# Technická specifikace

## Požadovaný budoucí stav

V rámci předmětu plnění bude obnoven centrální přepínač v lokalitě Žerotínovo náměstí a lokalitě Cejl. V obou lokalitách bude vybudován nový centrální přepínač ve vysoké dostupnosti, zabezpečující připojení přístupových přepínačů sítě Jihomoravského kraje a serverů Jihomoravského kraje. Obě lokality budou propojeny minimálně rychlostí 100Gbps ve vysoké dostupnosti. Lokality mohou být propojeny přes L3 konektivitu s podporou VXLAN pro serverovou infrastrukturu nebo přes L2 konektivitu s distribuovanou defaultní bránou pro serverovou infrastrukturu i přístupovou vrstvu sítě.

Přístupové přepínače Jihomoravského kraje a servery musí být připojeny redundantně k centrálním přepínačům v dané lokalitě. Centrální přepínače musí nabízet připojení pomocí linkové agregace přes oba centrální přepínače v dané lokalitě.

Součástí obnovy je implementace segmentačních firewallů, které zabezpečí bezpečnou a řízenou komunikaci mezi jednotlivými vrstvami datového centra, přístupovými sítěmi Jihomoravského kraje a mezi přístupovými sítěmi a sítěmi datového centra.

Autentizační server (NAC) bude implementován pro zabezpečený přístup do drátové i bezdrátové sítě Jihomoravského kraje a musí být integrován se stávající databází uživatelů Active Directory. Autentizační server musí zabezpečit i centralizovanou autentizaci administrátorů k aktivním prvků v síti.

Centrální dohled a management musí podporovat všechny zadavatelem provozované aktivní prvky a umožňovat dohled a správu z jednotného prostředí.

## Popis současného stavu

Zadavatel provozuje 67 přístupových switchů Aruba 6200F na dvou hlavních lokalitách a 95 Access Point Aruba 500.

## Potvrzení o pětileté záruce

Součástí předávacích protokolů bude písemné potvrzení od výrobce dodávaných technologií, že na předmět plnění byla u výrobce zakoupena minimálně 5letá rozšířená záruka výrobce s dobou opravy/výměny následující pracovní den s možností hlásit závadu 8 hodin denně v pracovní dny (označovaná zpravidla jako 8x5xNBD) platná od data zahájení implementace. Tato záruka musí být poskytována na místě instalace pracovníky výrobce nebo dodavatele.

## Potvrzení o určení zboží pro koncového zákazníka

V databázi výrobce dodávaných technologií musí být zadavatel veden jako první uživatel dodávaného zboží a souvisejících licencí/subskripcí/operačních systémů. Zadavatel požaduje originální a nová zařízení určená pro evropský trh. Před převzetím zboží si zadavatel vyhrazuje právo kontroly dle sériových čísel u výrobce. Pokud v databázi výrobce bude uveden jiný koncový uživatel než zadavatel, bude se jednat o porušení podmínky originálního a nového zařízení. Za účelem ověření těchto parametrů vybraný dodavatel na vyžádání před dodáním zboží předloží prohlášení výrobce dodávaného zařízení či jeho oficiálního zastoupení o tom, že na dodávané zboží zadavateli jako koncovému zákazníkovi bude poskytnuta k dodávanému zařízení záruka výrobce v plném výrobcem poskytovaném rozsahu.

## Minimální požadavky na záruku a služby

Na všechny části dodávané síťové infrastruktury je vyžadována záruka a záruční servisní podpora následujícího rozsahu (pokud není u konkrétního prvku uvedeno jinak):

*Účastník pro účely podání nabídky vyplní příslušnou tabulku, a to, zda splňuje požadované parametry a popis splnění požadavku (nesplnění některého z parametrů představuje nesplnění zadávacích podmínek).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Požadované parametry** | **Splňuje ANO/NE** | **Popis splnění požadavku** |
| 1 | Záruka a záruční podpora výrobce v úrovni 8x5xNBD - Exchange Minimálně 5 let |  |  |
| 2 | Součástí záruky musí být přímý přístup zadavatele k technické podpoře výrobce zařízení - Minimálně 5 let |  |  |
| 3 | Přístup k bezpečnostním opravám SW a HW po dobu životnosti dodaných prvků – Minimálně 5 let. |  |  |
| 4 | Přístup k aktualizaci software a firmware pro dodané prvky po dobu životnosti dodaných prvků – Minimálně 5 let. |  |  |

