEM nástrojů v návaznosti na další řešené dílčí projekty	
Záruka vysoké aktuálnosti a přesnosti signatur škodlivého kódu (přístup ke globální databázi bezpečnostních informací výrobce) a rychlosti reakce na nově objevené typy škodlivého kódu (update signatur a detekčních pravidel)	
Režim práce, který nepřeruší probíhající datovou komunikaci v případě selhání jednotlivé komponenty	
Řešení musí být navrženo tak, aby selhání jednotlivé komponenty neznamenalo celkové přerušení funkce antimalware a antibot ochrany v KSI zadavatele	
Podpora dynamických detekčních mechanismů pracujících na více sofistikovaném principu než AV vzorky pro ochrany před útoky, které nejsou ještě pro AV nástroje známy	
Globální korelace informací a vyhodnocení analýzy kódu pro maximální stupeň ochrany s minimalizací false-positive	

Provádění antimalware a antibot funkcí na 2 HW zařízeních v každém ze dvou DC, každý pár v DC v redundatním režimu (je povoleno pro tuto funkci využít HW zařízení dodané v rámci dalších poptávaných projektů, pokud to tato zařízení umožňují)	
Požadovaný počet a typ rozhraní: min. 2x 10Gbase-SR/zařízení	
Aktivní ochrana před malwarem s detekcí známých nebo podezřelých malware nezávislá na aktuálních databázích AV dodavatelů	
Ochrana před malwarem typu „zero day attack“, které nelze detekovat tradičními antiviry	
Možnost dohledání malwaru – jeho přenosy v síti mezi stanicemi a mutace přímo v GUI centralizované konzoli	
Ochrana proti aktivitě botnetů – reputace IP adres, DNS a URL záznamů	
Blokování komunikace na IP adresy řídicích center botnetů. Detekce aktivit botnetů pomocí behaviorální analýzy	
Prevence zero-day útoků na základě typu a obsahu komunikace	
Možnost emulace nových variant malwaru v případě, že není známa antivirová/antimalware signatura	
Emulace typů souborů, min: MS Office Powerpoint, Word, Excel, .pdf, .exe)	
Antimalware a antibot funkce musí být spravovatelné z nabízeného centrálního monitorovacího a konfiguračního systému (centrální dohledové konzole)	
Centrální dohledová konzole musí být schopna dohlížet a spravovat více zařízení s aktivovanou funkcí antimalware a antibot	

1.4.7 Systému pro pokročilou detekci průniků IDS /IPS

Požadovaná funkcionalita/vlastnost	**Doplní Uchazeč dle nabízeného řešení**
Výrobce komponent řešení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Systém musí umožňovat kontrolu a ochranu kritických segmentů jak vnějších (Internet, DMZ), tak i vnitřních (např. segmenty v DC); návrh seznamu kontrolovaných segmentů a způsobu jejich kontroly bude předmětem souvisejícího projektu	
Možnost integrace řešení do stávajících management systémů používaných u zadavatele a případně i (v návaznosti na další řešené projekty) možnost integrace do SIEM nástrojů	
Záruka vysoké aktuálnosti a přesnosti IPS signatur (přístup ke globální databázi bezpečnostních informací výrobce) a rychlosti reakce na nově objevené typy útoků (update IPS signatur a detekčních pravidel)	
Režim práce, který nepřeruší probíhající datovou komunikaci v případě selhání IPS komponenty	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Řešení musí být navrženo tak, aby selhání jednotlivé komponenty neznamenalo celkové přerušení funkce IPS	
Integrované korelace událostí s využitím globálních databází pro detekci kompromitovaných stanic a klasifikaci stupně jejich nebezpečnosti	
Detekce prostředí a automatické přizpůsobení detekčních mechanismů pro minimalizaci false-positive událostí	
Možnost rozšíření o aplikační firewall	
Možnost importu Snort pravidel, s možností úprav a vytváření pravidel vlastních	
Sdílení informací (uživatel, stanice, typ útoku apod.) se systémy řízení přístupu k síti	
Navrhované řešení musí respektovat princip ochrany investic	
Provádění IPS funkcí na 2 HW zařízeních v každém ze dvou DC, každý pár v DC v redundatním režimu (je povoleno pro tuto funkci využít HW zařízení dodané v rámci dalších poptávaných projektů, pokud to tato zařízení umožňují)	
Požadovaný počet a typ rozhraní: min. 2x 10Gbase-SR/zařízení	
Agregovaná propustnost IPS při plném zatížení se zapnutými inspekcemi alespoň 10 Gbps	
Počet inspektovaných spojení v reálném čase alespoň 7M	
Množství nově otvíraných spojení za sekundu, inspektovaných na IPS alespoň 170 k	
Podpora etherchannel load balancingu	
Podpora 802.1Q tagovaných rámců	
Možnost instalace přídavných modulů rozhraní	
Zařízení musí podporovat typy modulů pro případné rozšíření: 1000Base-T, 1000Base-SX, 10GBase-SR, 10Gbase-LR	
Možnost vypnutí ochrany v případě přetížení hardwaru zdrojů (hrozba zahlcení systému) nad definovanou prahovou hodnotu	
Možnost práce v L2 transparent módu	
Inspekce pro IPv4 i IPv6	
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií	
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	
Možnost psaní zákaznických filtrů	
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	
IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	
IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“, jako je spyware, phishing nebo Botnet C&C	
IPS musí umět detekovat a blokovat útoky na síťovou infrastrukturu firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače apod. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii	

Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo z management konzole	
Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku	
Podpora SNMPv3, privátní MIB, Syslog, SNMP Trap	
IPS musí být spravovatelné z nabízeného centrálního monitorovacího a konfiguračního sytému (centrální dohledové konzole)	
Centrální dohledová konzole musí být schopna dohlížet a spravovat více IPS senzorů	
Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	
Centrální dohledová konzole musí být schopna udržovat a spravovat operační systém IPS dohledového systému i senzorů	
Aktualizace lze na management platformu nahrát i ručně	
Provedení aktualizací lze načasovat a provést automaticky	
Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky zobrazeny v GUI dohledové konzole	
Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně i podle časového harmonogramu	
Centrální dohledová konzole musí být schopna exportovat reporty do formátů jako PDF, CSV apod.	
Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů	
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události apod.	
Podpora posílání událostí formou syslog, e-mail, SNMP na externí platformy	
Předdefinované IPS politiky na zařízeních	

1.4.8 ZABEZPEČENÍ DAT NA PC A MOBILNÍCH ZAŘÍZENÍCH

Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.4.9 NASAZENÍ SYSTÉMU OCHRANY DŮVĚRNOSTI DAT (DLP) + KLASIFIKACE DAT MPSV

Požadovaná funkcionalita/vlastnost	**Doplní Uchazeč dle nabízeného řešení**
Výrobce systému	
Odkaz na www stránky výrobce systému, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Řešení musí kapacitně pokrýt 50 uživatelů v pilotním ověření a 200 uživatelů v plošném nasazení	
Řešení musí podporovat rozšíření i na další vrstvy informačního systému zadavatele (storage, perimetr)	
Omezení úniku dat kopírováním na USB/Flash disky	
Omezení úniku dat e-mailem, freemailem	
Centrální management pro tvorbu a distribuci politik, včetně zasílání alertů a tvorby a zasílání reportů	
DLP komponenty musí být spravovány a vyrozumívány centrálně z jedné konzole	
Podpora dalších bezpečnostní řešení – navázání klasifikace, šifrování dat na systém prevence ztráty dat – DLP	
Řešení musí podporovat práci s klasifikačními kritérii uloženými v dokumentech i v metadatech dokumentů	
Podpora práce se strukturovanými i nestrukturovanými daty	
Řešení musí podporovat nasazení v reaktivním i monitorovacím módu	
Možnost napojení na požadovaný SIEM nástroj standardizovanými protokoly (např. SYSLOG, SNMP)	

1.4.10 Upgrade FW soustavy (interní)

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Výrobce komponent řešení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Vzhledem k důležitosti interní FW soustavy musí být řešení postaveno jako robustní a vysoce dostupné přes dvě DC zadavatele	
Předpokládaná je instalace dvou párů fyzických zařízení v HA režimu (cluster), každý pár v jiném DC	
Každé z fyzických zařízení bude připojeno k okolní infrastruktuře min. 2x 10G (10GBase-SR)	
Datová propustnost FW vyšší než 75 Gbps (měřeno dle RFC 3511 s 1518B UDP pakety)	
Podpora virtualizace (provoz alespoň 10 virtuálních kontextů v HA režimu)	
Analýza stávajícího nastavení FW soustav v DC zadavatele, optimalizace nastavení a přenos optimalizované konfigurace na novou HW platformu	
Integrace nových zařízení do stávajícího management systému pro správu FW soustavy	

