# 4 Doplnění přístupových přepínačů

Hlavními cíli opatření je zajištění náhrady zastaralých a výrobcem nepodporovaných přístupových Cisco přepínačů. Je zde snahou zajistit co nevyšší dostupnost VIS při případných pokusech zneužití bezpečnostních zranitelností přepínačů. A to dle §26 (Nástroje pro zajištění vysoké úrovně dostupnosti) prováděcí vyhlášky zákona 316/2014 Sb. Obdobnou problematiku řeší vytvoření redundantních datových spojů mezi přístupovými a páteřními přepínači.

Dále je snahou zajistit identickou bezpečnostní politiku skrz celou síťovou infrastrukturu. Využít, technicky a odborně pak rozšířit stávající bezpečnosti řešené pomocí IEEE 802.1x (Cisco ISE) přes celou síť a to z pohledu autentizace a autorizace při přístupu do LAN, včetně přiřazování příslušných VLAN uživateli/zařízení a tím řídit integritu sítě. Zde dojde k naplnění §17 (Nástroj pro ochranu integrity komunikačních sítí), §18 (Nástroj pro ověřování identity uživatelů), §19 (Nástroj pro řízení přístupových oprávnění), prováděcí vyhlášky zákona 316/2014 Sb.

Při aplikaci zasílání informací o datovém provozu do centrálních NetFlow kolektorů a jeho vyhodnocení z pohledu KBU dojde k realizaci §22 (Nástroj pro detekci kybernetických bezpečnostních událostí) prováděcí vyhlášky zákona 316/2014 Sb.

Obměna přepínačů na Interní informace datovém spoji Interní informace, které budou veškerou komunikaci šifrovat pomocí technologie MAC SEC, zajistí v této části sítě soulad §17 (Nástroj pro ochranu integrity komunikačních sítí) a §25 (Kryptografické prostředky) prováděcí vyhlášky zákona 316/2014 Sb.

## Společné vlastnosti přístupových přepínačů

Všechny doplňované přepínače musí splňovat níže uvedené parametry:

* **Plná funkcionalita 802.1x** – Umožní jednotné ověřování uživatelů do sítě na všech přístupových přepínačích. Přepínače musí splňovat i pokročilé funkce v rámci 802.1x protokolu jako jsou například Guest VLAN, Fail VLAN, Critical VLAN, ověření MAC adresou, CoA, přiřazení ACL na port na základě ověření, apod.. Je vyžadována plná podpora stávajícího řešení Cisco ISE.
* **First Hop Security pro IPv4 a IPv6** – Rozšiřující zabezpečení sítě, které zamezí možným útokům na podvržení DHCP serveru, ARP zpráv, či IP adres u IPv4 a Router Advertisementů, Neighbor Discovery protokolu, IP adresy či DHCP u IPv6.
* **Plnohodnotné (nesamplované) NetFlow** – Tato funkcionalita umožňuje detailní sledování datových toků procházejících přes kterýkoliv port, kteréhokoliv přepínače. Informace o datových tocích budou sledovány centralizovaným nástrojem a on-line vyhodnocovány pro okamžité odhalení možných bezpečnostních hrozeb
* **Stohování přepínačů** – Přepínače musí podporovat funkcionalitu stohování, tedy propojení několika fyzických prvků do jednoho logického celku. Celý logický přepínač je pak spravován jako jedno zařízení. Zároveň musí být k dispozici funkce agregace linek pomocí protokolu LACP přes rozdílné prvky stohu. Například tak, aby ve stohu o 4 prvcích bylo možné pomocí LACP sdružit jeden port z každého prvku. Důvodem tohoto požadavku je vysoká dostupnost sítě v případě selhání dílčího komponentu (jedna z linek mezi páteřním prvkem a přístupovým stohem, jeden prvek v přístupovém stohu, jeden z centrálních prvků, …)
* **Dynamický routing** – Dynamický routing umožní efektivní segmentaci sítě do menších bloků při zachování konfigurační jednoduchosti (není třeba nastavovat velké množství statických cest na všech přepínačích) a aktivní reakce na změny v síti. Z hlediska dynamického routingu je požadován protokol OSPF, který je otevřeným stadardem.
* **Servisní podpora** – Zadavatel požaduje servisní podporu v českém jazyce.
* **Operační systémy zařízení** – Zadavatel požaduje dodání všech zařízení se stejným operačním systémem a stejným chováním z hlediska funkce a konfigurace.