## Minimální technické požadavky

### Centrální přepínač – 4 kusy

*Účastník pro účely podání nabídky vyplní příslušné tabulky, a to, zda splňuje požadované parametry a popis splnění požadavku (nesplnění některého z parametrů představuje nesplnění zadávacích podmínek).*

1. **2 ks centrální přepínač Žerotínovo náměstí**

**Každý v konfiguraci:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje ANO/NE** | **Popis splnění požadavku** |
| **Základní vlastnosti** |  |  |  |
| Třída zařízení: L3 switch | ano |  |  |
| Formát zařízení: modulární chassis | ano |  |  |
| Počet slotů pro linkové karty | 5 |  |  |
| Maximální velikost zařízení: 7U | ano |  |  |
| Počet optických 100GE portů | 20x 100GbE QSFP28 |  |  |
| Počet optických 1/10/25GE portů s volitelným fyzickým rozhraním | 64x 1/10/25Gbit/s SFP28 |  |  |
| Interní hot-swap AC napájecí zdroje v redundantní konfiguraci | ano, minimálně s redundancí N+1 |  |  |
| Možnost rozšíření o zdroj s vyšším výkonem pro PoE | ano |  |  |
| Možnost osazení karet s podporou Class 4 a Class 6 PoE | ano |  |  |
| Možnost osazení dalších karet s podporou 40 a 100GE interface | ano |  |  |
| Celková propustnost chassis | 14 Tbit/s |  |  |
| Celkový paketový výkon přepínače | 10 Bpps |  |  |
| Paketový buffer | min. 8 MB per linková karta |  |  |
| Po osazení linkovými kartami s požadovaným počtem portů viz výše musí zůstat min. 2 volné pozice pro rozšíření o další 2 linkové karty v budoucnu | ano |  |  |
| **Vysoká dostupnost** |  |  |  |
| Možnost osadit v budoucnu redundantní management modul | ano |  |  |
| Podpora virtualizace funkcí dvou přepínačů - dvojice se chová jako jedno zařízení pro funkce linkové agregace a L3 výchozí brány | ano |  |  |
| Zařízení v rámci virtualizovaného páru si zachovávají vlastní control plane | ano |  |  |
| Virtualizace dvou přepínačů je prováděna přes standardní ethernet porty | ano |  |  |
| Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG) | ano |  |  |
| Minimální počet seskupení portů napříč různými chassis | 256 |  |  |
| **Základní funkce a protokoly** |  |  |  |
| Podpora "jumbo rámců" včetně velikosti 9198 Byte | ano |  |  |
| Podpora linkové agregace IEEE 802.1AX | ano |  |  |
| Konfigurovatelné rozkládání LACP zátěže podle L2,L3 | ano |  |  |
| Počet LACP skupin/linek ve skupině | 256/8 |  |  |
| Počet záznamů v tabulce MAC adres | 29 000 |  |  |
| Počet záznamů v tabulce ARP | 28 000 |  |  |
| Protokol pro definici šířených VLAN | MVRP |  |  |
| Podpora VLAN podle IEEE 802.1Q, minimálně 4000 aktivních VLAN | ano |  |  |
| VLAN translace - swap 802.1Q tagů na trunk portu | ano |  |  |
| Podpora zařazování do VLAN podle standardu 802.1v | ano |  |  |
| IEEE 802.1s - Multiple Spanning Tree | ano |  |  |
| STP instance per VLAN s 802.1Q tagováním BPDU | ano |  |  |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED | ano |  |  |
| Detekce jednosměrnosti optické linky | ano |  |  |
| DHCP server | ano |  |  |
| DHCP relay pro IPv4 a IPv6 | ano |  |  |
| Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace | ano |  |  |
| Statické směrování IPv4 a IPv6 | ano |  |  |
| Počet záznamů ve směrovací tabulce | 64 000 |  |  |
| Dynamické směrování OSPFv2, OSPFv3 a BGP včetně podpory BFD | ano |  |  |
| Podpora BGP a MP-BGP včetně podpory BFD | ano |  |  |
| Podpora Layer-3 routed port | ano |  |  |
| IGMP v2 a v3 | ano |  |  |
| MLD v1 a v2 | ano |  |  |
| Hardware podpora IPv4 a IPv6 ACL | ano |  |  |