Součástí projektu bude také sjednocení správy interní a externí FW soustavy a migrace virtuálního FW pro externí sítě (Govbone, CMS…) na externí FW soustavu	
Navrhované řešení musí respektovat princip ochrany investic	
FW Cluster	<prázdné>
Požadovaný počet a typ rozhraní: min. 2x 10Gbase-SR/zařízení, min. 8x1000Base-TX/zařízení	
Možnost řízení politik na základě uživatelských skupin z Active Directory	
Podpora software agenta na koncové stanice pro přesné získávání identit, min. pro systémy Windows a Mac	
Možnost identifikace uživatelů na základě webového portálu – podpora ověření jméno/heslo (nedoménoví uživatelé) a SSO Kerberos (doménoví uživatelé)	
Detekce a řízení síťových aplikací. Minimální počet rozpoznávaných aplikací: alespoň 3000	
Detekce a řízení síťových aplikací. Minimální počet aplikací/pluginů pro sociální sítě: alespoň 20000	
Případná možnost jednoduchého následného rozšíření platformy o další bezp. funkce: IPS	
Případná možnost jednoduchého následného rozšíření platformy o další bezp. funkce: příchozí a odchozí HTTPS inspekce	
Případná možnost jednoduchého následného rozšíření platformy o další bezp. funkce: emulace neznámých hrozeb malware	
Případná možnost jednoduchého následného rozšíření platformy o další bezp. funkce: blokování botnetů	
Podpora IPSec VPN tunelů	
Počet nových spojení za vteřinu (CPS): minimálně 170 000	
Možnost rozšíření o 4x 1Gb SFP rozhraní	
Možnost rozšíření o 2x 10Gb SFP+ rozhraní	
Počet současných spojení: min. 7 000 000	
Vysoce dostupné řešení bezpečnostních bran s možností režimu active-standby a active-active	
Stavová synchronizace TCP, UDP a NAT spojení	
Out of band management	
Konfigurace bezpečnostní politiky prostřednictvím GUI rozhraní Vzdálené připojení pomocí protokolů SSH a HTTPS	
Podpora debuggování problémových scénářů na úrovni L2 – L7	
Možnost nasazení pravidelného automatického zálohování konfigurace (na základě časového rozvrhu), s možností automatického nahrání na vzdálený SCP server	
Bezpečnostní logy ukládány na fyzicky oddělenou management platformu	
Virtuální FW	<prázdné>
Podpora automatického vytváření statických (1-1) i dynamických (1-N) NAT pravidel pro jednotlivé management objekty	
Kontrola síťových protokolů na aplikační vrstvě, včetně dynamického otevíraní portů pro specifické síťové protokoly (např. DCE-RPC, FTP, SIP, H.323, MGCP)	
Kontrola síťových protokolů na aplikační vrstvě v případě využívání nestandardních portů	
Řízení přístupu MS DCE-RPC na základě UUID	

Každá virtuální firewall instance musí implementovat: vlastní bezpečnostní politiku, stavové, routovací a ARP tabulky, síťové nebo virtuální rozhraní. Řízení hardwarových zdrojů pro jednotlivé virtuální firewall instance (CPU, paměť)	
Dynamické řízení hardwarových zdrojů pomocí nastavení priorit pro jednotlivé virtuální firewall instance.	
Monitoring využívaných zdrojů pro jednotlivé virtuální firewall instance (počet spojení, využívání CPU, paměť)	
Vytváření dedikovaných virtuálních instancí zabezpečujících přepínání a směrování paketů mezi virtuálními firewally, a mezi virtuálními firewally a externími segmenty	
Přímá propagace veřejných IP adres virtuálních firewall instancí ze stejného síťového rozsahu, bez nutnosti NATovaní (virtuální L2 propoj v rámci virtualizační platformy)	
Podporované režimy virtuálních firewall instancí – L3 routovací a L2 transparentní režim	
Load balancing virtuálních firewall instancí mezi fyzické členy clusteru firewall platformy	
Je-li potřeba, počet dodávaných licencí pro dedikované virtuální prvky zabezpečující přepínání a směrování (L2, L3) – nad rámec licencí pro virtuální firewall instance, min. 5 ks	
Management FW	<prázdné>
Jednotný management pro všechny bezpečnostní aplikace s možností definice administrátorských rolí	
Centrální jednotná správa politik z grafické aplikace	
Funkcionalita korelace logů, analýzy a správy bezpečnostních událostí s předefinovanými pohledy/dotazy	
Definice bezpečnostních pravidel na základě identity uživatele nebo jeho uživatelské skupiny z AD	
Možnost vytváření uživatelsky definovatelných reportů (na základě log záznamů a bezpečnostních událostí)	
Funkce centrálního logování s dostupností logů a událostí: min. 60 dnů zpět	
Management musí být fyzicky oddělen od firewall platformy – na samostatném hardwaru nebo jako softwarová licence na virtuálním serveru	
Podpora tvorby revizí jednotlivých verzí bezpečnostní politiky	
Podpora vyhledávání v pravidlech, vyhledávání textových výrazů/objektů/IP adres nebo prohledávaní všech objektů	
Management musí být schopen dohledat pro každý objekt jeho výskyt v aktivních i neaktivních pravidlech nebo v jiných objektech (např. ve skupinách)	
Možnost segmentace politik do samostatných logických oddílů	
Hit count statistiky pro jednotlivá pravidla za účelem optimalizace bezpečnostní politiky	
Integrovaný monitoring musí poskytovat grafické rozhraní pro sledování parametrů v reálném čase (využití paměti, CPU, počet navázaných spojení, počet nově otevřených spojení za sekundu, propustnost, atd.)	
Centrální ukládání logů z firewall platforem	
Práce s bezpečnostními logy, a to zejména filtrace a prohledávaní logů, export do souboru, definování vlastních permanentních filtrů	