Kromě těchto parametrů jsou požadovány další funkcionality, které jsou detailně rozepsány v následujících sekcích u jednotlivých modelů přístupových přepínačů.

## Doplnění licencí TACACS pro stávající technologii Cisco ISE

|  |  |  |
| --- | --- | --- |
| *Požadavek na funkcionalitu* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| **Licence ISE** |  |  |
| Licence TACACS pro ISE pro dvojici stávajících ISE serverů | ANO |  |

## Přístupový přepínač – 24 portů

Parametry specifikované v úvodní kapitole a parametry v následující tabulce definují minimální požadavky zadavatele na dodávané zařízení. Specifikace vychází ze současného stavu sítě zadavatele, studie proveditelnosti „Bezpečnost komunikační infrastruktury“ a předpokládaných změn a rozšíření v síti zadavatele na následujících cca 6 let.

| *Požadavek na funkcionalitu* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| --- | --- | --- |
| **Počet kusů** | **4** |  |
| **Základní vlastnosti** |  |  |
| Třída zařízení | L2-L3 switch |  |
| Typ chlazení | aktivní |  |
| Možnost montáže do racku | ANO |  |
| Sada pro montáž do racku součástí dodávky | ANO |  |
| Max. rozměry (v x š x h) [cm] | 4.5x44.5x45 |  |
| Počet portů 10/100/1000 RJ45 | 24 |  |
| Počet portů 10 Gbit/s a jejich typ | 2 SFP+ |  |
| PoE IEEE 802.3af. 802.3at | ANO |  |
| Dostupný výkon pro napájení portů | 370W |  |
| Wirespeed (neblokující) na všech portech | ANO |  |
| Možnost připojit externí redundantní napájecí zdroj | ANO |  |
| **Výkonnostní parametry** |  |  |
| Minimální propustnost L2/L3 přepínacího systému | 210 Gbit/s |  |
| Minimální paketový výkon přepínače | 95 Mp/s |  |
| Minimální počet MAC adres | 16000 |  |
| **Vlastnosti stohování** |  |  |
| Stohování bez snížení počtu požadovaných ethernetových portů | ano |  |
| Kompletní příslušenství pro stohování součástí (kabely, atd.) | ANO |  |
| Možnost agregace do počtu prvků | 8 |  |
| Propustnost stohovacího propoje | 80 Gbit/s |  |
| Všechna zařízení ve virtuálním celku se podílí na forwardingu paketů (distribuovaný switching) | ANO |  |
| Virtuální zařízení se ve všech ohledech chová jako jeden síťový prvek | ANO |  |
| Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením | ANO |  |
| Seskupení portů (IEEE 802.3ad) mezi různými prvky stohu | ANO |  |
| Kterýkoli prvek ve stohu může být řídícím prvkem stohu (1:N redundance) | ANO |  |
| Bezvýpadkové přepnutí na záložní řídící prvek | ANO |  |
| **Protokoly fyzické vrstvy** |  |  |
| IEEE 802.3-2005 | ANO |  |
| Podpora "jumbo rámců" | 9200 Bytes |  |
| **Protokoly 2. vrstvy** |  |  |
| IEEE 802.3ad (LACP) | ANO |  |
| Minimální počet LACP skupin | 24 |  |
| Počet aktivních linek v jedné LACP skupině | 8 |  |
| IEEE 802.1Q | ANO |  |
| Minimální počet aktivních VLAN | 1000 |  |
| IEEE 802.3az | ANO |  |
| HW připravený na nasazení IEEE 802.1ae | ANO |  |
| IEEE 802.1s - Multiple spanning tree | ANO |  |
| IEEE 802.1w - Rapid spanning Tree | ANO |  |
| IEEE 802.1p | ANO |  |
| STP instance per VLAN s 802.1Q tagováním BPDU, minimální počet podporovaných STP instancí = 128 | ANO |  |
| Kompatibilita s CDP | ANO |  |
| Detekce připojených zařízení pomocí LLDP a LLDP-MED | ANO |  |
| Detekce jednosměrnosti optické linky (např. UDLD) | ANO |  |
| STP root guard | ANO |  |
| STP loop guard | ANO |  |
| Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard) | ANO |  |
| Multicast/broadcast storm control - hardwarové omezení datového toku unicast/multicast rámců na portu v procentech | ANO |  |