| ACL definice na základě skupiny fyzických portů | ano |  |  |
| ACL aplikovatelný na interface, LAG, VLAN | ano |  |  |
| BPDU a Root guard | ano |  |  |
| DHCP snooping pro IPv4 a IPv6 | ano |  |  |
| HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps | ano |  |  |
| 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port | ano |  |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) | ano |  |  |
| Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675 | ano |  |  |
| Podpora Critical VLAN | ano |  |  |
| Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely. | ano |  |  |
| Uživatelské role mohou být lokálně definované v přepínači nebo mohou být dynamicky stáhnuty z RADIUS serveru na základě výsledku autorizace. | ano |  |  |
| Podpora IPv6 RA Guard | ano |  |  |
| IP source guard / dynamic IP lockdown | ano |  |  |
| Podpora Dynamic ARP protection | ano |  |  |
| Port security | ano |  |  |
| Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU | ano |  |  |
| Podpora IPv4 a IPv6 QoS | ano |  |  |
| IEEE 802.1p - minimální počet front | 8 |  |  |
| **SDN funkce** |  |  |  |
| Podpora service insertion včetně technologie VXLAN | ano |  |  |
| Podpora BGP EVPN s využitím VXLAN | ano |  |  |
| Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izololovat více koncových zařízení na jednom portu do unikátních tunelů | ano |  |  |
| Přiřazení koncového zařízení do tunelu na základě výsledku autorizace | ano |  |  |
| **Analytické a automatizační nástroje** |  |  |  |
| Podpora REST API pro automatizaci nastavení sítě. | ano |  |  |
| Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači | ano |  |  |
| Integrovaný nástroj na odchyt paketů | ano |  |  |
| Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události | ano |  |  |
| Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů. Možnost vynášení stavu monitorovaných metrik do grafů atp. | ano |  |  |
| Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase. | ano |  |  |
| Interní úložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení | ano |  |  |
| Kapacita interního úložiště dat pro analytické účely | 30 GB |  |  |
| **Management** |  |  |  |
| USB-C konzolový port | ano |  |  |
| 1xRJ45 OoB management port s podporou ethernetu | ano |  |  |
| Podpora minimálně 64 virtuálních směrovacích instancí (VRF) | ano |  |  |
| Minimální počet VRF instancí | 64 |  |  |
| Konfigurace zařízení v člověku čitelné textové formě | ano |  |  |
| Podpora automatických i manuálních snapshotů konfigurace systému | ano |  |  |
| USB port pro diagnostiku, přenos konfigurace a firmware | ano |  |  |
| Přímé bezdrátové připojení ke konzoli zařízení skrze bluetooth | ano |  |  |
| Podpora managementu přes IPv4 i IPv6 | ano |  |  |
| SSHv2 a HTTPS pro IPv4 a IPv6 | ano |  |  |
| Podpora SNMPv2c a SNMPv3 | ano |  |  |
| RMON | ano |  |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ano |  |  |
| Lokálně vynucené RBAC na úrovni přepínače | ano |  |  |
| Dualní flash image | ano |  |  |
| Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů | ano |  |  |
| Podpora RADIUS včetně RADIUS CoA (RFC3576) | ano |  |  |
| Podpora TACACS+ | ano |  |  |
| Analýza síťového provozu sFlow podle RFC 3176 | ano |  |  |
| Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN | ano |  |  |
| Podpora IP SLA pro měření zpoždění provozu VoIP | ano |  |  |
| Podpora Zero Touch Provisioning (ZTP) | ano |  |  |