Podpora pravidelného automatického zálohování konfigurace (na základě časového rozvrhu), s možností nahrání zálohy na vzdálený SCP server	
Minimální podporovaná velikost diskové kapacity pro dlouhodobé ukládaní log záznamů (je-li disková kapacita omezena licencí, licence pro požadovanou velikost musí být součástí nabídky) = min. 16 TB	

1.4.11 Nasazení Aplikační FW soustavy

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Výrobce komponent řešení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Nasazení čtveřice nezávislých HW zařízení ve funkci webového aplikačního HW, každý pár v jiné lokalitě DC	
Podpora IPv6	
Možnost připojení min. 8x 10/100/1000BaseTX	
Možnost rozšíření o SFP+ moduly	
Nezávislé rozhraní pro management	
Datová propustnost zařízení alespoň 10 Gbps či více na L4/L7	
Minimální propustnost L4 HTTP požadavků: 1,25 M za sekundu	
Minimální počet současných L4 spojení: 10 M	
SSL akcelerace v HW	
Počet SSL transakcí za sekundu min. 4500 (při použití 2K klíče)	
Počet současných SSL transakcí min. 850 000	
Integrace s nástrojem na detekci zranitelností webových aplikací (samostatný projekt)	
Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP top10	
Zdvojené napájení	
Možnost doprogramovat si filtrovací pravidla pro aplikace	
Ochrana AJAX a JSON aplikací	
Ochrana proti OWASP Top 10 útokům	
Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force)	
Podpora Captcha metody – automatické odlišení skutečných uživatelů od robotů	
Integrovaný XML firewall	
Podpora maskování/odstranění citlivých informací – čísla kreditních karet, číslo pojištění…	
Automatické nahrávání a aplikování nových signatur	
Podpora pozitivního a negativního bezpečnostního modelu (dle OWASP)	
Blokování útočníků na základě geolokace (až na úroveň regionů)	

Podpora ICAP pro antivirovou kontrolu – pro SOAP a SMTP	
Ochrana SMTP a FTP na alikační úrovni	
Podpora SSL (šifrování a dešifrování)	
Podpora standardů PCI DSS, HIPAA, Basel II a SOX	
Podpora různých typů reportů – PCI, geolokační reporty	
Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials a Microsoft SharePoint	
Podpora application visibility a reportingu – monitorování URI	
Možnost importu zranitelnosti aplikací z alespoň některých z následujících skenerů: • Cenzic Hailstorm • WhiteHat Sentinel • IBM Rational AppScan QualysGuard Web Application Scanning	
Podpora aplikačního firewallu ve virtuálních kontextech	
Podpora REST API	
Autentikace klientů přes LDAP/Radius	
Rozšířená podpora CSHUI – detekce aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu	
Možnost aktivovat L4-7 LoadBalancing, ICSA certifikovaný webový a síťový firewall, SSL VPN na jedné platformě HW	
Možnost připojení monitorovacích nástrojů třetích stran prostřednictvím otevřeného API	
Možnost přidat vlastní funkce pomocí skriptování	
Podpora Active-Active, Active-Passive módů	
Podpora ISAP	
Povolení/zakázání ICMP pro VIP	
Podpora pro TLS 1.2	
Podpora SSL Forward proxy	
Granulární logování / logování per aplikace	
K dispozici jako autonomní box, nebo ve formě šasi	
Management: sériový port, GUI, příkazový řádek, iLO	
Podpora alespoň pro 15 metod rozvažování zátěže	
Podpora filtrace paketů	
Podpora ToS, QoS (marking/preservation/mimic)	
Podpora rozvažování zátěže založené na poměrech (ratio based) s CARP perzistencí	
Plná podpora IPv6, IPv4/IPv6 gateway	
Podpora SSL certifikátů podepsaných SHA-2 algoritmem	
Podpora práce s 4096bit klíči	
Podpora SNMP (v1/v2c/v3)	