| **Protokoly 3. vrstvy** |  |  |
| IPv4 a IPv6 statické směrování | ANO |  |
| OSPFv2 | ANO |  |
| OSPFv3 | ANO |  |
| IPv4 a IPv6 QoS | ANO |  |
| Hardware podpora IPv4 a IPv6 ACL | ANO |  |
| Policy based routing (PBR) pro IPv4 a IPv6 | ANO |  |
| **Multicast** |  |  |
| IGMP Snooping v1/v2/v3 | ANO |  |
| MLD snooping v1/v2 | ANO |  |
| IPv4 a IPv6 multicast VLAN | ANO |  |
| PIM DM, SM, SSM | ANO |  |
| **Bezpečnost** |  |  |
| DHCP snooping | ANO |  |
| Dynamic ARP inspection (DAI) | ANO |  |
| Verifikace mapování IP-MAC (např. IP source guard) | ANO |  |
| IPv6 First Hop Security RA guard | ANO |  |
| IPv6 First Hop Security DHCPv6 guard | ANO |  |
| IPv6 First Hop Security IPv6 SourceGuard | ANO |  |
| IPv6 First Hop Security IPv6 Binding Integrity Guard | ANO |  |
| Definování povolených MAC adres a počtu MAC adres na interface | ANO |  |
| Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy) | ANO |  |
| Ověřování 802.1X - minimálně 1024 ověřených uživatelů na systém | ANO |  |
| Ověřování MAC adres | ANO |  |
| Zařazování do VLAN a přidělení přístupových filtrů na základě 802.1X ověření | ANO |  |
| Zařazování do VLAN a přidělení přístupových filtrů na základě MAC-autentizace | ANO |  |
| Ověřování přístupu do sítě s podporou odlišných Guest VLAN (nedojde k pokusu o přihlášení), Fail VLAN (přihlášení selže) a Critical VLAN (nedostupnost RADIUS serveru) | ANO |  |
| IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu | ANO |  |
| Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x) | ANO |  |
| NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955) | ANO |  |
| Sběr dat pro NetFlow nebo IPFIX z každého portu přepínače | ANO |  |
| Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů | ANO |  |
| Statistiky určovány z každého paketu daného "flow" | ANO |  |
| Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb | ANO |  |
| Návaznost skriptů interpretovaných přepínačem po detekci daných parametrů "flow" | ANO |  |
| Zobrazení sbíraných infromací o "flow" přímo v přepínači včetně "TopN" pohledu. | ANO |  |
| Export statistik "flow" selektivně na více kolektorů | ANO |  |
| **Management** |  |  |
| CLI rozhraní | ANO |  |
| SSHv2 | ANO |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ANO |  |
| SNMPv2c | ANO |  |
| SNMPv3 | ANO |  |
| Sériová nebo USB konzolová linka | ANO |  |
| AAA ověřování uživatelů (autentizace, autorizace, accounting) -RADIUS, TACACS+ | ANO |  |
| Port mirroring | ANO |  |
| VLAN mirroring | ANO |  |
| Vzdálený mirroring (RSPAN) | ANO |  |
| Více monitorujících portů současně | ANO |  |
| Měření zakončení a délky metalického kabelu (TDR) | ANO |  |
| Podpora uživatelsky modifikovatelné automatické reakce/obsluhy událostí při provozu přepínače (pomocí skriptů) | ANO |  |
| Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute) | ANO |  |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |  |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů | ANO |  |
| NTP | ANO |  |
| DHCP server | ANO |  |

## Přístupový přepínač – 48 portů

Parametry specifikované v úvodní kapitole a parametry v následující tabulce definují minimální požadavky zadavatele na dodávané zařízení. Specifikace vychází ze současného stavu sítě zadavatele, studie proveditelnosti „Bezpečnost komunikační infrastruktury“ a předpokládaných změn a rozšíření v síti zadavatele na následujících cca 6 let.