1. **2 ks switch Cejl**

**Identický model jako switch v lokalitě Žerotínovo náměstí.**

**Každý v konfiguraci:**

*Účastník pro účely podání nabídky vyplní příslušné tabulky, a to, zda splňuje požadované parametry a popis splnění požadavku (nesplnění některého z parametrů představuje nesplnění zadávacích podmínek).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje ANO/NE** | **Popis splnění požadavku** |
| **Základní vlastnosti** |  |  |  |
| Třída zařízení: L3 switch | ano |  |  |
| Formát zařízení: modulární chassis | ano |  |  |
| Počet slotů pro linkové karty | 5 |  |  |
| Maximální velikost zařízení: 7U | ano |  |  |
| Počet optických 100GE portů | 16x 100GbE QSFP28 |  |  |
| Počet optických 1/10/25GE portů s volitelným fyzickým rozhraním | 32x 1/10/25Gbit/s SFP28 |  |  |
| Interní hot-swap AC napájecí zdroje v redundantní konfiguraci | ano, minimálně s redundancí N+1 |  |  |
| Možnost rozšíření o zdroj s vyšším výkonem pro PoE | ano |  |  |
| Možnost osazení karet s podporou Class 4 a Class 6 PoE | ano |  |  |
| Možnost osazení dalších karet s podporou 40 a 100GE interface | ano |  |  |
| Celková propustnost chassis | 14 Tbit/s |  |  |
| Celkový paketový výkon přepínače | 10 Bpps |  |  |
| Paketový buffer | 8 MB per linková |  |  |
| Po osazení linkovými kartami s požadovaným počtem portů viz výše musí zůstat min. 3 volné pozice pro rozšíření o další 3 linkové karty v budoucnu | ano |  |  |
| **Vysoká dostupnost** |  |  |  |
| Možnost osadit v budoucnu redundantní management modul | ano |  |  |
| Podpora virtualizace funkcí dvou přepínačů - dvojice se chová jako jedno zařízení pro funkce linkové agregace a L3 výchozí brány | ano |  |  |
| Zařízení v rámci virtualizovaného páru si zachovávají vlastní control plane | ano |  |  |
| Virtualizace dvou přepínačů je prováděna přes standardní ethernet porty | ano |  |  |
| Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG) | ano |  |  |
| Minimální počet seskupení portů napříč různými chassis | 256 |  |  |
| **Základní funkce a protokoly** |  |  |  |
| Podpora "jumbo rámců" včetně velikosti 9198 Byte | ano |  |  |
| Podpora linkové agregace IEEE 802.1AX | ano |  |  |
| Konfigurovatelné rozkládání LACP zátěže podle L2,L3 | ano |  |  |
| Počet LACP skupin/linek ve skupině | 256/8 |  |  |
| Počet záznamů v tabulce MAC adres | 29 000 |  |  |
| Počet záznamů v tabulce ARP | 28 000 |  |  |
| Protokol pro definici šířených VLAN | MVRP |  |  |
| Podpora VLAN podle IEEE 802.1Q, minimálně 4000 aktivních VLAN | ano |  |  |
| VLAN translace - swap 802.1Q tagů na trunk portu | ano |  |  |
| Podpora zařazování do VLAN podle standardu 802.1v | ano |  |  |
| IEEE 802.1s - Multiple Spanning Tree | ano |  |  |
| STP instance per VLAN s 802.1Q tagováním BPDU | ano |  |  |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED | ano |  |  |
| Detekce jednosměrnosti optické linky | ano |  |  |
| DHCP server | ano |  |  |
| DHCP relay pro IPv4 a IPv6 | ano |  |  |
| Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace | ano |  |  |
| Statické směrování IPv4 a IPv6 | ano |  |  |
| Počet záznamů ve směrovací tabulce | 64 000 |  |  |
| Dynamické směrování OSPFv2, OSPFv3 a BGP včetně podpory BFD | ano |  |  |
| Podpora BGP a MP-BGP včetně podpory BFD | ano |  |  |
| Podpora Layer-3 routed port | ano |  |  |
| IGMP v2 a v3 | ano |  |  |
| MLD v1 a v2 | ano |  |  |
| Hardware podpora IPv4 a IPv6 ACL | ano |  |  |