1.4.12 FILTROVÁNÍ INTERNETOVÉHO PROVOZU

Požadovaná funkcionalita/vlastnost	**Doplní Uchazeč dle nabízeného řešení**
Výrobce komponent řešení	

Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Standardní uživatelé: nasazení čtveřice nezávislých HW zařízení ve funkci HTTP/HTTPS proxy ve dvou lokalitách DC, každý pár pracující v redundantním režimu	
Uživatelé VPN JobKlub a Kiosek: využití dvojice nezávislých HW zařízení ve funkci HTTP/HTTPS proxy v jedné lokalitě DC, pár pracující v redundantním režimu	
Připojení každého zařízení ke stávající infrastruktuře min. 2x 1GE (preferováno 1000Base-TX připojení) s možností práce v LACP módu	
Webový filtr orientovaný na webové stránky navštěvované uživateli v ČR	
Funkce HTTP/HTTPS proxy pro min. 14 500 uživatelů (proxy pro standardní uživatele) a pro min. 500 uživatelů (proxy pro uživatele speciálních VPN JobKlub a Kiosek)	
Podpora inspekce HTTPS provozu	
Antivirová ochrana aplikovaná na kontrolovaný provoz (licence na dobu alespoň 3 let)	
Navrhované řešení musí respektovat princip ochrany investic	
Podpora široké škály autentizačních mechanismů (Active Directory, LDAP, RADIUS nebo s vlastní, již existující autentizační infrastrukturou)	
Pravidla vázaná na konkrétního uživatele nebo skupinu uživatelů pro stanovení různých politik pro různé pracovní týmy	
Podpora single-sign-on politiky pro uživatele nebo jeho pracovní pozici nezávisle na počítači, ze kterého pracuje	
Volitelný modul antivirové kontroly (podpora více AV produktů třetích stran)	
Antivirová ochrana kontrola HTTP, HTTPS, FTP, FTPS	
Kontrola komprimovaných souborů	
Kontrola stahovaných souborů	
Filtrace stahovaných souborů dle: velikosti a/nebo přípony souboru	
Ověřování přípony souboru (true-type file detection)	
Možnost detailně a jednoduše analyzovat databáze záznamů o činnosti jednotlivých zaměstnanců nebo týmů	
Možnost reportingu navštívených webových stránek s informací, zda byl přístup blokován nebo povolen	
Více jak 60 kategorií v základu, možnost používat logické operátory mezi nimi a tími přesněji nastavit obsah, který je pro uživatele povolen nebo zakázán	
Možnost samostatné kategorie pro www šířící malware	
Možnost vlastní specifikace kategorií	
Možnost zařazení www do více kategorií	
Možnost kategorizace podle URL, ne podle celé domény či části domény	

Podpora white-list a black-list pro přesnější doladění obsahu pro dané uživatele	
Možnost snadného propojení s proxy serverem (např. Squid) anebo funkce proxy serveru	
Možnost zpřístupnění požadovaného webu v monitorovaném režimu a/nebo na pouze omezenou dobu	
Možnost filtrace P2P sítí	
Možnost automatické i manuální aktualizace	
Centrální vzdálená správa zařízení pro filtraci	
Logování událostí v jednom místě	

1.4.13 Ochrana proti DDOS útokům

Požadovaná funkcionalita/vlastnost	**Doplní Uchazeč dle nabízeného řešení**
Výrobce komponent řešení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Ochrana dvou nezávislých datových přípojek do internetu (každá v jiné lokalitě DC)	
Předpokládaná instalace samostatných HW zařízení pro DoS/DDoS ochranu	
Ochrana před DoS/DDoS útoky na principu zneužití šířky přenosového pásma (flooding)	
Ochrana před DoS/DDoS útoky na principu zneužití zdrojů serverů (application DoS: HTTP, SIP, TCP SYN flood atd.)	
Režim práce zařízení: L2 transparent	
Možnost připojení min. 4x 1000BaseTX a 2x slot pro 1Gbps SFP moduly	
Nezávislé rozhraní pro management 10/100/1000BaseTX	
Možnost režimu interního fail-open/fail-close pro 1000BaseTX rozhraní	
Datová propustnost alespoň 2 Gbps či více	
Podpora IPv6 a ochrana proti DoS/DDoS útokům vedeným i pomocí IPv6	
Zdvojené napájení	
Podpora režimu práce v tzv. clusteru	
Plná integrace se stávajícím managementem	
Navrhované řešení musí respektovat princip ochrany investic	
Síťová podpora	<prázdné>
VLAN (802.1Q)	
Podpora MPLS RD	
Podpora enkapsulace (pro bezpečnostní inspekci) VLAN, MPLS, L2TP, GRE, GTP, IP-in-IP	
Plně transparetní na bezpečnostních portech	
Podpora Jumbo rámců	
Metody ochrany – přehled	<prázdné>