|  |  |  |
| --- | --- | --- |
| *Požadavek na funkcionalitu* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| **Počet kusů** | **20** |  |
| **Základní vlastnosti** |  |  |
| Třída zařízení | L2-L3 switch |  |
| Typ chlazení | aktivní |  |
| Možnost montáže do racku | ANO |  |
| Sada pro montáž do racku součástí dodávky | ANO |  |
| Max. rozměry (v x š x h) [cm] | 4.5x44.5x45 |  |
| Počet portů 10/100/1000 RJ45 | 48 |  |
| Počet portů 10 Gbit/s a jejich typ | 2 SFP+ |  |
| PoE IEEE 802.3af. 802.3at | ANO |  |
| Dostupný výkon pro napájení portů | 370W |  |
| Wirespeed (neblokující) na všech portech | ANO |  |
| Možnost připojit externí redundantní napájecí zdroj | ANO |  |
| **Výkonnostní parametry** |  |  |
| Minimální propustnost L2/L3 přepínacího systému | 210 Gbit/s |  |
| Minimální paketový výkon přepínače | 130 Mp/s |  |
| Minimální počet MAC adres | 16000 |  |
| **Vlastnosti stohování** |  |  |
| Stohování bez snížení počtu požadovaných ethernetových portů | ano |  |
| Kompletní příslušenství pro stohování součástí (kabely, atd.) | ANO |  |
| Možnost agregace do počtu prvků | 8 |  |
| Propustnost stohovacího propoje | 80 Gbit/s |  |
| Všechna zařízení ve virtuálním celku se podílí na forwardingu paketů (distribuovaný switching) | ANO |  |
| Virtuální zařízení se ve všech ohledech chová jako jeden síťový prvek | ANO |  |
| Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením | ANO |  |
| Seskupení portů (IEEE 802.3ad) mezi různými prvky stohu | ANO |  |
| Kterýkoli prvek ve stohu může být řídícím prvkem stohu (1:N redundance) | ANO |  |
| Bezvýpadkové přepnutí na záložní řídící prvek | ANO |  |
| **Protokoly fyzické vrstvy** |  |  |
| IEEE 802.3-2005 | ANO |  |
| Podpora "jumbo rámců" | 9200 Bytes |  |
| **Protokoly 2. vrstvy** |  |  |
| IEEE 802.3ad (LACP) | ANO |  |
| Minimální počet LACP skupin | 24 |  |
| Počet aktivních linek v jedné LACP skupině | 8 |  |
| IEEE 802.1Q | ANO |  |
| Minimální počet aktivních VLAN | 1000 |  |
| IEEE 802.3az | ANO |  |
| HW připravený na nasazení IEEE 802.1ae | ANO |  |
| IEEE 802.1s - Multiple spanning tree | ANO |  |
| IEEE 802.1w - Rapid spanning Tree | ANO |  |
| IEEE 802.1p | ANO |  |
| STP instance per VLAN s 802.1Q tagováním BPDU, minimální počet podporovaných STP instancí = 128 | ANO |  |
| Kompatibilita s CDP | ANO |  |
| Detekce připojených zařízení pomocí LLDP a LLDP-MED | ANO |  |
| Detekce jednosměrnosti optické linky (např. UDLD) | ANO |  |
| STP root guard | ANO |  |
| STP loop guard | ANO |  |
| Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard) | ANO |  |
| Multicast/broadcast storm control - hardwarové omezení datového toku unicast/multicast rámců na portu v procentech | ANO |  |
| **Protokoly 3. vrstvy** |  |  |
| IPv4 a IPv6 statické směrování | ANO |  |
| OSPFv2 | ANO |  |
| OSPFv3 | ANO |  |
| IPv4 a IPv6 QoS | ANO |  |
| Hardware podpora IPv4 a IPv6 ACL | ANO |  |
| Policy based routing (PBR) pro IPv4 a IPv6 | ANO |  |
| **Multicast** |  |  |
| IGMP Snooping v1/v2/v3 | ANO |  |
| MLD snooping v1/v2 | ANO |  |
| IPv4 a IPv6 multicast VLAN | ANO |  |
| PIM DM, SM, SSM | ANO |  |
| **Bezpečnost** |  |  |
| DHCP snooping | ANO |  |
| Dynamic ARP inspection (DAI) | ANO |  |
| Verifikace mapování IP-MAC (např. IP source guard) | ANO |  |
| IPv6 First Hop Security RA guard | ANO |  |
| IPv6 First Hop Security DHCPv6 guard | ANO |  |
| IPv6 First Hop Security IPv6 SourceGuard | ANO |  |
| IPv6 First Hop Security IPv6 Binding Integrity Guard | ANO |  |
| Definování povolených MAC adres a počtu MAC adres na interface | ANO |  |
| Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy) | ANO |  |
| Ověřování 802.1X - minimálně 1024 ověřených uživatelů na systém | ANO |  |
| Ověřování MAC adres | ANO |  |
| Zařazování do VLAN a přidělení přístupových filtrů na základě 802.1X ověření | ANO |  |
| Zařazování do VLAN a přidělení přístupových filtrů na základě MAC-autentizace | ANO |  |
| Ověřování přístupu do sítě s podporou odlišných Guest VLAN (nedojde k pokusu o přihlášení), Fail VLAN (přihlášení selže) a Critical VLAN (nedostupnost RADIUS serveru) | ANO |  |
| IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu | ANO |  |
| Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x) | ANO |  |
| NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955) | ANO |  |
| Sběr dat pro NetFlow nebo IPFIX z každého portu přepínače | ANO |  |
| Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů | ANO |  |
| Statistiky určovány z každého paketu daného "flow" | ANO |  |
| Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb | ANO |  |
| Návaznost skriptů interpretovaných přepínačem po detekci daných parametrů "flow" | ANO |  |
| Zobrazení sbíraných infromací o "flow" přímo v přepínači včetně "TopN" pohledu. | ANO |  |
| Export statistik "flow" selektivně na více kolektorů | ANO |  |
| **Management** |  |  |
| CLI rozhraní | ANO |  |
| SSHv2 | ANO |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ANO |  |
| SNMPv2c | ANO |  |
| SNMPv3 | ANO |  |
| Sériová nebo USB konzolová linka | ANO |  |
| AAA ověřování uživatelů (autentizace, autorizace, accounting) -RADIUS, TACACS+ | ANO |  |
| Port mirroring | ANO |  |
| VLAN mirroring | ANO |  |
| Vzdálený mirroring (RSPAN) | ANO |  |
| Více monitorujících portů současně | ANO |  |
| Měření zakončení a délky metalického kabelu (TDR) | ANO |  |
| Podpora uživatelsky modifikovatelné automatické reakce/obsluhy událostí při provozu přepínače (pomocí skriptů) | ANO |  |
| Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute) | ANO |  |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |  |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů | ANO |  |
| NTP | ANO |  |
| DHCP server | ANO |  |