| ACL definice na základě skupiny fyzických portů | ano |  |  |
| ACL aplikovatelný na interface, LAG, VLAN | ano |  |  |
| BPDU a Root guard | ano |  |  |
| DHCP snooping pro IPv4 a IPv6 | ano |  |  |
| HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps | ano |  |  |
| 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port | ano |  |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) | ano |  |  |
| Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675 | ano |  |  |
| Podpora Critical VLAN | ano |  |  |
| Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely. | ano |  |  |
| Uživatelské role mohou být lokálně definované v přepínači nebo mohou být dynamicky stáhnuty z RADIUS serveru na základě výsledku autorizace. | ano |  |  |
| Podpora IPv6 RA Guard | ano |  |  |
| IP source guard / dynamic IP lockdown | ano |  |  |
| Podpora Dynamic ARP protection | ano |  |  |
| Port security | ano |  |  |
| Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU | ano |  |  |
| Podpora IPv4 a IPv6 QoS | ano |  |  |
| IEEE 802.1p - minimální počet front | 8 |  |  |
| **SDN funkce** |  |  |  |
| Podpora service insertion včetně technologie VXLAN | ano |  |  |
| Podpora BGP EVPN s využitím VXLAN | ano |  |  |
| Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izololovat více koncových zařízení na jednom portu do unikátních tunelů | ano |  |  |
| Přiřazení koncového zařízení do tunelu na základě výsledku autorizace | ano |  |  |
| **Analytické a automatizační nástroje** |  |  |  |
| Podpora REST API pro automatizaci nastavení sítě. | ano |  |  |
| Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači | ano |  |  |
| Integrovaný nástroj na odchyt paketů | ano |  |  |
| Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události | ano |  |  |
| Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů. Možnost vynášení stavu monitorovaných metrik do grafů atp. | ano |  |  |
| Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase. | ano |  |  |
| Interní úložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení | ano |  |  |
| Kapacita interního úložiště dat pro analytické účely | 30 GB |  |  |
| **Management** |  |  |  |
| USB-C konzolový port | ano |  |  |
| 1xRJ45 OoB management port s podporou ethernetu | ano |  |  |
| Podpora minimálně 64 virtuálních směrovacích instancí (VRF) | ano |  |  |
| Minimální počet VRF instancí | 64 |  |  |
| Konfigurace zařízení v člověku čitelné textové formě | ano |  |  |
| Podpora automatických i manuálních snapshotů konfigurace systému | ano |  |  |
| USB port pro diagnostiku, přenos konfigurace a firmware | ano |  |  |
| Přímé bezdrátové připojení ke konzoli zařízení skrze bluetooth | ano |  |  |
| Podpora managementu přes IPv4 i IPv6 | ano |  |  |
| SSHv2 a HTTPS pro IPv4 a IPv6 | ano |  |  |
| Podpora SNMPv2c a SNMPv3 | ano |  |  |
| RMON | ano |  |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ano |  |  |
| Lokálně vynucené RBAC na úrovni přepínače | ano |  |  |
| Dualní flash image | ano |  |  |
| Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů | ano |  |  |
| Podpora RADIUS včetně RADIUS CoA (RFC3576) | ano |  |  |
| Podpora TACACS+ | ano |  |  |
| Analýza síťového provozu sFlow podle RFC 3176 | ano |  |  |
| Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN | ano |  |  |
| Podpora IP SLA pro měření zpoždění provozu VoIP | ano |  |  |
| Podpora Zero Touch Provisioning (ZTP) | ano |  |  |