Behaviorální analýza provozu (NBA – network behavioral analysis)	
Systém prevence průniku (IPS – Intrusion Prevention system)	
Ochrana před útoky na odepření služby (útoky typu flood – SYN, ICMP, TCP, UDP atd.)	
Blokování na základě seznamu IP (ACL – Access Control List)	
Možnost zvolit mezi pouze „monitorováním“ a „monitorováním a blokováním“	
Maximální přesnost detekce (eliminace falešných detekcí) pomocí dotazovacího mechanismu (challenge). Podezřelému zdroji je poslán dotaz (TCP paket, HTTP redirecticon, JAVA script) a vyhodnotí se jeho reakce	
Behaviorální analýza provozu (NBA – Network Behavioral Analysis)	<prázdné>
Rozpoznávání a blokování zneužití legálních aplikací (L7 floody, např. HTTP GET Flood)	
Rozpoznávání a blokování horizontálního i vertikálního skenování	
Rozpoznávání a blokování typu „brute force“	
Rozpoznávání a blokování neznámých útoků (zero-day attacks)	
Rozpoznávání a blokování šíření malwaru	
Průběžné sledování útoků a automatická úprava dynamicky generovaných řetězců při změně útoku	
Analýza a učení se chování pro síť, HTTP servery, DNS servery, aplikační servery	
Ochrana před útoky na odepření služby (DoS a DDoS)	<prázdné>
Rozpoznávání a blokování ICMP flood	
Rozpoznávání a blokování IGPM flood	
Rozpoznávání a blokování TCP SYN, SYN ACK, FIN, RESET, fragment flood	
Rozpoznávání a blokování TCP paketů, které nepatří k navázanému spojení (TCP Out of state flood)	
Podpora SYN-cookies mechanismu	
Anomalie protokolů a provozu	<prázdné>
Rozpoznávání a blokování podle předdefinovaných řetězců (signatur)	
Rozpoznávání a blokování na základě protokolových anomálií	
Rozpoznávání a blokování na základě anomálií provozu (rate based)	
Možnost definovat vlastní řetězce (signatury) pro rozpoznávání a blokování	
Způsob nasazení	<prázdné>
V cestě (inline)	
TAP, SPAN porty jen pro monitoring	
Mimo cestu (Out of path)	
Možnost zvolit mezi pouze „monitorováním“ a „monitorováním a blokováním“	
Možnost definovat různá pravidla pro různé části sítě i různé uživatele	
Hardware	<prázdné>
Minimálně 4x 1Gbps rozhraní	
Minimálně 2x 1Gbps SFP rozhraní	
Dedikovaný ethernet management port	
Sériový port (RS-232)	

Propustnost zařízení při DDoS útoku, min. 2 Gbps	
Počet současně navázaných spojení, min. 2 mil	
Možnost licenčního navýšení výkonu propustnosti na 3 Gbps	
Latence, max. 60 microseconds	
Napájení systému – AC	
Možnost použití DC napájení	
Redundantní napájení	
Obnova systému ze záložního média	
Možnost nasazení páru zařízení (aktivní – záložní)	
Ochrana před přetížením	

1.4.14 ZABEZPEČENÍ FYZICKÉHO PŘÍSTUPU DO POČÍTAČOVÉ SÍTĚ

Požadovaná funkcionalita/vlastnost	**Doplní Uchazeč dle nabízeného řešení**
Výrobce komponent řešení	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Zavedení mechanismu pro identifikaci, autentizaci a autorizaci počítačů a uživatelů při přístupu ke KSI zadavatele prostřednictvím přístupových přepínačů (instalovaná báze je uvedena v popisu současného stavu v příloze č. 10)	
Zajištění autentizované konektivity u neinteraktivních zařízení (tiskárny, IP kamery apod.) připojených do KSI zadavatele prostřednictvím přístupových přepínačů	
Vazba řešení na stávající zdroje (databáze) informací o uživatelích a jejich právech (viz popis stávajícího stavu)	
Zajištění monitoringu všech úspěšných/neúspěšných pokusů o konektivitu do KSI zadavatele a efektivní řešení pro centrální management prostředí	
Pokročilý reporting v reálném čase – kdo, jakým zařízením, kdy a kam přistupuje / přistupoval do sítě	
Redundance navrženého řešení: řešení dimenzováno na počet obsluhovaných koncových stanic min. 15 000	
Škálovatelnost celého řešení z hlediska dalšího zvyšování redundance i z hlediska počtu obsluhovaných koncových zařízení	
Možnost nasazení pokročilejších technologií jako např. profiling zařízení (analýza a klasifikace zařízení podle různých atributů, např. podle výrobce, modelu, OS apod.)	
Možnost tzv. bezpečnostního auditu zařízení (tzv. posture assessment) a reakce na jednotlivé hrozby – kontrola zdravotního stavu zařízení	