## Přístupový přepínač – 24 portů MACsec

Parametry specifikované v úvodní kapitole a parametry v následující tabulce definují minimální požadavky zadavatele na dodávané zařízení. Specifikace vychází ze současného stavu sítě zadavatele, studie proveditelnosti „Bezpečnost komunikační infrastruktury“ a předpokládaných změn a rozšíření v síti zadavatele na následujících cca 6 let. U tohoto přepínače je požadováno šifrování na druhé vrstvě OSI modelu 802.1AE – MACsec na všech portech.

|  |  |  |
| --- | --- | --- |
| *Požadavek na funkcionalitu* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| **Počet kusů** | **1** |  |
| **Základní vlastnosti** |  |  |
| Třída zařízení | L2-L3 switch |  |
| Typ chlazení | aktivní |  |
| Možnost montáže do racku | ANO |  |
| Sada pro montáž do racku součástí dodávky | ANO |  |
| Rozměry (v x š x h) [cm] | 4.5x44.5x45 |  |
| Počet portů 10/100/1000 RJ-45 | 24 |  |
| Počet portů 1 Gbit/s a jejich typ | 4xSFP |  |
| Redundantní interní napájecí zdroj, vyměnitelný za chodu | ANO |  |
| Možnost kombinace AC a DC zdroje v jednom zařízení | ANO |  |
| Redundantní ventilátory | ANO |  |
| **Výkonnostní parametry** |  |  |
| Minimální propustnost přepínacího subsystému | 90 Gbit/s |  |
| Minimální paketový výkon přepínače | 60 Mp/s |  |
| Minimální počet MAC adres | 32000 |  |
| Minimální kapacita záznamů v HW směrovací tabulce pro IPv4 | 24000 |  |
| **Vlastnosti stohování** |  |  |
| Stohování bez snížení počtu požadovaných ethernetových portů | ANO |  |
| Možnost agregace do počtu prvků | 8 |  |
| Propustnost stohovacího propoje | 80 Gbit/s |  |
| Všechna zařízení ve virtuálním celku se podílí na forwardování paketů (distribuovaný switching) | ANO |  |
| Virtuální zažízení se ve všech ohledech chová jako jeden síťový prvek | ANO |  |
| Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením | ANO |  |
| Seskupení portů (IEEE 802.3ad) mezi různými prvky stohu | ANO |  |
| Kterýkoli prvek ve stohu může být řídícím prvkem stohu (1:N redundance) | ANO |  |
| Bezvýpadkové přepnutí na záložní řídící prvek | ANO |  |
| **Protokoly fyzické vrstvy** |  |  |
| IEEE 802.3-2005 | ANO |  |
| Podpora "jumbo rámců" | ANO |  |
| **Protokoly 2. vrstvy** |  |  |
| IEEE 802.3ad | ANO |  |
| IEEE 802.1Q | ANO |  |
| Minimální počet aktivních VLAN | 1000 |  |
| IEEE 802.1X - Port Based Network Access Control | ANO |  |
| IEEE 802.1s - multiple spanning trees | ANO |  |
| IEEE 802.1w - Rapid Tree Spanning Protocol | ANO |  |
| IEEE 802.1p - Minimální počet vnitřních front | 8 |  |
| STP instance per VLAN s 802.1Q tagováním BPDU, minimální počet podporovaných STP instancí = 128 | ANO |  |
| Kompatibilita s CDP | ANO |  |
| Detekce připojených zařízení pomocí LLDP a LLDP-MED | ANO |  |
| Detekce jednosměrnosti optické linky (např. UDLD) | ANO |  |
| STP root guard | ANO |  |
| STP loop guard | ANO |  |
| Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard) | ANO |  |
| Multicast/broadcast storm control - hardwarové omezení datového toku unicast/multicast rámců na portu v procentech | ANO |  |
| **Protokoly 3. vrstvy** |  |  |
| IPv4 a IPv6 statické směrování | ANO |  |