### Napojení stávající infrastruktury

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Celkový počet kompatibilních modulů pro připojení stávající infrastruktury, plně kompatibilní se stávající infrastrukturou** | | | | |
| QSFP28 transceiver 100GBASE-LR4, SM, 10km určený pro osazení do dodávaných switchů, originální modul od výrobce switche (nestačí kompatibilní nebo alternativní) | 2x |  | |  |
| QSFP28 transceiver 100GBASE-LR4, SM, 10km určený pro osazení do dodávaných switchů | 6x | |  |  |
| QSFP28 aktivní optický kabel 100Gbps pro lokální propojení dvou aktiv. prvků přes QSFP28 sloty, DMI, 10m, určený pro osazení do dodávaných switchů | 8x | |  |  |
| Direct Attach Copper Cable 100Gbit QSFP28 to QSFP28 v délce 5m, určený pro připojení serverů (síťové karty 100GbE ) a dodávaných switchů, originální modul od výrobce switche (nestačí kompatibilní nebo alternativní) | 12x | |  |  |
| SFP+ transceiver 10GBASE-LR/LW, SM 10km, 1310nm, LC Duplex, DMI, určený pro osazení do dodávaných switchů a osazení stávajících switchů accessové vrstvy (Aruba CX 6200), originální modul od výrobce switche (nestačí kompatibilní nebo alternativní) | 4x | |  |  |
| SFP+ transceiver 10GBASE-LR/LW, SM 10km, 1310nm, LC Duplex, DMI, určený pro osazení do dodávaných switchů a osazení stávajících switchů accessové vrstvy (Aruba CX 6200) | 248x | |  |  |
| SFP28 transceiver 10Gbps, MM, 850nm,100m (OM4), určený pro osazení do dodávaných switchů, originální modul od výrobce switche (nestačí kompatibilní nebo alternativní) | 2 | |  |  |
| SFP28 transceiver 10/25Gbps, MM, 850nm,100m (OM4), určený pro osazení do dodávaných switchů | 14x | |  |  |