Možnost upozornění uživatele nebo izolace nevyhovujícího zařízení (tzv. assisted remediation) z hlediska bezpečnostního auditu – možnost dočasného umístnění zařízení do karantény a jeho asistovaná náprava do akceptovatelného stavu	
Možnost zřizování a poskytování dočasného přístupu pro hosty – samoregistrace hostů nebo sponzorský schvalovací přístup	
Možnost integrace se systémy detekce útoků (pokud je detekována kompromitovaná stanice v síti, bude možné ji automaticky eliminovat na přístupové vrstvě)	
Možnost sdílení informací (uživatel, stanice, „compliance" apod.) se systémy detekce útoků a malware	
Navrhované řešení musí respektovat princip ochrany investic	
Obecná charakteristika ověřovacího řešení	<prázdné>
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.)	
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	
Poskytuje AAA funkce (viz níže)	
Podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control)	
Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování kapacity	
Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace	
Je dostupné ve formě Appliance (hardware i software podporovaný jedním výrobcem)	
Je dostupné ve formě virtuálního stroje na platformách ESX nebo ESXi	
AAA funkce (ověřování, autorizace a záznamy o průběhu připojování uživatelů a zařízení k síti)	<prázdné>
Podporované protokoly	<prázdné>
RADIUS pro autentizaci, autorizaci, zaznamenávání	
Proxy funkce pro externí RADIUS	
PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST	
Podporované databáze uživatelů (s možností definovat pořadí průchodu)	<prázdné>
Interní (pro uživatele i koncová zařízení)	
Active Directory	
LDAP (RFC 2251)	
RADIUS Token indentity source (RFC 2865)	
RSA RADIUS token server	
Certificate authentication profile	
Ověřování uživatelů a zařízení	<prázdné>
Ověření uživatelů heslem nebo certifikátem	
Ověření MAC adresou připojovaného zařízení	
Rozpoznávání typu koncových zařízení a jejich stavu	<prázdné>

Automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se síťovou infrastrukturou	
Předdefinované profily pro běžná mobilní zařízení (zařízení s OS Android, SymbianOS, Apple, Blackberry, HTC)	
Ověření stavu koncových zařízení pomocí softwarovéha agenta nebo web agenta na koncovém zařízení Systém musí rozpoznat: • instalovaný operační systém (Windows 7, Microsoft Windows Vista Business, Windows Vista Ultimate, Windows Vista Enterprise, Windows Vista Home, Windows XP (Professional, Home, Media Center Edition, Tablet PC), Windows 2000, Windows 98, Windows SE, and Windows ME; Mac OS X v10.5.x, v10.6.x) • opravy instalované v operačním systému • verze instalovaných programů • hodnoty položek v registry databázi systémů Windows • stav aplikací, zejména antivirů	
Autorizace: pružný systém pro definici pravidel pro přístup k síti	<prázdné>
Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle: • uživatele (role, skupiny) • stavu a typu koncového zařízení (viz výše) • místa připojení • historie připojení	
Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě	
Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě	
Podpora Change of Authorization (CoA, RFC 3576)	
Řízení přístupu i možným zapojením do trasy komunikace autorizovaných zařízení	
Podpora přidělení značek prvkům přístupové infrastruktury podle klientské identity/skupiny, pro škálovatelné filtrování přístupů	
Možnost jednoduše identifikovat/označit přenášená data uživatele (rámce) v chráněné oblasti	
Řízení autentizace a založení důvěryhodné infrastruktury mezi jednotlivými prvky sítě, pro bezpečný a šifrovaný transport dat	
Spolupráce na uvedení stanic do požadovaného stavu (informací, odkazem, spuštěním programu, aktualizací antiviru, aktualizací OS, stažením souboru)	
Accounting	<prázdné>
Zaznamenávání aktivity uživatelů a zařízení připojených k síti	
Dotazovací systém, korelace záznamů, centralizované výkazy	
Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů)	
Funkce GUEST serveru	<prázdné>
Vytváření casově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i ve WiFi	
Oprávnění přidělovaná správcem přístupu přes portál pro snadné vytváření dočasných účtů	
Samoobslužný portál pro uživatele	
Ověření přes HTTP a HTTPS	