| OSPFv2 | ANO |  |
| OSPFv3 | ANO |  |
| IPv4 a IPv6 QoS | ANO |  |
| Hardware podpora IPv4 a IPv6 ACL | ANO |  |
| Policy based routing (PBR) pro IPv4 a IPv6 | ANO |  |
| **Multicast** |  |  |
| IGMP Snooping v1/v2/v3 | ANO |  |
| MLD snooping v1/v2 | ANO |  |
| IPv4 a IPv6 multicast VLAN | ANO |  |
| PIM DM, SM, SSM | ANO |  |
| **Bezpečnost** |  |  |
| Šifrování na L2 dle IEEE 802.1AE na všech portech | ANO |  |
| DHCP snooping | ANO |  |
| Dynamic ARP inspection (DAI) | ANO |  |
| Verifikace mapování IP-MAC (např. IP source guard) | ANO |  |
| IPv6 First Hop Security RA guard | ANO |  |
| IPv6 First Hop Security DHCPv6 guard | ANO |  |
| IPv6 First Hop Security IPv6 SourceGuard | ANO |  |
| IPv6 First Hop Security IPv6 Binding Integrity Guard | ANO |  |
| Definování povolených MAC adres a počtu MAC adres na interface | ANO |  |
| Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy) | ANO |  |
| Ověřování 802.1X - minimálně 1024 ověřených uživatelů na systém | ANO |  |
| Ověřování MAC adres | ANO |  |
| Zařazování do VLAN a přidělení přístupových filtrů na základě 802.1X ověření | ANO |  |
| Zařazování do VLAN a přidělení přístupových filtrů na základě MAC-autentizace | ANO |  |
| Ověřování přístupu do sítě s podporou odlišných Guest VLAN (nedojde k pokusu o přihlášení), Fail VLAN (přihlášení selže) a Critical VLAN (nedostupnost RADIUS serveru) | ANO |  |
| IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu | ANO |  |
| Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x) | ANO |  |
| NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955) | ANO |  |
| Sběr dat pro NetFlow nebo IPFIX z každého portu přepínače | ANO |  |
| Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů | ANO |  |
| Statistiky určovány z každého paketu daného "flow" | ANO |  |
| Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb | ANO |  |
| Návaznost skriptů interpretovaných přepínačem po detekci daných parametrů "flow" | ANO |  |
| Zobrazení sbíraných infromací o "flow" přímo v přepínači včetně "TopN" pohledu. | ANO |  |
| Export statistik "flow" selektivně na více kolektorů | ANO |  |
| **Management** |  |  |
| CLI rozhraní | ANO |  |
| SSHv2 | ANO |  |
| Omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ANO |  |
| SNMPv2c | ANO |  |
| SNMPv3 | ANO |  |
| Sériová nebo USB konzolová linka | ANO |  |
| AAA ověřování uživatelů (autentizace, autorizace, accounting) -RADIUS, TACACS+ | ANO |  |
| Port mirroring | ANO |  |
| VLAN mirroring | ANO |  |
| Vzdálený mirroring (RSPAN) | ANO |  |
| port mirroring ACL (mirroruje pouze definované toky) | ANO |  |
| Vzdálený port mirroring (RSPAN) | ANO |  |
| Více monitorujících portů současně | ANO |  |
| Měření zakončení a délky metalického kabelu (TDR) | ANO |  |
| Podpora uživatelsky modifikovatelné automatické reakce/obsluhy událostí při provozu přepínače (pomocí skriptů) | ANO |  |
| Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute) | ANO |  |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |  |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů | ANO |  |
| NTP | ANO |  |
| DHCP server | ANO |  |

