# 6 Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě

## High-level popis požadovaného řešení

### Stávající stav

Síť KÚPK je zabezpečena implementací technologie Cisco ISE. Cisco ISE jako autentizační systém řídí přístup k portům LAN a k WiFi pomocí technologie 802.1X. Při provozu řešení vznikají provozní problémy s autentizací pracovních stanic, které je třeba řešit vytvářením výjimek z autentizace. Současně je třeba monitorovat stavy jednotlivých autentizačních relací. Existující nástroje jsou pro potřeby KÚPK nedostatečné a cílem je jejich rozšíření nástroji dle níže uvedené funkční specifikace.

## Požadavky na řešení

### Nástroj na řízení výjimek pomocí autentizace MAC adres zařízení

Aplikace musí být schopna spravovat databázi velkého množství MAC adres zařízení nejrůznějšího typu, kterým je nutné přiřadit krátkodobou nebo dlouhodobou výjimku pro přístup do sítě. Operace, provedené v aplikaci, musí být prostřednictvím REST API synchronizovány s Cisco ISE. Systém musí umožňovat přidávání a odebírání MAC adres zařízení externích pracovníků, interních zaměstnanců, počítačů určených k nové instalaci nebo k reinstalaci, speciálních zařízení jako jsou tiskárny, IP telefony apod. a zařízení, která mají mít omezený nebo zablokovaný přístup do sítě (blacklisting).

Přístup do aplikace a k jejím funkcím musí být založen na Active Directory skupinách tak, aby bylo možné definovat role uživatelů. Aplikace musí umožnit definici Read-Only a Read-Write přístupu pro uživatele.

Expirace záznamů MAC adres musí být umožněna manuálně, zásahem uživatele v GUI aplikace, ale i automaticky, kdy budou MAC adresy ze systému odebírány po vypršení předem nastaveného času.

Aplikace musí umožnit auditování akcí prováděných všemi uživateli při práci s jednotlivými záznamy i provedených automaticky. Aplikace musí mít uživatelsky přívětivé rozhraní a předdefinovaná workflow, která umožní efektivní práci uživatelů.

Jednotlivé operace se záznamy musí být možné provádět nejen ručně, uživateli, ale i automaticky pomocí REST API volání z externích aplikací, aby bylo možné aplikaci integrovat do existujících IT nástrojů.

Aplikace musí být integrovaná s Podpůrnou aplikací pro provozní monitoring 802.1X autentizace musí být schopná pracovat v HA režimu.

Aplikace musí umožnit registraci minimálně 500 zařízení a být licenčně rozšiřitelná až na 1000 zařízení.

|  |  |  |
| --- | --- | --- |
| *Požadavek na funkcionalitu* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| Aplikace umožňuje správu MAC adres, které pro přístup do sítě potřebují časově omezenou výjimku. | ANO |  |
| Aplikace umožňuje správu MAC adres, které pro přístup do sítě potřebují časově neomezenou výjimku. | ANO |  |
| Aplikace umožňuje správu MAC adres počítačů určených k nové instalaci. | ANO |  |
| Aplikace umožňuje správu MAC adres počítačů určených pro reinstalaci. | ANO |  |
| Aplikace umožňuje správu MAC adres zařízení externích pracovníků (kontraktorů). | ANO |  |
| Aplikace umožňuje správu MAC adres zařízení interních zaměstnanců (BYOD, nedoménová zařízení). | ANO |  |
| Aplikace umožňuje správu MAC adres zařízení, která nepodporují standard 802.1X. | ANO |  |
| Aplikace umožňuje správu MAC adres zařízení, která mají mít zablokovaný nebo omezený přístup do sítě. | ANO |  |
| Přístup k funkcionalitám se řídí na základě členství v Active Directory skupině. | ANO |  |
| Na základě členství v Active Directory je možné v aplikaci odlišit Read-Only a Read-Write přístup. | ANO |  |
| Aplikace umožňuje načtení MAC adresy zařízení z předem definovaných portů. | ANO |  |
| Aplikace obsahuje vestavěná workflow pro efektivní práci uživatelů. | ANO |  |
| Aplikace umožňuje propojení s Podpůrnou aplikací pro provozní monitoring 802.1X autentizace. | ANO |  |
| Aplikace umožňuje manuální správu MAC adres přes webové rozhraní. | ANO |  |
| Aplikace umožňuje automatizovanou správu MAC adres přes REST API. | ANO |  |
| Aplikace nabízí automatické odmazání MAC adres, kterým vyprší časově omezená výjimka. | ANO |  |
| Aplikace ukládá záznam o veškerých operacích s MAC adresami, uskutečněných manuálně přes webové rozhraní jakýmkoliv uživatelem, automaticky a přes REST API. | ANO |  |
| Aplikace umožňuje vytvářet reporty o výjimkách na základě nejrůznějších parametrů. | ANO |  |
| Aplikace umožňuje udržovat konzistenci v databázi výjimek zavedených do Cisco ISE přes aplikaci. | ANO |  |
| Aplikaci je možné provozovat v High-availability režimu. | ANO |  |
| Aplikaci je možné konfigurovat přes webové rozhraní. | ANO |  |