Podpora BYOD	<prázdné>
Onboarding (registrace, provisioning, nastavení klientských zařízení)	
Onboarding/provisioning proces formou samoobsluhy	
Specifické politiky pro BYOD zařízení	
Možnost nastavení limitu BYOD zařízení pro jednoho uživatele	
Podpora MDM	<prázdné>
Podpora workflow pro registrace do MDM	
Podpora výměny informací z MDM platformy a využití v politikách (např. pokud je zařízení „compliant“)	
Ovládání MDM přímo z prostředků bezpečnostního managementu zařízení (zamykání, mazání apod.)	
Uživatelská samoobsluha přes web portál (např. zamknutí přístupu pro ztracené zařízení)	
Další vlastnosti	
Aktivace šifrování MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují)	
Funkce pro správu ověřovacího systému	<prázdné>
Centralizovaná správa	
Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému	
Zjednodušení správy vytvářeními skupin uživatelů, koncových a síťových zařízení	
Grafické rozhraní pro definici pravidel přístupu k síti	
Grafické rozhraní pro monitorování, definici výkazů, řešení problémů	
Diagnostika problemů (systémová, údaje o chybách přihlašování, TCP dump, packet capture)	
Zaznamenávání událostí na externí syslog server	
Podpora SNMPv3	
NTP pro synchronizaci času	
SMTP pro zasílání zpráv a výstrah přes e-mail	

1.4.15 NASAZENÍ MOBILE DEVICE MANAGEMENT (MDM)

Požadovaná funkcionalita/vlastnost	Doplní Uchazeč dle nabízeného řešení
Výrobce systému	
Odkaz na www stránky výrobce systému, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
Řešení musí pokrýt 500 uživatelů s možností budoucího rozšíření	
Podpora operačních systémů IOS, Android a Windows Phone	
Vynucování síly použitých hesel v aplikacích třetích stran, například při vstupu do zařízení	
Možnost po nějaké době neaktivity zařízení zamknout	
Vzdálené vymazání dat	
Vzdálené zamykání účtu/blokování zařízení	
Vynucování bezpečnostních politik	

Pravidelné spuštění aktualizace softwaru	
Omezení využití dalších zařízení typu externí paměti apod.	
Systém centralizované distribuce SW	
Zabezpečení datového obsahu (jedná se pouze o data uložená v zařízení)	
Možnost integrace s Active Directory (ověření uživatelů)	
Možnost integrace s Microsoft Exchange (integrace pošty)	
Podpora Cloud i „On-premises“, centrálního managementu	
Centrální management a vyrozumívání celého řešení	

1.4.16 BEZPEČNOSTNÍ STANDARDY SI

Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Nabízené řešení (projekt) splňuje všechny požadavky uvedené v příslušné kapitole v příloze č. 6 (kapitola 5)	

1.4.17 KONSOLIDACE AVO PRO STANICE A SERVERY

Požadovaná funkcionalita/vlastnost	**Doplní Uchazeč dle nabízeného řešení**
Výrobce systému	
Odkaz na www stránky výrobce systému, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	

Požadovaná funkcionalita/vlastnost	**Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE**
Pro stanice	
Ochrana proti známým virům a malwaru minimálně na základě signatur	
Ochrana na úrovni síťové komunikace (tj. zamezení průniku škodlivého kódu do pracovní stanice a serverů již na úrovni síťové vrstvy)	
Centrální správu AVO systému s pokročilou možností reportů a statistik a instalace klientů	
Možnost napojení na požadovaný SIEM nástroj standardizovanými protokoly (např. SYSLOG, SNMP)	
Aktualizace z internetu anebo z centrálního uzlu umístěného v síti zadavatele, který při hromadné aktualizaci klientů šetří přenosové pásmo do internetu	
Podpora MS Windows 7, 8, 8.1	
Pro servery	
Ochranu proti rootkit hrozbám, známým virům a malwaru	
Vyhodnocování hrozeb na základě tzv. reputace – tj. aktivní ochrana, která vychází z celosvětové důvěryhodnosti používaných souborů, a která je proto nezávislá na aktuálnosti virových definic	
Centrální správu AVO systému z jedné administrátorské konzole s pokročilou možností reportů a statistik	
Možnost napojení na požadovaný SIEM nástroj standardizovanými	

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje/nesplňuje požadavek (doplní Uchazeč) ANO/NE
protokoly (např. SYSLOG, SNMP)	
Jediný agent na koncovém zařízení, který řídí všechny požadované funkcionality	
Aktualizace z internetu anebo z centrálního uzlu umístěného v síti MPSV, který při hromadné aktualizaci klientů šetří přenosové pásmo do internetu	
Řešení musí podporovat následující platformy OS serverů: MS Windows Server 2008, 2008R2, 2012, 2012R2	