### NAC server – 2 kusy

|  |  |  |  |
| --- | --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavek** | **Splňuje ANO/NE** | **Popis splnění požadavku** |
| **Základní funkce platformy** |  |  |  |
| Autentizační platforma (AAA) pro řízení přístupu uživatelů a zařízení do LAN a WiFi. | ano |  |  |
| On-premise appliance, nepřipouští se cloud řešení. | ano |  |  |
| Virtuální appliance bez nutnosti dodatečných licencí např. pro OS nebo database. | ano |  |  |
| Podporované hypervisory: VMware (.OVA formát), Hyper-V, KVM. | ano |  |  |
| Plná kompatibilita s infrastrukturou zadavatele, na které bude probíhat ověřování. | ano |  |  |
| Podpora 802.1X autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN. | ano |  |  |
| Podpora minimálně pro 1500 současně autentizovaných zařízení (pomocí 802.1X) přes oba servery (cluster) | ano |  |  |
| Možnost vytváření active-active clusterů. Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality a umožňovat navýšení počtu podporovaných uživatelů přidáním další instance. | ano |  |  |
| Podpora minimálně následujících autentizačních metod: PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, Tunnel Extensible Authentication Protocol (TEAP), MAC autentizace. | ano |  |  |
| Platforma musí umožňovat úplné oddělení autentizace a autorizace, např. autentizace proti službě Active Directory, ale autorizace proti externí SQL databázi. | ano |  |  |
| Autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, typ zařízení, osobní profil či členství ve skupině v Active Directory. | ano |  |  |
| Podpora dalších způsobů autentizace a autorizace. Minimálně: LDAP, MS AD, Token, MAC auth, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta). | ano |  |  |
| Podpora změny autorizačního stavu zařízení bez nutnosti změny definice autorizační politiky, např. pro odpojení nebo karanténu koncových zařízení. | ano |  |  |
| Podpora autorizace pomocí externího Cloud zdroje identity: Azure Active Directory. | ano |  |  |
| Podpora RADIUS CoA podle RFC3576 pro změnu autorizace ověřeného zařízení | ano |  |  |
| Podpora RadSec (RADIUS over TLS) a RadSec proxy pro IPv4 a IPv6 |  |  |  |
| Možnost autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. za účelem omezení celkového času online či objemu přenesených dat za delší časové období. | ano |  |  |
| Sběr dodatečných informací o připojených zařízeních (profilování) jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace lze využít pro doplňkové ověření přístupu zařízení do sítě. | ano |  |  |
| Sběr dodatečných informací o připojených IoT zařízeních (profilování), pomocí aktivních metod jako jsou: SNMP, WMI a NMAP scan. Tyto informace lze využít pro doplňkové ověření přístupu zařízení do sítě. | ano |  |  |
| Automatická identifikace a označení privátních (randomizovaných) MAC adres koncových zařízení. | ano |  |  |
| Platforma obsahuje funkci otestovaní autentizační politiky, včetně flexibilní volby typu autentizace, atributů klienta, atd. | ano |  |  |
| Podpora REST API pro většinu základních úkonů AAA platformy. Podpora REST volání vyvolaného autentizační či autorizační událostí (pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.). | ano |  |  |
| Zpracovávání SYSLOG hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení. | ano |  |  |
| Možnost vlastní tvorby parseru/integrace SYSLOG hlášení pro možnost uživatelské integrace s libovolnými systémy třetích stran. | ano |  |  |
| Podpora SYSLOG podle RFC 5424. | ano |  |  |
| Možnost registrace zařízení pomocí MAC adresy pro non-IT uživatele - omezená funkce administračního rozhraní, se zařazením zařízení do skupiny s definovanou politikou přístupu. | ano |  |  |
| Podpora TACACS+ autentizace správců síťových zařízení. | ano |  |  |
| Možnost integrace s MDM (Mobile Device Management) platformami třetích stran (minimálně AirWatch, Citrix, MobileIron, JAMF, inTune). | ano |  |  |
| Možnost rozšíření o nadstavbovou software komponentu pro koncové stanice jako trvalý či dočasný NAC agent, který zajišťuje ochranu formou posture assessments a health checks. NAC agent podporuje v návaznosti na autentizační proces kontrolu systémových procesů, aplikací, klíčů registru, použití USB zařízení, přítomnost anti-viru, firewallu. |  |  |  |
| **Funkce pro řízení přístupu hostů – LAN a WiFi Guest Captive portál** | | |  |
| Podpora HTTP a HTTPS web autentizace (Captive portál). | ano |  |  |
| Podpora CAPPORT - RFC 8908 | ano |  |  |
| Podpora autentizace hostů pomocí účtů sociálních sítí: Google, Google Plus, Facebook, Facebook WIFI, Twitter, LinkedIn, Microsoft. | ano |  |  |
| Podpora autentizace lokálními účty v rámci portálu, ověření pomocí jméno+heslo, autentizační kód. | ano |  |  |
| Možnost samoobslužné registrace hosta do sítě s SMS a email ověřením. | ano |  |  |
| Přístup zdarma pouze s akceptací podmínek užití. | ano |  |  |
| Tarify lze omezit časově, z hlediska rychlosti připojení či objemu přenesených dat. | ano |  |  |
| Vynucení odpojení zařízení ihned po naplnění jakéhokoliv z limitů. | ano |  |  |
| Perzistence autentizace/registrace s využitím MAC cache a zobrazení jen uvítacích stránek s osobním oslovením hosta při opakovaných návštěvách. Konfigurovatelné hodnoty trvání MAC cache pro různé hosty v rámci jedné služby (např. jedno SSID). | ano |  |  |
| Možnost vytváření účtů samoobslužnou registrací. | ano |  |  |
| Možnost provozovat více graficky i obsahově unikátních portálů v rámci jedné instalace. | ano |  |  |
| Redakční systém pro plnou grafickou a obsahovou úpravu jednotlivých captive portálů umožňuje:   * Úprava barev, fontů, pozadí a loga. * Úprava registračních formulářů – přidávání a odebírání polí pro vstupní data formuláře včetně validace vkládaného obsahu. * Možnost vkládání animací, videí a dalšího dynamického obsahu. * Vytváření specifických stránek pro různé typy zařízení a operačních systémů (např. pro efektivní navedení do specifického app store). | ano |  |  |
| **Management** |  |  |  |
| HTTPS rozhraní s podporou konfiguračních průvodců a před konfigurovaných šablon. | ano |  |  |
| Appliance podporuje šifrování disku nebo souborů. | ano |  |  |
| Appliance podporuje CLI přístup a umožňuje v něm konfiguraci základních nastavení. | ano |  |  |