### Podpůrná aplikace pro provozní monitoring 802.1X autentizace

Nabídka musí obsahovat aplikaci, která poskytne komplexní informace o stavu 802.1X autentizace a umístění zařízení na portech předem definovaných přepínačů. V aplikaci by mělo být možné minimálně vyhledávání MAC adres, přepínačů a uživatelů, stavových informací o autentizační relaci a vzdálené vynucení reautentizace. Přístup do aplikace a k jejím funkcím musí být založen na Active Directory skupinách tak, aby bylo možné definovat role uživatelů a povolit pouze nezbytně nutné přístupy. Aplikace by měla uchovávat historii dění na přepínačích po předem definovanou dobu. Aplikace musí být schopná pracovat v HA režimu.

Aplikace musí být integrovaná s Nástrojem na řízení výjimek pomocí autentizace MAC adres zařízení.

|  |  |
| --- | --- |
| *Požadavek na funkcionalitu* | *Splněno: ANO / NE / Hodnota* |
| Aplikace umožňuje přístup k informacím o stavu 802.1x autentizace zařízení v síti. |  |
| V aplikaci je možné definovat přepínače, které budou monitorovány. |  |
| Aplikace umožňuje vyhledávat umístění určitého zařízení v síti na základě jeho MAC adresy. |  |
| Aplikace umožňuje vyhledávat zařízení na základě jména uživatele nebo jména zařízení. |  |
| Aplikace umožňuje analyzovat stav autentizačních relací na portech předem definovaných přepínačů. |  |
| Aplikace umožňuje zobrazení předem definovaných informací o uživateli nebo pracovní stanici z Active Directory. |  |
| Aplikace umožňuje zobrazení informací o autentizační relaci z přepínače. |  |
| Aplikace umožňuje zobrazení informací o autentizační relaci z Cisco ISE. |  |
| Aplikace umožňuje zobrazení informací o konfiguraci portu přepínače. |  |
| Aplikace umožňuje vynutit vzdálenou reautentizaci nebo odpojení zařízení od sítě. |  |
| Aplikace umožňuje propojení s Nástrojem na řízení výjimek pomocí autentizace MAC adres zařízení. |  |
| Přístup k funkcionalitám se řídí na základě členství v Active Directory skupině. |  |
| Aplikace uchovává historii dění v síti po předem definovanou dobu. |  |
| Aplikaci je možné provozovat v High-availability režimu. |  |
| Aplikaci je možné konfigurovat přes webové rozhraní. |  |

### Integrace do existujících procesů KÚPK

Součástí dodávky musí být analýza stávajících IT procesů KÚPK, jejich případná změna a integrace dodávaných nástrojů tak, aby došlo ke zvýšení efektivity správy 802.1X řešení. Jde především o procesy detekce chybových stavů, vytváření výjimek a proces reimage pracovních stanic na zabezpečených portech.