## Rozšiřující modul pro stávající páteřní prvky Cisco Interní informace

Do existujících páteřních prvků požaduje zadavatel dodat kompatibilní rozšiřující moduly, které v páteřních prvcích rozšíří počet portů. Rozšiřující modul musí poskytnout minimálně 8x 10 Gbit SFP+ rozhraní a musí v páteřním přepínači fungovat v režimu line-rate.

Požadovaný počet kusů: 2

Interní informace

## Optické transceivery 10 Gbit SingleMode

Pro nahrazované přepínače požaduje zadavatel dodání kompatibilních optických transceiverů a to jak na stranu páteřních prvků, tak na stranu přístupových prvků. Transceivery musí pracovat na rychlosti 10 Gbit po SingleMode vlákně.

|  |  |  |
| --- | --- | --- |
| *Požadavek na funkcionalitu* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| **Počet kusů** | **56** |  |
| **Základní vlastnosti** |  |  |
| Třída zařízení | optický transceiver |  |
| Formát zařízení | výměnný modul |  |
| Rychlost | 10Gb |  |
| Dosah | 10km |  |
| optický mód | SMF |  |
| Vlnová délka světla | 1310 nm |  |
| teplotní rozsah | standard |  |
| konektor vlákno | LC duplex |  |
| konektor box | GLC |  |

## Stohovací sady pro přístupové přepínače

Zadavatel v několika serverovnách plánuje stohování přístupových přepínačů. Pro tyto účely zadavatel požaduje dodání stohovací technologie, která bude kompatibilní se všemi dodávanými přístupovými přepínači.

|  |  |  |
| --- | --- | --- |
| *Požadavek na funkcionalitu* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| **Počet kusů** | 12 |  |
| **Parametry** |  |  |
| Max. počet členů stohu | 8 |  |
| Propustnost stohu | 80 Gbit/s |  |
| Dedikované porty pro stohování | ANO |  |