### Centrální management

|  |  |  |  |
| --- | --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje ANO/NE** | **Popis splnění požadavku** |
| **Základní vlastnosti** |  |  |  |
| Centrální správu a monitoring všech dodaných přepínačů | ano |  |  |
| Public cloud nativní aplikace dodávána formou služby na minimálně 60 měsíců | ano |  |  |
| Plně kompatibilní s nabízenými aktivními prvky | ano |  |  |
| Licence pro správu všech dodávaných přepínačů | ano |  |  |
| Možnost flexibilního rozšiřování pomocí licencí minimálně až na 500 zařízení | ano |  |  |
| Podpora dohledu minimálně 10 000 klientů/uživatelů | ano |  |  |
| Vysoká dostupnost management nástroje – HA režim | ano |  |  |
| Definice společných konfiguračních elementů nad skupinou zařízení | ano |  |  |
| Hierarchická konfigurace nad skupinou a individuální konfigurace platná pro jednotlivá zařízení | ano |  |  |
| Konfiguračních audit – možnost porovnat rozdíly skupinová vs. individuální konfigurace zařízení | ano |  |  |
| Hromadná aktualizace firmware, možnost plánovaných upgrade pro pouze definovanou podmnožinu | ano |  |  |
| Grafický dashboard zobrazující aktuální a historické informace o připojených klientech | ano |  |  |
| Podpora hromadné změny více zařízení konfigurací pomocí šablon | ano |  |  |
| Komunikace s přepínači přes zabezpečené HTTPS rozhraní | ano |  |  |
| Minimální datová retence monitorovacích dat a statistik 90 dnů | ano |  |  |
| RESTful API pro možnost integrace s externími systémy a možnost vyčítat provozní statistiky | ano |  |  |
| Streaming API umožňující proaktivní zasílání změn stavů a statistik bez nutnosti pravidelného načítání statistik skrze pasivní REST API. | ano |  |  |
| Integrované diagnostické nástroje, které umožňují spouštět vzdáleně CLI příkazy | ano |  |  |
| Možnost rozdělení zařízení do skupin a hromadná konfigurace zařízení ve skupině | ano |  |  |
| Zobrazení stavu a konfigurace portů přepínače, zobrazení spotřeby PoE po jednotlivých portech, zobrazení stavu hardwaru (CPU, RAM, chlazení, teplota, napájecí zdroje) | ano |  |  |
| Zobrazení seznamu sousedních zařízení přepínače | ano |  |  |
| Možnost přímého přístupu do CLI daného zařízení z portálu centrální správy | ano |  |  |
| Automatické upozornění na aktualizaci firmwaru přepínače | ano |  |  |
| Real-time diagnostika událostí týkajících se konkrétního klienta – okamžité zobrazování stavů připojení, autentizace atp. bez nutnosti čekání na pravidelný update interval. | ano |  |  |
| Podpora automatizovaného strojového učení systému pro automatické odhalování konkrétních zařízení či skupin zařízení, které mají společné negativní projevy některého z monitorovaných parametrů. | ano |  |  |
| Monitorování síťových služeb jako je DNS, DHCP či RADIUS ověřování klientů, jejich chybovost a zpoždění. | ano |  |  |
| Reportovací modul pro vytváření souhrnných reportů z dat za poslední období. Minimálně tyto reporty: PCI, bezpečnostní report, kapacitní plánování sítě, Klient inventory, využití sítě klienty | ano |  |  |
| Dohled přepínačů, zobrazení událostí a alertů | ano |  |  |
| Nástroje pro ověření konektivity přepínače spouštěné přímo z management nástroje (ping, traceroute) | ano |  |  |
| Možnost definování seznamu příkazů pro diagnostiku problémů a jejich hromadné spuštění | ano |  |  |
| Export výsledků diagnostických příkazů, možnost odeslání na Email | ano |  |  |
| **Řízení přístupu do administrace a provisioning prvků** |  |  |  |
| Záznam příkazů zadávaných/odesílaných na aktivní prvek, včetně uživatele který je zadával (Audit) | ano |  |  |
| Podpora různých uživatelských rolí, možnost definice oprávnění pouze ke skupinám zařízení | ano |  |  |
| Administrace do centrální správy s podporou dvoufaktorové autentizace | ano |  |  |
| Instalační a monitorovací aplikace dostupná pro Android a IOS. Umožňuje naskenovat a přidat zařízení pod centrální správu. Dále umožňuje monitorovat stav zařízení a připojených klientů včetně objemu přeneseného provozu. | ano |  |  |
| Provisioning přepínačů do centrální správy probíhá automaticky po registraci zakoupených zařízení do nástroje centrální správy (vyplnění identifikačních údajů zařízení) | ano |  |  |
| Možnost přiřazení detailních práv pro jednotlivé administrátory řešení minimálně s rozlišením úrovní čtení, zápisu a úplného zamezení přístupu pro jednotlivé moduly řešení (správa a hierarchie zařízení, správa sítí, monitoring sítí) | ano |  |  |